

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники

Кафедра
«Информационная
безопасность систем и технологий»

Специальность 10.05.02 –

Информационная безопасность
телекоммуникационных систем

Специализация -

Разработка защищенных
телекоммуникационных систем

ДИПЛОМНАЯ РАБОТА

на тему

СИСТЕМА МОНИТОРИНГА СЕТЕВЫХ КОМПОНЕНТОВ В
РАСПРЕДЕЛЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ
ДАННЫХ

Студент _____ Посоркин Сергей Владимирович

Руководитель _____ Мещеряков А.А

Нормоконтролёр _____ Фатеев А.Г

Рецензент главный специалист лаборатории средств
обнаружения НИКИРЭТ - филиал ФГУП ФНПЦ
ПО «Старт» им. М.В Проценко _____ Иванов В.Э

Работа допущена к защите (протокол заседания кафедры от _____ № _____)

Заведующий кафедрой _____ С.Л. Зефилов

Работа защищена с отметкой _____ (протокол заседания ГЭК
от _____ № _____)

Секретарь ГЭК _____ А.Г. Фатеев

Пенза 2017

РЕФЕРАТ

Отчет о дипломной работе содержит 122 страницы, 9 источников, 1 таблица, 84 рисунка, 9 приложений.

ИНФОРМАЦИОННАЯ СИСТЕМА ПЕРСОНАЛЬНЫХ ДАННЫХ, ПЕРСОНАЛЬНЫЕ ДАННЫЕ, МЕТОДЫ МОНИТОРИНГА СЕТЕВЫХ КОМПОНЕНТОВ, СЕТЕВОЕ ОБОРУДОВАНИЕ, ИНФОРМАЦИОННЫЕ ПОТОКИ, СТРУКТУРА ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ, КОММУТАЦИОННОЕ ОБОРУДОВАНИЕ, КОНФИГУРАЦИИ ФАЙЛОВ, ТРЕБОВАНИЯ К КОММУТАЦИОННОМУ ОБОРУДОВАНИЮ, ТРЕБОВАНИЯ К ПЕРСОНАЛЬНОМУ КОМПЬЮТЕРУ.

Данная ВКР выполняется как составная часть ОКР на разработку системы, выполняемой на предприятии, где выполнялась ВКР. Информация о характеристиках, функциональных возможностях и местах размещения является информацией ограниченного распространения, которую возможно предоставлять только после согласования с заказчиком ОКР. Поэтому в дипломной работе рассматривается как распределенная ИСПДн.

Целью ВКР является разработка системы мониторинга сетевых компонентов для распределенной информационной системы персональных данных.

Актуальность данной ВКР заключается в том, что данная разработка будет использоваться в рамках выполнения ОКР. ИСПДн, для которой разрабатывается система мониторинга сетевых компонентов, является территориально разнесенной системой, объединяющей локальные объекты информатизации, построенной на базе ЛВС. Каждая ЛВС на объекте разделена на сегменты (участки) обрабатывающие ПДн и не обрабатывающие ПДн, но все они объединены в единую систему ИСПДн. Оборудование не обрабатывающие ПДн находится на границе КЗ и использует беспроводные каналы связи. В нормативных документах по защите информации не предъявляются требования по обеспечению

безопасности информации на объектах информатизации или его составных частях не обрабатывается информация, подлежащая защите.

В данной ИСПДн, на локальном объекте в сегменте ЛВС не обрабатывающего ПДн могут возникнуть угрозы информационной безопасности, не отнесенные к актуальным, в случае несанкционированного подключения оборудования к ЛВС.

Для этого будет разработана система мониторинга сетевых компонентов, которая осуществляет контроль коммутационного оборудования с помощью протоколов контроля доступа. В случае нарушения правил доступа или нарушения конфигураций доступа, будет отправлено сообщение на АРМ администратора безопасности, для принятия решения. Требования по сертификату такого оборудования не предъявляется, т.к система является дополнительным инструментом для администратора безопасности. Эта система будет применена в распределенной ИСПДн как дополнительный инструмент безопасности.

Для создания системы мониторинга сетевых компонентов в распределенной ИСПДн в ходе ВКР было:

- а) изучена структура информационной системы персональных данных с точки зрения обеспечения мониторинга коммутационного оборудования;
- б) изучены возможные методы мониторинга состояния коммутационного оборудования;
- в) изучен протокол SNMP для анализа состояния коммутационного оборудования;
- д) осуществлен выбор программного обеспечения для системы мониторинга;
- е) разработаны требования к коммутационному оборудованию и осуществлен выбор коммутационного оборудования;
- ж) разработаны требования к характеристикам ПЭВМ для системы мониторинга;

- и) разработан перечень контролируемых событий на коммутационном оборудовании;
- к) разработаны типовые конфигурации файлов для коммутационного оборудования, используемого в ИСПДн;
- л) разработана конфигурация (настройка) программного обеспечения используемого для системы мониторинга.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УДК 004.056

Политехнический институт

УТВЕРЖДАЮ

Факультет приборостроения,
информационных технологий и
электроники

Зав. кафедрой ИБСТ
к.т.н., доцент С.Л. Зефирова

Выпускающая кафедра:

«___» _____ 2016 г.

Информационная безопасность систем
и технологий

Учебная группа 11ПТ1

ТЕХНИЧЕСКОЕ ЗАДАНИЕ НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ

Студента группы 11ПТ1 Посоркина Сергея Владимировича

Специальность 10.05.02 Информационная безопасность
– телекоммуникационных систем

Тема дипломной работы:

Система мониторинга сетевых компонентов в распределенной
информационной системе персональных данных.

Руководитель ВКР

Начальник отделения защиты информации НИКИРЭТ – филиал ФГУП
ФНПЦ ПО «Старт» им. М.В. Проценко А.А. Мещеряков

Нормоконтролер

к.т.н., доцент кафедры ИБСТ

А.Г. Фатеев

1 Цели и задачи ВКР

Цель работы – разработать систему мониторинга сетевых компонентов для распределенной информационной системы персональных данных.

Система мониторинга сетевых компонентов в распределенной информационной системе персональных данных предназначена для отслеживания подозрительных вызовов и несанкционированного доступа к персональным данным, несанкционированного доступа к сетевым компонентам.

2 Тактико-технические требования к выполнению ВКР

Система мониторинга сетевых компонентов для распределенной информационной системы персональных данных включает в себя:

- автоматизированное рабочее место на базе ПЭВМ;
- программное обеспечение, необходимое для мониторинга сетевых компонентов, функционирующее в среде Microsoft Windows.

Технические требования:

- управляющая часть системы мониторинга должна состоять из автоматизированного рабочего места на базе ПЭВМ, функционирующего на базе семейства операционной системы Microsoft Windows;
- программное обеспечение системы мониторинга должно функционировать в операционной системе Microsoft Windows;
- программное обеспечение должно обеспечивать регистрацию сообщений от коммутационного оборудования;
- программное обеспечение должно обеспечивать обработку сообщений от коммутационного оборудования;
- программное обеспечение должно обеспечивать отображение информации о состоянии коммутационного оборудования.

В ВКР должны быть рассмотрены следующие вопросы:

- изучение структуры информационной системы персональных данных с точки зрения обеспечения мониторинга коммутационного оборудования;

- возможные методы мониторинга состояния коммутационного оборудования;
- использование протокола SNMP для анализа состояния коммутационного оборудования;
- выбор программного обеспечения для системы мониторинга;
- требования к коммутационному оборудованию;
- требования к характеристикам ПЭВМ для системы мониторинга;
- разработка перечня контролируемых событий на коммутационном оборудовании;
- разработка типовых конфигурации файлов для коммутационного оборудования, используемого в ИСПДн;
- разработка конфигурации или настройка программного обеспечения используемого для мониторинга.

3 Требования к разрабатываемой документации

Отчет по ВКР выполняется в соответствии с требованиями ГОСТ 7.32.

Перечень и содержание графической части ВКР:

- структура информационной системы персональных данных – 1 л., ф. А1 (плакат);
- структура информационных потоков в информационной системе персональных данных – 1 л., ф. А1 (плакат);
- состав системы мониторинга – 1 л., ф. А1 (плакат);
- состав программного обеспечения системы мониторинга – 1 л., ф. А1 (плакат);
- структура информационного обмена при мониторинге сетевых компонентов – 1 л., ф. А1 (плакат);
- порядок настройки системы мониторинга – 1 л., ф. А1 (плакат).

Электронная копия отчета и графической части ВКР должна быть представлена на магнитном или оптическом носителе.

4 Сроки выполнения ВКР

Тема утверждена приказом ректора ПГУ № ____ от «__» _____ 2016 г.

Дата выдачи задания « __ » _____ 2016 г.

Время дипломного проектирования с « __ » _____ 2016 г. по « __ » _____ 2016 г.

Задание к исполнению принял « __ » _____ 2016 г.

Исполнитель ВКР _____ Посоркин С.В.

СОДЕРЖАНИЕ

Введение.....	15
1 Изучение структуры информационной системы персональных данных с точки зрения обеспечения мониторинга коммутационного оборудования.....	17
2 Возможные методы мониторинга состояния коммутационного оборудования	29
3 Использование протокола SNMP для анализа состояния коммутационного оборудования	38
4 Выбор программного обеспечения для системы мониторинга.....	41
5 Требования к коммутационному оборудованию.....	45
6 Требования к характеристикам ПЭВМ для системы мониторинга....	51
7 Разработка перечня контролируемых событий на коммутационном оборудовании.....	53
8 Разработка типовых конфигураций файлов для коммутационного оборудования, используемого в ИСПДн.....	54
9 Разработка конфигурации или настройка программного обеспечения используемого для системы мониторинга.....	55
Заключение	92
Список использованных источников	94
Приложение А Структура ИСПДн.....	95
Приложение Б Структура информационных потоков в ИСПДн.....	97
Приложение В Состав системы мониторинга	99
Приложение Г Состав программного обеспечения системы мониторинга.....	101
Приложение Д Файл конфигурации для коммутатора cisco 2960-s....	103
Приложение Е Файл конфигурации для межсетевого экрана ССПТ-2.....	111
Приложение Ж Порядок настройки системы мониторинга.....	117

Приложение И Структура информационного обмена при мониторинге сетевых компонентов.....	119
Приложение К Результат проверки системы "Антиплагиат".....	121

ОПРЕДЕЛЕНИЯ

В отчете применяют следующие термины с соответствующими определениями:

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники [1].

Безопасность персональных данных - состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных [1].

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств [1].

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных [1].

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) [1].

Автоматизированное рабочее место - комплекс программно-технических средств, используемый для подготовки и ввода в систему в электронном виде информации, а также для организации регламентированного доступа пользователей к информации, содержащейся в системе [2].

Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций [2].

Доступ к информации - возможность получения информации и ее использования [3].

Информация - сведения (сообщения, данные) независимо от формы их представления [3].

Обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам [3].

Защита информации от несанкционированного доступа - деятельность, направленная на предотвращение или существенное затруднение несанкционированного доступа к информации (или воздействия на информацию) [4].

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации [4].

Несанкционированный доступ - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных [5].

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АРМ СБ – автоматизированное рабочее место службы безопасности

АРМ ТО – автоматизированное рабочее место технического обслуживания

АРМ А – автоматизированное рабочее место администратора

АРМ АБ – автоматизированное рабочее место администратора безопасности

АРМ УК – автоматизированное рабочее место управления криптосетью

БСУУ – блок считывателей управляющий универсальный

БМ – блок мониторный

БД – база данных

ИБ – информационная безопасность

ИС – информационная система

ИСПДн – информационная система персональных данных

ИТ – информационные технологии

ЛВС – локально вычислительная сеть

МСС – мультисервисная сеть связи

МЭ – межсетевой экран

МТ – мобильный терминал

НСД – несанкционированный доступ

ОДС – оборудование дистанционного считывания

ОСБД – объектовый сервер базы данных

ПТС – программно – технические средства

ПЗИ – подсистема защиты информации

РД – руководящий документ

СС – сервер связи

СМ – стойка мониторная

СБ – служба безопасности

СЗИ – средства защиты информации

СКЗИ – средства криптографической защиты

COB – средства обнаружения вторжений

MIB – management Information Base

OID – object identifier

SNMP – simple network management protocol

VPN – virtual Private Network, виртуальная частная сеть

Wi-Fi – wireless Fidelity, семейство стандартов передачи цифровых потоков данных по радиоканалам

ВВЕДЕНИЕ

Обеспечение информационной безопасности (ИБ) — является важной целью в обществе с быстрым развитием информационных технологий. Обеспечение информационной безопасности особенно важно, когда информация является персональными данными или сведениями, ограниченными в распространении. Поэтому работая с большим количеством информации можно воспользоваться одним из методов обеспечения информационного безопасности как мониторинг коммутационного оборудования.

Мониторинг коммутационного оборудования — является одним из способов обеспечения ИБ и непростой задачей, которая может вызвать значительные затраты сил, времени и денежных средств, данная задача является частью работы администраторов ИБ. Разработка системы мониторинга сетевых компонентов позволит упростить обеспечение ИБ. Для этого в данной дипломной работе разрабатывается система мониторинга сетевых компонентов, которая будет осуществлять контроль сетевого оборудования с помощью протоколов контроля доступа. В случае нарушения правил доступа или нарушения конфигураций доступа, будет отправлено сообщение на АРМ администратора безопасности, для принятия решения.

В процессе работы были выполнены следующие этапы:

- изучена структура информационной системы персональных данных с точки зрения обеспечения мониторинга коммутационного оборудования;
- изучены возможные методы мониторинга состояния коммутационного оборудования;
- использование протокола SNMP для анализа состояния коммутационного оборудования;
- осуществлен выбор программного обеспечения для системы мониторинга;
- разработаны требования к коммутационному оборудованию;

- разработаны требования к характеристикам ПЭВМ для системы мониторинга;
- разработан перечень контролируемых событий на коммутационном оборудовании;
- разработаны типовые конфигурации файлов для коммутационного оборудования, используемого в ИСПДн;
- разработаны конфигурации (настройка) программного обеспечения используемого для системы мониторинга.

1 Изучение структуры информационной системы персональных данных с точки зрения обеспечения мониторинга коммутационного оборудования

В ходе дипломного проектирования была изучена информационная система персональных данных с точки зрения обеспечения мониторинга коммутационного оборудования и обеспечения защиты. Изучение структуры информационной системы персональных данных так же включает в себя анализ информационных потоков в данной ИСПДн. Структура ИСПДн представлена в приложении А.

Информационная система персональных данных является территориально распределенной информационной системой, которая включает в свой состав объекты информатизации, пользователей ИСПДн, программно-технический комплекс и линии связи.

Объектом информатизации информационной системы персональных данных является совокупность информационных ресурсов, программно – технических средств и локальной сети, используемых в соответствии с заданной информационной технологией, помещений на объектах, в которых они установлены.

Телекоммуникационное взаимодействие объектов ИСПДн реализовано через развертываемую защищенную сеть VPN с использованием СКЗИ, функционирующую через мультисервисную сеть связи (МСС) провайдера связи на базе технологии MPLS VPN L3.

Информационная система персональных данных включает в себя следующие объекты информатизации:

- центральный сервер базы данных;
- объекты ИСПДн (спортивные объекты);
- центр управления и технической поддержки.

Центральный сервер базы данных состоит из:

- сервера базы данных (центрального);
- сервера связи;

- сервера безопасности;
- сервера хранения данных;
- СКЗИ;
- коммутационного оборудования;
- межсетевого экрана;
- узел связи.

Центральному серверу базы данных необходимо получать информацию из билетной системы. Для получения информации из билетной системы, центральный сервер базы данных имеет доступ к сети интернет, откуда получает данные из билетной системы. Для безопасного соединения с сетью интернет в центральном сервере базы данных используется подключение через межсетевой экран. Для обеспечения связи с другими объектами информатизации и системами, коммутационное оборудование подключено к сети провайдера на базе технологии MPLS VPN L3.

Объект ИСПДн (спортивные объекты) состоит из:

- помещения службы безопасности;
- помещение технической поддержки;
- серверной стадиона;
- КПП №1..N;
- узла связи;
- коммутационного оборудования.

Помещение службы безопасности включает в себя:

- АРМ службы безопасности;
- принтер.

К автоматизированному рабочему месту службы безопасности подключен принтер. Для связи с серверной стадиона, АРМ СБ подключено к линии связи по сети Ethernet.

Помещение технической поддержки включает в себя:

- АРМ технического обслуживания;

- АРМ администратора;
- принтер.

Автоматизированные рабочие места имеют подключение к принтеру. АРМ ТО и АРМ администратора для связи с серверной стадиона подключены к линии связи по сети Ethernet.

Серверная стадиона состоит из:

- сервера ОСБД;
- сервера безопасности;
- узла связи;
- коммутационного оборудования;
- межсетевых экранов.

Серверная стадиона подключена к системе управления объектом. Для обеспечения безопасности, подключение реализовано через межсетевой экран. Так же для обеспечения безопасного подключения КПП к серверной стадиона, коммутационное оборудование подключено через межсетевой экран. Для обеспечения связи с другими объектами информатизации и системами, коммутационное оборудование подключено к сети провайдера на базе технологии MPLS VPN L3.

КПП включает в себя:

- коммутационное оборудование;
- оборудование безопасности;
- авто проезды;
- мобильные терминалы;
- Wi-Fi точку доступа;
- линию связи.

Оборудование безопасности состоит из:

- БСУУ (для считывания идентификатора и служебной информации, управления исполнительным устройством (турникетами)), БМ

(для отображения информации об абоненте) для организации входа и/или выхода аккредитованных лиц, гостей;

– ОДС, обеспечивает автоматическое сканирование идентификаторов, служебной информации. ОДС используется для дистанционного считывания идентификатора пропускных документов при свободном выходе абонентов с объекта. ОДС обеспечивает передачу сообщений о фактах регистрации идентификаторов в базу данных ОСБД как события доступа.

Авто-проезды состоят из мобильного беспроводного ручного терминала, реализующего функции сканирования идентификатора и отображение фотографии абонента на дисплее. Мобильный терминал обеспечивает обслуживание абонентов на транспортном КПП и у калиток на КПП. Передача данных мобильным терминалом осуществляется по стандарту Wi-Fi IEEE 802.11 a/b/g.

Оборудование безопасности и авто проезды подключены к коммутационному оборудованию по линии связи с помощью сети Ethernet.

Объект информатизации центр управления и технической поддержки состоит из:

- сервера базы данных (Резервный);
- сервер безопасности;
- резервный сервер связи;
- СКЗИ;
- коммутационного оборудования;
- межсетевого экрана;
- АРМ администратора;
- АРМ администратора безопасности;
- АРМ управления криптосетью;
- АРМ администратора БД;
- АРМ ТО;

- узел связи.

Сервера центра управления и технической поддержки подключены к автоматизированным рабочим местам через узел связи. Центру управления и технической поддержки необходимо получать информацию из билетной системы. Для получения информации из билетной системы, центр управления и технической поддержки имеет доступ к сети интернет, откуда получает данные из билетной системы. Для безопасного соединения с сетью интернет в центре управления и технической поддержки используется подключение через межсетевой экран. Для обеспечения связи с другими объектами информатизации и системами, коммутационное оборудование подключено к сети провайдера на базе технологии MPLS VPN L3.

Система аккредитации (основной дата-центр), система аккредитации (резервный дата-центр), система регистрации зрителей (основной дата-центр), система регистрации зрителей (резервный дата-центр), система управления соревнованиями, связаны с другими объектами информатизации через узел связи, с помощью подключения коммутационного оборудования к сети провайдера на базе технологии MPLS VPN L3.

Пользователями информационной системы персональных данных являются:

- сотрудники службы безопасности объекта где развернута ИСПДн;
- системные администраторы;
- администраторы баз данных;
- администраторы безопасности;
- эксплуатационно-технический персонал.

Функции пользователей обеспечиваются с помощью соответствующего набора программно-технических средств (ПТС), объединенных локальными сетями на объектах.

Анализ информационных потоков в информационной системе персональных данных. Информационная система персональных данных обрабатывает различные виды информации такие как:

- персональные данные;
- служебная информация.

Структура информационных потоков для ИСПДн представлена в приложении Б.

Объект информатизации центральный сервер базы данных осуществляет обработку и хранение информации, которая поступает от других объектов информатизации или систем. Объект информатизации центральный сервер базы данных осуществляет передачу и прием следующей информации:

- ФИО, ФОТО, данные документов удостоверяющих личность, номер пропуска, и т.д.;
- получение подтверждающих квитанций, служебной информации;
- информация о билетах (штрих-код, код соревнования и т.д.);
- информация об использованных билетах.

Информация поступает и передается по выделенной сети провайдера на базе технологии MPLS VPN L3.

В объекте информатизации основной сервер связи осуществляет временное хранение информации из внешних систем (аккредитации, регистрации зрителей, билетной и др.), поступающей в ИСПДн. Так же осуществляет передачу информации в БД, обмен информацией с внешними системами (в том числе передача информации через сеть интернет (не ПДн), удаление переданной информации. Основной сервер связи осуществляет хранение информации в системе хранения данных.

В объекте информатизации центральный сервер БД осуществляет хранение и обработку информации поступающей от окончного оборудования, информации поступающей из внешних систем (аккредитации, регистрации зрителей, билетной и др.). Так же центральный сервер БД

осуществляет обработку поступающих запросов от АРМ, формирование и отправку ответов на запросы, архивирование и хранение архивов БД.

В объекте информатизации сервер безопасности осуществляет хранение и обработку служебной информации и информации об обеспечении безопасности.

Все данные в объекте информатизации передаются по линии связи и коммутационному оборудованию.

Объект информатизации центр управления и технической поддержки передает и получает информацию из билетной системы через сеть интернет. От билетной системы центр управления и технической поддержки получает следующую информацию:

- информация о билетах (штрих-код, код соревнования и т.д.);
- информация об использованных билетах.

Так же центр управления и технической поддержки через сеть интернет осуществляет обмен электронными письмами и СМС оповещениями о работе ИСПДн с персоналом технической поддержки.

Сервер безопасности осуществляет хранение и обработку служебной информации и информации об обеспечении безопасности.

Резервный кластер БД осуществляет хранение информации из внешних систем (аккредитации, регистрации зрителей, билетной и др.), поступающей в ИСПДн в аварийных ситуациях (выход из строя основного сервера БД, нарушения в работе каналов связи с основным сервером, проведение ремонтных работ и пр.).

Резервный сервер связи осуществляет временное хранение информации из внешних систем (аккредитации, регистрации зрителей, билетной и др.), поступающей в ИСПДн в аварийных ситуациях (выход из строя основного сервера связи, нарушения в работе каналов связи с основным сервером, проведение ремонтных работ и пр.). Так же резервный сервер связи осуществляет передачу информации в БД, обмен информацией с внешними

системами (в том числе передача информации через сеть Интернет (не ПДн)), удаление переданной информации.

АРМ управления криптосетью осуществляет хранение архивов событий, вывод на печать информации о событиях криптосистемы, хранение файлов конфигурации и ключевой информации. Администратор криптографической системы передает управляющие команды конфигурирования и управления криптографическим и сетевым оборудованием ИСПДн в АРМ. АРМ управления криптосетью отображает информацию о состоянии криптографической системы. Так же возможно чтение и запись информации со съемных носителей.

АРМ администратора БД осуществляет:

- настройку и конфигурацию БД;
- просмотр и формирование отчетов состояния БД;
- мониторинг и удаленное управление БД.

Администратор БД передает информацию об управляющих командах конфигурирования и управления в АРМ администратора БД. АРМ администратора БД отображает информацию о состоянии (в том числе и ПДн).

АРМ системного администратора осуществляет:

- обновление систем;
- мониторинг состояния и удаленное управление парком серверов;
- администрирование домена, VM, DNS, отказоустойчивых кластеров.

Системный администратор передает информацию об управляющих командах конфигурирования и управления. АРМ системного администратора отображает информации о состоянии системы.

АРМ ТО осуществляет:

- обновление файлов периферийного оборудования;
- хранение архивных копий СПО;
- управление периферийным оборудованием;

- отображение информации о состоянии периферийного оборудования в режиме реального времени;
- обмен сообщениями текстовыми и звуковыми между сотрудниками.

Технический персонал передает информацию об управляющих командах конфигурирования периферийным оборудованием, осуществляет загрузку файлов конфигурации периферийного оборудования. АРМ ТО отображает информацию о состоянии периферийного оборудования ИСПДн. Так же возможно чтение и запись информации со съемных носителей.

АРМ администратора безопасности осуществляет:

- хранение архивов событий;
- вывод на печать информации о событиях СЗИ;
- хранение файлов конфигурации.

Администратор безопасности передает информацию об управляющих командах конфигурирования и управления системы защиты информации. АРМ администратора безопасности отображает информацию о состоянии системы защиты информации.

Все данные в объекте информатизации передаются по линии связи и коммутационному оборудованию.

По сети общего пользования (выделенная сеть провайдера L3) передается следующая информация:

- (ФИО, ФОТО, данные документов удостоверяющих личность, номер пропуска, и т.д.);
- получение подтверждающих квитанций.

Данная информация предназначена для систем аккредитации, регистрации зрителей, управления соревнованиями. Эта информация поступает на защищенный узел связи на каждой системе.

Объект информатизации стадион, по выделенной сети провайдера осуществляет обмен информацией между центральным кластером БД и объектовым кластером БД.

В помещении СБ, АРМ СБ осуществляет формирование запросов к объектовому и центральному кластеру БД ПДн. Так же обрабатывает полученные ответы. Оператор передает информацию о данных (ПДн) для отправки запросов в БД. АРМ СБ отображает информацию (ПДн) о результатах запроса. Так же АРМ СБ осуществляет вывод результатов запроса на бумажный носитель (печать на принтере) или на съемный магнитный носитель.

В помещении ТП, АРМ ТО и АРМ администратора передает информацию по линии связи. Информация, содержащаяся в АРМ ТО описана выше. АРМ администратора осуществляет:

- обновление систем;
- мониторинг состояния и удаленное управление серверной стадионой;
- администрирование домена, VM, DNS, отказоустойчивых кластеров;
- настройка и конфигурация БД;
- просмотр и формирование отчетов состояния БД;
- мониторинг и удаленное управление БД;
- хранение архивов событий, вывод на печать информации о событиях, хранение файлов конфигурации.

Системный администратор передает информацию об управляющих командах конфигурирования и управления. АРМ администратора отображает информацию о состоянии (в том числе и ПДн). Так же имеется возможность осуществлять чтение и запись на съемные накопители, и вывод результатов, отчетов на печать.

В серверной стадионой, сервер ОСБД осуществляет:

- хранение и обработку информации, поступающей от окончного оборудования, информации поступающей из основного (резервного) кластера БД;
- обработку поступающих запросов от АРМ;

- формирование и отправку ответов на запросы;
- архивирование и хранение архивов БД.

КПП состоят из мобильных терминалов и оборудования безопасности.

Мобильные терминалы осуществляют:

- считывание идентификаторов;
- отправку запросов в объектовую базу данных;
- обработку ответов из объектовой БД;
- временное хранение и отображение информации на дисплее устройства (фотографию и ФИО);
- отправку информации о результатах прохода.

Оборудование безопасности осуществляет:

- считывание идентификаторов;
- временное хранение информации о считанных идентификаторах;
- удаление после отправки информации в объектовую базу данных.

Для безопасной передачи данных с мобильных терминалов используется подключение Wi-Fi точки доступа через межсетевой экран.

К стадиону подключена система управления стадионом через межсетевой экран, которая получает информацию о заполняемости стадиона (количество зафиксированных проходов по билетам).

В связи с большим количеством информации, которая циркулирует в ИСПДн, необходимо осуществлять контроль целостности, доступности и конфиденциальности этой информации. Данный контроль над информацией можно осуществлять путем контроля состояния коммутационного оборудования, межсетевых экранов. С помощью настройки ПО для контроля коммутационного оборудования и межсетевых экранов, можно обеспечить безопасное подключение всех компонентов информационной системы. Однако не всегда возможно обеспечить доступность информации, так как могут возникнуть угрозы, не являющиеся актуальными, такие как несанкционированное подключение к коммутационному оборудованию.

Чтобы обеспечить доступность, целостность информации, необходимо производить мониторинг коммутационного оборудования, тем самым обеспечить контроль состояния коммутационного оборудования, и сохранить доступность, целостность информации.

Система мониторинга сетевых компонентов состоит из программных средств и аппаратных средств.

Программные средства состоят из:

- программного обеспечения для системы мониторинга - 10

Страйк: Мониторинг сети Pro;

- стандартный набор программ для Windows;
- ОС Windows.

Аппаратные средства состоят из:

- АРМ на базе ПЭВМ;
- коммутационное оборудование в объектах информатизации.

Состав системы мониторинга представлен в приложении В.

2 Возможные методы мониторинга состояния коммутационного оборудования.

Существует множество методов мониторинга сетевых компонентов. В рамках дипломного проектирования было рассмотрено несколько методов мониторинга:

- а) методы мониторинга основанные на сетевых компонентах. Такие методы основаны на мониторинге коммутационного оборудования;
- б) методы основанные не на сетевых компонентах. Подобные способы несколько урезаны в собственных возможностях, чем интегрированные в коммутационное оборудование, но при этом имеют и свои плюсы.

Методы мониторинга, основанные на сетевых компонентах – заданы в коммутационном оборудовании. Методы мониторинга, основанные на сетевых компонентах могут быть реализованы с помощью:

- мониторинга через протокол SNMP (Simple Network Management Protocol – простой протокол управления сетью) – данный протокол является распространенным протоколом, и имеет задачи управления сетевыми устройствами и получение информации об их работе. Мониторинг по протоколу SNMP осуществляется с помощью ПО установленного на АРМ СБ. Как правило, всё современное коммутационное оборудование обладает базой управляющей информации (MIB – Management Information Base). В этой базе содержится масса полезной информации о состоянии устройства: счетчики производительности, действующие процессы, значения сетевого трафика на интерфейсах и т.д. Каждая запись в базе сопровождается уникальным идентификатором OID (object identifier). Зная OID записи, в которой хранится интересующий параметр, можно настроить программу на его контроль. Программа по протоколу SNMP будет подключаться к устройству, по OID получать значение параметра и сравнивать его с заданным значением. В случае несоответствия параметра заданному значению, программа сигнализирует об этом;

– мониторинг с помощью RMON. Данный мониторинг имеет возможность объединять разные сетевые компоненты и системы, с помощью которых можно контролировать данные при осуществлении мониторинга. Отличительной чертой RMON от SNMP является то, что в RMON можно настроить параметры, которые будут осуществлять мониторинг коммутационного оборудования в соответствии с уровнями доступа. У RMON имеется несколько версий, таких как RMON1 и RMON2.

RMON может состоять из таких компонентов как:

- АРМ управления;
- агент.

Агент выступает в роли хранилища информации с сетевых компонентов. АРМ управления осуществляет обработку данных полученных на агентом;

– мониторинг с помощью syslog. Syslog – является стандартом отправки сообщений о происходящих в системе событиях (логов), использующийся в IP сетях. Сведения из системных сообщений можно использовать для мониторинга коммутационного оборудования. Syslogs поддерживается на различных устройствах, начиная от принтеров до маршрутизаторов и брандмауэров. Протокол syslog прост, при наступлении определенных событий, коммутационное оборудование посылает короткое текстовое сообщение, размером меньше 1024 байт получателю сообщения. Сообщения отправляются по UDP или TCP.

Методы, основанные не на сетевых компонентах, такие как:

- активный мониторинг;
- пассивный мониторинг;
- комбинированный мониторинг.

Активный мониторинг. Данный мониторинг работает на основе получения сведений от коммутационного оборудования, такими сведениями могут выступать задержка пакетов, потеря пакетов и т.п.

Основной командой при активном мониторинге является команда ping, на основе сведений полученных после выполнения данной команды можно сделать вывод о задержки пакетов, доставки пакетов, потери пакетов и т.п. Помимо команды ping, неплохой командой является команда traceroute, с помощью которой возможно определить топологию сети. Обе команды работают на основе отправки ICMP-пакетов от одного коммутационного оборудования к другому и анализа ответов. На рисунке 2.1 показан пример команды ping, которая посылает echo-запросы от источника к получателю и в обратном направлении.

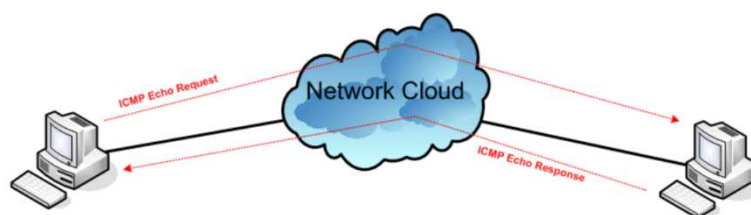


Рисунок 2.1 – Пример команды ping

Пассивный мониторинг. Пассивный мониторинг в отличие от активного мониторинга работает путем контроля одного коммутационного оборудования и собирает информацию только о нем. Тем самым контроль происходит немного лучше, чем при активном мониторинге. Контроль осуществляется только тогда, когда трафик передается по каналу передачи.

Пассивный мониторинг работает с такой информацией как количество переданных битов, информацию о переданных протоколах, время между получением и отправкой пакетов и т.п. Пассивный мониторинг может быть осуществлён, при помощи ПО, которое имеет возможность анализа пакетов.

Пассивный мониторинг является бюджетным вариантом в отличии от активного мониторинга. В пассивном мониторинге имеется главный недостаток, который заключается в том, что анализ пакетов может происходить не в реальном времени передачи или отправки данных пакетов, а только после осуществления данных действий.

Пассивный мониторинг может быть лучше активного в том, что не осуществляется внедрения в сеть и он остается незаметным.

Комбинированный мониторинг. Данный метод мониторинга использует хорошие стороны пассивного и активного мониторинга.

Не смотря на множество различных методов мониторинга, мониторинг сетевых компонентов может строиться на одном из следующих способов:

- проверка физической доступности оборудования (доступность может быть нарушена в результате отключения самого оборудования, либо отказе каналов связи). Как минимум, это означает проверку доступности по ICMP-протоколу (ping), причем желательно проверять не только факт наличия ответа, но и время прохождения сигнала, и количество потерянных запросов: аномальные значения этих величин, как правило, сигнализируют о серьезных проблемах в конфигурации оборудования. Некоторые из этих проблем легко отследить при помощи трассировки маршрута traceroute);
- проверка состояния (работоспособности) коммутационного оборудования;
- детальная проверка параметров коммутационного оборудования;
- проверка параметров, специфичных для сервисов и служб данного конкретного окружения.

Для разработки системы мониторинга сетевых компонентов, в ИСПДн имеется следующее коммутационное оборудование:

- коммутатор Hewlett Packard Enterprise 5120;
- коммутатор Hewlett Packard Enterprise 5130;
- коммутатор Cisco Catalyst 2960-s;
- криптошлюз ViPNet Coordinator HW1000 v2;
- точка доступа PicoStation 2HP;
- точка доступа NanoStation M5;
- межсетевой экран ССПТ-2.

Однако не каждое коммутационное оборудование имеет возможность совмещать разные методы и способы мониторинга.

Hewlett Packard Enterprise 5120. Данный коммутатор является коммутатором 2 уровня, поддерживающий статическую маршрутизацию и

списки ACL. Данный коммутатор подойдет как для малых, так и для больших сетей. Данный коммутатор обеспечивает хорошую работу за счет контроля качества обслуживания (QoS) это позволяет применять различные политики качества обслуживания. Является удобным при администрировании.

Функции управления коммутатором:

- IMC — Intelligent Management Center;
- интерфейс командной строки;
- веб-браузер;
- SNMP Manager.

Имеет возможность контроля состояния с помощью ICMP-ping, syslog и SNMP ловушек.

Hewlett Packard Enterprise 5130. Аналогичен Hewlett Packard Enterprise 5120, добавлена возможность RIP-маршрутизации уровня 3 и технология экономии электроэнергии Energy Efficient Ethernet. Помимо этого имеет расширенные функции качества обслуживания (QoS) и поддерживает гибкие методы проверки подлинности (802.1X, MAC и веб-аутентификация), повышающие безопасность системы и обеспечивающие аутентификацию приложений на основе политик.

Cisco Catalyst 2960-s. Данный коммутатор является лидером среди аналогичных продуктов. При использовании данного коммутатора можно смело надеяться на безопасность работы сети, в которой будет использовано данное оборудование. Данный коммутатор поддерживает подключение по Fast Ethernet и поддержку PoE.

Функции коммутаторов Cisco Catalyst серии 2960-S:

- порт каскадирования, поддерживающий технологии Ethernet 10 и 1 Гбит/с с помощью адаптера SFP+;
- поддержка протоколов snmp и syslog;
- поддержка USB-накопителей для резервного копирования и распространения файлов;

- возможность подключения настольных компьютеров к 24 портам Gigabit Ethernet;

- технология PoE+;
- широкий набор программных средств, для работы с коммутатором.

ViPNet Coordinator HW1000 v2. ViPNet Coordinator HW1000 — это криптошлюз. Данный криптошлюз имеет аппаратную платформу построенную на базе серверов компании «AquaServer». Данный криптошлюз надежно защищает информацию от НСД и подмены.

Он легко интегрируется в существующую инфраструктуру, надежно защищает передаваемую по каналам связи информацию от несанкционированного доступа и подмены.

Криптошлюз поддерживает следующие виды маршрутизации:

- статическая маршрутизация;
- видимость для NAT;
- поддержка DHCP;
- обладает функцией сервера доступа для удаленных VPN-клиентов с установленным ПО ViPNet Client;

- возможность в ручную регулировать излишнюю фрагментацию трафика;

- имеет возможность назначения виртуальных IP-адресов;
- поддерживает функцию NAT.

Криптошлюз поддерживает следующие виды фильтрации:

- контроль фрагментированных пакетов, предотвращение DoS-атак;

- пакетная фильтрация по IP-адресу источника;
- режим невидимости для внешних хостов;
- функция межсетевого экрана;
- антиспуфинг.

Настройка и управление:

- удаленная настройка базовых параметров через ViPNet Administrator;
- удаленная/локальная настройка через консоль ViPNet;
- поддержка SNMP ловушек;
- мониторинг текущего состояния ViPNet SGA 3;
- поддержка протокола syslog.

PicoStation 2HP. Является доступной точкой доступа и способна обеспечить интернетом небольшой офис или дом.

Данная точка доступа имеет всенаправленную антенну. Так же данная точка доступа обладает технологией электропитания от витой пары.

Точка доступа Ubiquiti PicoStation 2HP может работать при любой погоде, которую можно размещать как внутри помещения, так и снаружи. Точка доступа Ubiquiti PicoStation 2HP имеет пропускную способность канала 54 Мб/с, что достаточно, чтобы десяток абонентов комфортно работали с сетью.

Имеет возможность мониторинга с помощью протокола ICMP-ping.

NanoStation M5. Ubiquiti NanoStation M5 — является беспроводной точкой доступа, данная точка доступа имеет неплохие характеристики, что позволяет ей обслуживать большое количество потребителей.

Данная точка доступа способна обеспечивать интернетом клиентов в радиусе 5 км, и предоставить доступ к сетевым сервисам десяткам абонентам в офисе площадью до 300 кв.м. Точка доступа имеет хороший и наглядный интерфейс, что позволяет произвести настройку без каких либо затруднений.

Данная точка доступа может быть применена для различных сфер применения, таких как конференцсвязь, поддержка оборудования и т.д. Одним из плюсов можно выделить легкость монтажа данной точки доступа.

Точка доступа Ubiquiti NanoStation M5 имеет четырехсекционную антенну, которая позволяет расширить угол развертки до 43°.

Так же точка доступа имеет возможность настройки ширины канала передачи/приема в пределах от 10 до 40 МГц.

Ubiquiti NanoStation M5 работает в любую погоду, не боясь ни экстремально высоких температур, ни суровой зимы.

Межсетевой экран ССПТ-2. Данный межсетевой экран является новейшей разработкой, которая выполняет функции межсетевого экрана, но является «невидимым», что достигается путем отсутствия адресов на интерфейсах данного оборудования. Данная функция скрытности позволяет надежно защитить систему и сеть, куда будет установлен данный межсетевой экран.

Межсетевой экран ССПТ-2 предназначен для защиты систем, в которых обрабатывается информация с различными уровнями конфиденциальности. Помимо этого межсетевой экран применяется для разграничения ЛВС для обеспечения защиты информации от НСД с помощью:

- обладает функцией пакетной фильтрации;
- имеет возможность управления транспортными соединениями между узлами ЛВС;
- осуществляет контроль данных на прикладном уровне.

Межсетевой экран ССПТ-2 имеет такие функциональные характеристики как:

- возможность управления сессиями;
- возможность многоуровневой, многопротокольной скрытной пакетной фильтрации;
- режим работы с помощью NAT;
- возможность аутентификации входящих и исходящих запросов;
- способность блокировки сетевых flood-атак;
- выгрузка файлов регистрации событий и пакетов с использованием протоколов FTP и SYSLOG;

- защита канала управления на основе алгоритмов шифрования ГОСТ 28147-89 [6] и ГОСТ Р 34.10-2001 [7];
- способность контроля интерфейсов с помощью доверенных адресов;
- “зеркалирование” трафика;
- горячее резервирование при отказе оборудования.

Межсетевой экран ССПТ-2 обладает монитором централизованного управления, обеспечивает возможность одновременного управления несколькими ССПТ-2.

3 Использование протокола SNMP для анализа состояния коммутационного оборудования

В настоящее время для мониторинга состояния коммутационного оборудования используются приложения, такие как системы HP OpenView фирмы Hewlett-Packard, Microsoft System Center Operations Manager , 10 strike software и другие разнообразные средства мониторинга.

В основе этих средств лежит использование протокола SNMP (Simple Network Management Protocol). Протокол SNMP предназначен для сбора и передачи служебной информации (status information) между различными компьютерами.

SNMP (Simple Network Management Protocol), он является протоколом для сетевого управления. История создания данного протокола начинается с 1988 г., его создание было обусловлено тем, что было необходимо как-то управлять большим количеством сетевых устройств. С момента создания данного протокола, он набрал не малую популярность и стал как один из стандартов. После создания протокола, он неоднократно был переработан и были выпущены новые версии SNMPv1, SNMPv2 и SNMPv3.

SNMP — является протоколом из семейства TCP/IP . Его начало было положено сообществом интернета (Internet community), данное сообщество использовало данный протокол для контроля и устранения неполадок в маршрутизаторах. SNMP протокол позволяет контролировать и передавать информацию о состоянии:

- компьютеров, работающих под управлением Windows NT;
- серверов;
- маршрутизаторов и коммутаторов;
- терминалов;
- компьютеров, работающих под управлением Windows Server.

Сети которые управляются с помощью протокола SNMP обычно строятся из:

- управляемого устройства;

- агента — это ПО которое запускается на коммутационном оборудовании, которое необходимо контролировать;

- система сетевого управления — это ПО, взаимодействующие с менеджерами управления с целью поддержки единой структуры данных, отражающих состояние сети.

Управляемое устройство — это ПС с помощью которого реализован интерфейс управления сети. Управляемые устройства могут обмениваться информацией с менеджером. Управляемые устройства могут являться разными видами устройств: маршрутизаторы, серверы, коммутаторы и т. п.

Агентом называется программный модуль сетевого управления, установленный на коммутационном оборудовании. С помощью агента информация переводится в форму SNMP или наоборот.

В состав системы сетевого управления входит приложение, отслеживающее и контролирующее управляемые устройства. С помощью системы сетевого управления происходит обработка данных, необходимых для управления сетью.

Как правило, все современные управляемые сетевые устройства (рабочие станции, ноутбуки, коммутаторы, принтеры, роутеры, модемы, web-камеры и т.д.) обладают так называемой базой управляющей информации (MIB — Management Information Base). В этой базе содержится масса полезной информации о состоянии устройства: счетчики производительности, активные процессы, значения сетевого трафика на интерфейсах и т.д. В некоторых устройствах количество разнообразных записей в таких базах достигает десятков тысяч. Каждая запись в базе сопровождается уникальным идентификатором OID (object identifier). Зная OID записи, в которой хранится интересующий параметр, можно настроить программу на его контроль. Программа мониторинга сетевых компонентов по протоколу SNMP будет подключаться к устройству, по OID получать значение параметра и сравнивать его с заданным значением. В случае несоответствия параметра заданному значению, программа будет

сигнализировать об этом. Поэтому с помощью протокола SNMP можно производить мониторинг состояния коммутационного оборудования.

4 Выбор программного обеспечения для системы мониторинга

Не смотря на множество различных методов мониторинга, мониторинг сетевых компонентов непосредственно связан с программным обеспечением, которое имеет совместимость с операционной средой и коммутационным оборудованием. В ходе дипломного проектирования был рассмотрен ряд ПО для осуществления мониторинга:

а) сетевая программа от российского разработчика 10 Страйк: Мониторинг сети Pro. Данное ПО позволяет производить мониторинг:

1) мониторинг icmp(ping) (Программа периодически посылает пакеты удаленному хосту и ждет от него ответа в течение заданного времени. Если ответ приходит, программа сверяет время отклика с заданным значением и сообщает об этом администратору. В большинстве случаев, для того, что бы считать удаленный хост доступным, достаточно просто признака получения ответа. Однако в ряде ситуаций этого бывает не достаточно. Например, в сотовой связи, когда превышение значения времени отклика может сигнализировать о «забитости» канала или выходе из строя сетевого оборудования, как причина этого. Поэтому, зная статистику значений времени отклика можно проанализировать работу коммутационного и другого оборудования и вовремя принять решение о его замене или ремонте;

2) мониторинг коммутационного оборудования по протоколу SNMP. Программа по протоколу SNMP будет подключаться к устройству, по OID получать значение параметра и сравнивать его с заданным значением. В случае несоответствия параметра заданному значению, программа сигнализирует об этом;

3) мониторинг коммутационного оборудования по протоколу Syslog. Программа по протоколу Syslog будет получать системные сообщения от коммутационного оборудования;

б) Microsoft System Center Operations Manager – является системой мониторинга от Microsoft, осуществляет мониторинг с помощью протокола SNMP. Данное ПО работает под разными семействами ОС;

в) Zabbix – данное программное обеспечение имеет свободный доступ и осуществляет функции мониторинга коммутационного оборудования. Данное программное обеспечение состоит из следующих компонентов:

1) сервер мониторинга – осуществляет опрос коммутационного оборудования и сбор данных;

2) прокси – осуществляет сбор информации о производительности и доступности коммутационного оборудования;

3) агент – запускается на коммутационном оборудовании для контроля ресурсов и приложений;

4) веб-интерфейс – средство визуального представления Zabbix;

д) HP Open View – семейство программных продуктов компании Hewlett Packard по управлению системами и сетями связи. OpenView является всеобъемлющим решением по управлению ИТ - инфраструктурой предприятия любого размера и направления деятельности. Построено на основе модульной архитектуры. Осуществляет мониторинг и управление локальными вычислительными сетями, серверными платформами, приложениями, рабочими местами пользователей, организация диспетчерской службы, предоставление инструментария для выстраивания ИТ инфраструктуры согласно процессов ITIL/ITSM;

е) Nagios – программа с открытым кодом, предназначенная для мониторинга компьютерных систем и сетей. Она следит за указанными узлами и службами, и оповещает администратора в том случае, если какая-либо служба прекращает (или возобновляют) свою работу. Осуществляет мониторинг сетевых служб (SMTP, POP3, HTTP, NNTP, ICMP, SNMP),

мониторинг состояния серверов (загрузка процессора, использование диска, системные логи).

Так как в ТЗ на ВКР указывается на то, что программное обеспечение должно функционировать в ОС Microsoft Windows, были отброшены следующие программные продукты:

- Nagios;
- Zabbix.

Эти программные продукты работают с ОС Linux.

Из оставшихся программных продуктов таких как:

- HPe Open View;
- Microsoft System Center Operations Manager;
- 10 Страйк: Мониторинг сети Pro.

Можно отбросить первые 2, так как они имеют большую стоимость. Остается последний программный продукт, он имеет приемлемую стоимость, много функциональных возможностей и является российским продуктом, поэтому для системы мониторинга выбор останавливается на нем.

Выбранное ПО, «10 Страйк: Мониторинг сети Pro» состоит из:

- службы мониторинга;
- базы данных;
- графической консоли.

Основные функции ПО «10 Страйк: Мониторинг сети Pro»:

- мониторинг распределенных сетей;
- хранение результатов и настроек в единой SQL-СУБД;
- использование удаленных агентов на ПК;
- мониторинг по различным протоколам;
- управление через веб-интерфейс;
- просмотр графиков изменения контролируемых параметров;
- возможность мониторинга Syslog;

- возможность мониторинга SNMP Trap.

Состав программного обеспечения системы мониторинга приведен в приложении Г.

5 Требования к коммутационному оборудованию

Были разработаны требования к коммутаторам, которые приведены ниже.

Интерфейсы:

- количество портов доступа – не менее 24;
- интерфейсы доступа - RJ-45 10/100/1000 Base-T;
- uplink порты – не менее 4 фиксированных порта Gigabit Ethernet

SFP.

Коммутация:

- производительность коммутации – не менее 10 Гбит/с;
- размер буфера кадров – не менее 256 кБайт;
- размер таблицы MAC-адресов – не менее 8000.

Управление трафиком:

- поддержка протоколов группы SNMP;
- поддержка и тегирование VLAN: поддержка IEEE 802.1Q и 4,094

одновременных идентификаторов VLAN;

- отслеживание групповой адресации по протоколу IP;
- отслеживание сетевого трафика IGMP;
- отслеживание сетевого трафика MLD;
- очередь на основе приоритетов (SP);
- кольцевой список с весовыми коэффициентами (WRR);
- взвешенное произвольное раннее обнаружение (WRED).

Безопасность:

- поддержка Port security;
- ограничение количества MAC-адресов на порт;
- использование аппаратных высокоскоростных списков

управления доступом (ACL);

- поддержка GUI или MIB;
- поддержка SSL;

- поддержка DHCP;
- поддержка IP Source Guard;
- предотвращение ARP Spoofing;
- представление парольной информации в CLI и файле конфигурации в зашифрованном виде.

Управление:

- поддержка SNMP;
- не мене 2-х ipv6;
- IMC — Intelligent Management Center;
- интерфейс командной строки;
- веб-браузер;
- возможность сохранения файла конфигурации в текстовом виде, с последующим восстановлением полной конфигурации коммутатора при ее обнулении путем вставки данного текстового файла в окно терминала через буфер обмена;
- генерация Syslog сообщений и SNMP Traps при изменении состояния;
- SNMP Manager;
- поддержка нескольких файлов конфигурации;
- позволяет контролировать вход и выход порта;
- поддержка ping (IPv6) и traceroute (IPv6);
- поддержка TFTP/FTP для загрузки файлов ПО;
- определяет MAC-адрес другого хоста IP в той же подсети; поддерживает статические ARP. ARP позволяет обнаруживать дублированные IP-адреса;
- поддержка DHCP;
- протокол дейтаграмм пользователя (UDP);
- возможность просмотра серийного номера коммутатора и информации о sfr модуле (через cli и snmp).

Поддержка списка контроля доступа (ACL):

- поддержка не менее 100 ACL разного типа;
- поддержка ACL на основе портов;
- поддержка ACL на основе MAC-адресов (запрещенные MAC-адреса не должны изучаться);
- поддержка ACL на основе IP адресов;
- поддержка ACL на основе портов TCP/UDP;
- поддержка ACL на основе 802.1q.

Качество обслуживания:

- управление Broadcast позволяет ограничивать скорость широковещательного трафика, чтобы сократить нежелательного сетевого трафика широковещательной рассылки;
- расширенный классификатор на основе QoS, классифицирует трафик с использованием нескольких критериев соответствия, основанные на уровнях 2, 3 и 4;
- уровня приоритета и ограничение скорости для выбранного трафика на порт, VLAN, или всего коммутатора;
- поддержка дисциплин обслуживания очередей SP, WRR, SP+WRR.

Групповые рассылки:

- поддержка IGMP Snooping;
- интернет-протокол управления группы (IGMP) использует Any-Source Multicast (ASM) или Source-Specific Multicast (SSM) для управления многоадресной сетей IPv6.

Поддержка IPv6:

- поддержка IPv6 для управления;
- поддержка IPv6 ACL;
- поддержка IPv6 ICMP;
- поддержка IPv6 в полях DHCP.

Физические и электрические характеристики:

- диапазон рабочих температур от 0 до 45 С⁰;
- потребляемая мощность 650 Вт (максимум);
- тепловыделение 3599,66 кДж/ч ;
- влажность при эксплуатации от 10 до 90% без конденсации;
- напряжение на входе от 100 до 240 переменного тока, номинальное значение (от 90 до 264 В переменного тока, максимум) (в зависимости от выбранного источника питания);
- память и процессор система хранения: 128 Мбайт флеш-памяти, 128 Мбайт SDRAM; емкость буфера пакетов: 0,5 Мбайт.

Требования к межсетевому экрану ССПТ-2.

Характеристики межсетевого экрана ССПТ-2:

- должно быть 4 фильтрующих интерфейса;
- возможные типы интерфейса - Ethernet 10BASE-T/100BASE-TX/1000BASE TX/10000BASE TX;
- скорость, 10000 мбит/сек;
- количество управляющих интерфейсов - 1;
- возможные типы интерфейса - Ethernet 10BASE-T/100BASE-TX/1000BASE TX;
- тип корпуса – для стоечного исполнения;
- габаритные размеры - 25x156x225 мм.

Функциональные характеристики межсетевого экрана ССПТ-2:

- возможность управления сессиями;
- возможность многоуровневой, многопротокольной скрытной пакетной фильтрации;
- режим работы с помощью NAT;
- возможность аутентификации входящих и исходящих запросов;
- способность блокировки сетевых flood-атак;

- выгрузка файлов регистрации событий и пакетов с использованием протоколов FTP и SYSLOG;

- защита канала управления;

- способность контроля интерфейсов с помощью доверенных адресов;

- “зеркалирование” трафика;

- горячее резервирование при отказе оборудования.

Режим скрытной фильтрации для систем защиты информации, в данном режиме межсетевой экран ССПТ-2:

- не изменяет параметров проходящих через него пакетов;

- не подвержен воздействию компьютерных атак;

- позволяет выявлять аномальные или неавторизованные воздействия.

Сертификат:

- сертификат ФСБ РФ;

- сертификат ФСТЭК.

Физические и электрические характеристики:

- диапазон рабочих температур от 0 до 45 С⁰;

- потребляемая мощность 650 Вт (максимум);

- влажность при эксплуатации от 10 до 90% без конденсации.

Исходя из требований к коммутационному оборудованию, для создания системы мониторинга сетевых компонентов рассматриваемых в дипломной работе:

- коммутатор Hewlett Packard Enterprise 5120;

- коммутатор Hewlett Packard Enterprise 5130;

- коммутатор Cisco Catalyst 2960-s;

- криптошлюз ViPNet Coordinator HW1000 v2;

- точка доступа PicoStation 2HP;

- точка доступа NanoStation M5;

- межсетевой экран ССПТ-2.

Для примера было выбрано следующие коммутационное оборудование:

- коммутатор Cisco Catalyst 2960-s;
- межсетевой экран ССПТ-2.

6 Требования к характеристикам ПЭВМ для системы мониторинга

АРМ на базе ПЭВМ для системы мониторинга должен состоять из:

- системного блока;
- монитора;
- сети.

Требования к АРМ на без ПЭВМ приведены в таблице 1.

Таблица 1 – Требования к АРМ на базе ПЭВМ для системы мониторинга

№	Наименование	Требование
1	Процессор	Не менее 4-х ядер с частотой не менее 3 GHz или 2-ядерный с частотой не менее 4 GHz.
2	Оперативная память	Не мене 4 Гб.
3	Монитор	1. Разрешение экрана: не менее 1280x800. 2. Геометрия экрана: для удобства работы рекомендуется 16:9. 3. Диагональ: не менее 15`` (для продуктивной работы с графиками и большими объемами данных рекомендуется от 19``).
4	Операционная система	Windows 2000 Professional (SP4), или Windows XP Professional (SP2), или Windows Vista, или Windows 7, или Windows 8

Продолжение таблицы 1

№	Наименование	Требование
5	Дополнительное общесистемное ПО	1. Один из допустимых интернет-браузеров: – Internet Explorer версии 9.0 или выше; 2. Microsoft Office версии 2000 или выше; 3. Adobe Acrobat Reader версии 9 или выше; 4. Adobe Flash Player версии 10 или выше 5. 10 Страйк: Мониторинг Сети Pro версии 4.6 или выше
6	Подключение к сети	Скорость соединения с данного АРМ: – минимальная: 600 Кбит/с; – рекомендуемая: 1 Мбит/с и выше.
7	Дополнительные требования	1. Должна обеспечиваться антивирусная защита АРМ. 2. Должна обеспечиваться защита АРМ от несанкционированного доступа.

7 Разработка перечня контролируемых событий на коммутационном оборудовании

Одной из важных функций мониторинга является контроль событий. Коммутационное оборудование совместно с программным обеспечением для системы мониторинга имеет возможность отслеживать события, производить контроль событий на коммутационном оборудовании. Происходящие события фиксируются и сигнализируют о той или иной угрозе информационной безопасности. Для коммутационного оборудования выбранного на этапе 2 дипломной работы и программного обеспечения выбранного на этапе 4 дипломной работы, разработан перечень контролируемых событий. Перечень контролируемых событий был разработан с учетом возможностей мониторинга коммутационного оборудования.

Перечень контролируемых событий:

- работоспособность коммутационного оборудования;
- несанкционированное подключение к порту;
- мониторинг используемых портов;
- мониторинг не используемых портов;
- удаленное подключение администратора;
- события ACL;
- выборочная загрузка портов.

Таким образом система мониторинга сетевых компонентов будет иметь функции согласно перечня контролируемых событий.

8 Разработка типовых конфигураций файлов для коммутационного оборудования, используемого в ИСПДн

Для того, чтобы коммутационное оборудование, совместно с программным обеспечением для системы мониторинга сетевых компонентов функционировало, произведена настройка коммутационного оборудования для контроля событий, согласно перечню контролируемых событий.

На коммутаторе cisco 2960-s, для контроля событий, согласно перечню контролируемых событий, были произведены следующие настройки:

- установка пароля для входа в управляющий режим коммутатора;
- установка пароля для входа по telnet;
- установка шифрования пароля;
- установка имени коммутатора;
- установка ip адреса и маски коммутатора;
- установка подсети коммутатора;
- добавление ACL;
- включение сбора информации по протоколу SNMP;
- включение сбора информации по протоколу syslog.

Файл конфигураций, с пояснениями настройки для коммутатора cisco 2960-s, представлен в приложении Д.

На межсетевом экране ССПТ-2, для контроля событий, согласно перечню контролируемых событий, были произведены следующие настройки:

- установка ip адреса и маски меж сетевого экрана;
- установка регистрации пакетов;
- установка выгрузки системных сообщений по протоколу syslog;
- установка ip адреса сервера приема syslog сообщений.

Файл конфигураций, с пояснениями настройки для меж сетевого экрана ССПТ-2, представлен в приложении Е.

9 Разработка конфигурации или настройка программного обеспечения используемого для системы мониторинга

Для системы мониторинга сетевых компонентов было настроено программное обеспечение 10 Страйк мониторинг сети Pro. Описание порядка настройки приведены ниже. Так же порядок настройки приведен в приложении Ж.

Мониторинг сетевых компонентов, это обмен информацией программного обеспечение 10 Страйк мониторинг сети Pro с коммутационным оборудование. Для наглядности информационного обмена при мониторинге сетевых компонентов приведена структура информационного обмена при мониторинге сетевых компонентов.

Структура информационного обмена при мониторинге сетевых компонентов приведена в приложении И.

1 шаг. Приобретен лицензионный программный продукт 10 Страйк: Мониторинг сети Pro у официального поставщика 10-Strike Software.

2 шаг. Вставлен установочный диск с ПО 10 Страйк: Мониторинг сети Pro в оптический привод компьютера.

3 шаг. Запущен установочный файл ПО 10 Страйк: Мониторинг сети Pro с диска.

4 шаг. В мастере установки ПО прочтено лицензионное соглашение и приняты условия соглашения, показано на рисунке 9.1. Во вкладке выбор компонентов выбрана полная установка, после чего нажата кнопка «Готово», показано на рисунке 9.2.

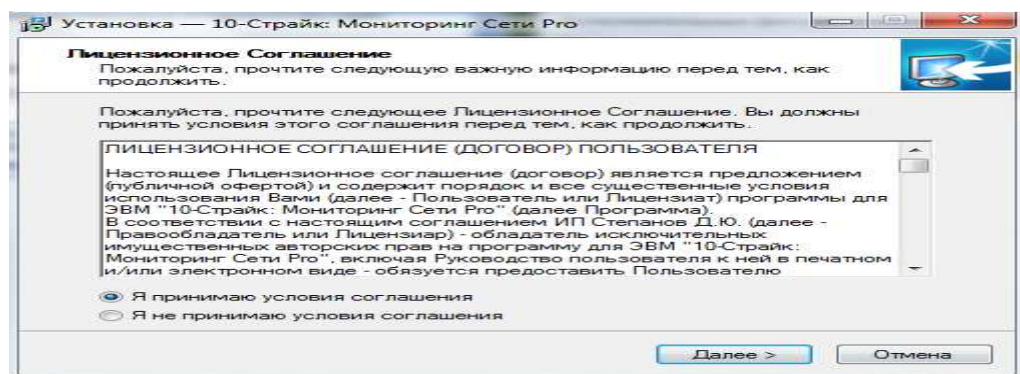


Рисунок 9.1 –Лицензионное соглашение

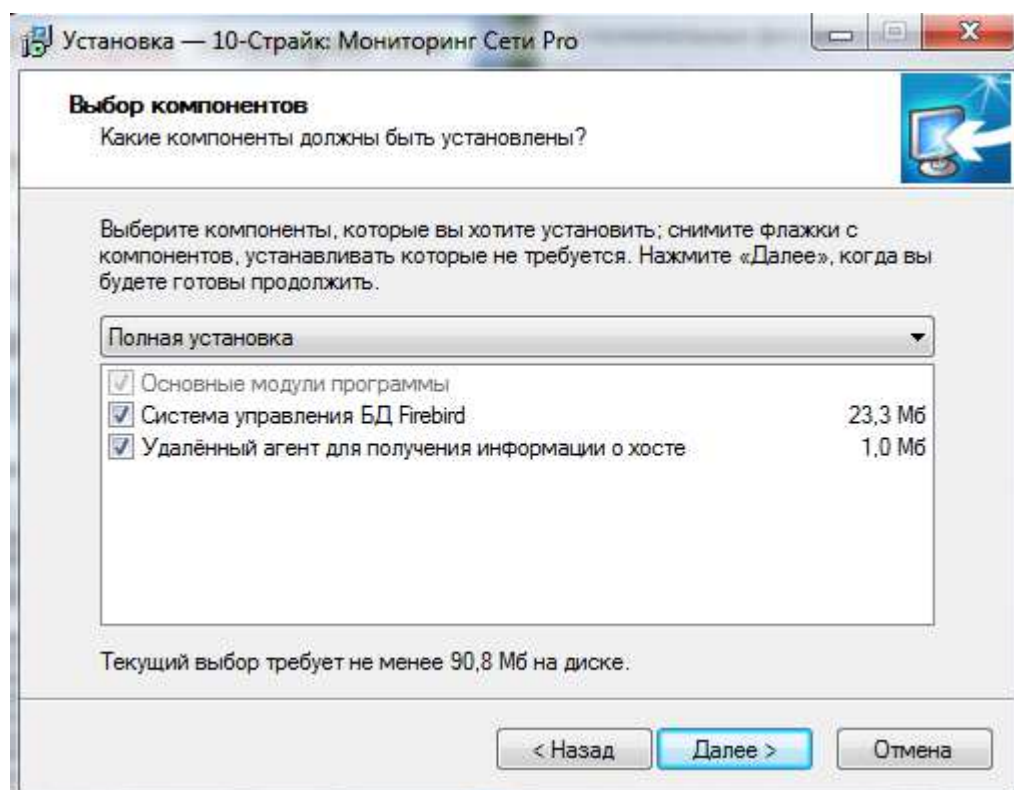


Рисунок 9.2 – Выбор компонентов

5 шаг. После завершения установки ПО на компьютер, на рабочем столе появился ярлык, кликнув два раза по ярлыку установленного ПО, произведен вход в программу.

6 шаг. При запуске программы, в диалоговом окне, нажата кнопка «У меня есть ключ», введен ключ и нажата кнопка «ОК», ПО зарегистрировано.

7 шаг. После запуска программы выбрана вкладка «Главная» и на вкладке выбрано «Сканировать сеть» путем нажатия на него курсором мыши. Главное меню программы показано на рисунке 9.3.

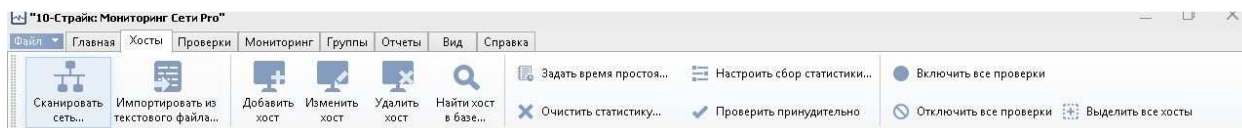


Рисунок 9.3 – Главное меню программы

8 шаг. После нажатия появилось диалоговое окно «Мастер сканирования сети» в нем задан диапазон IP адресов для сканирования, заданы способы и параметры сканирования и нажата кнопка «Далее». Демонстрация 8 шага показана на рисунке 9.4.

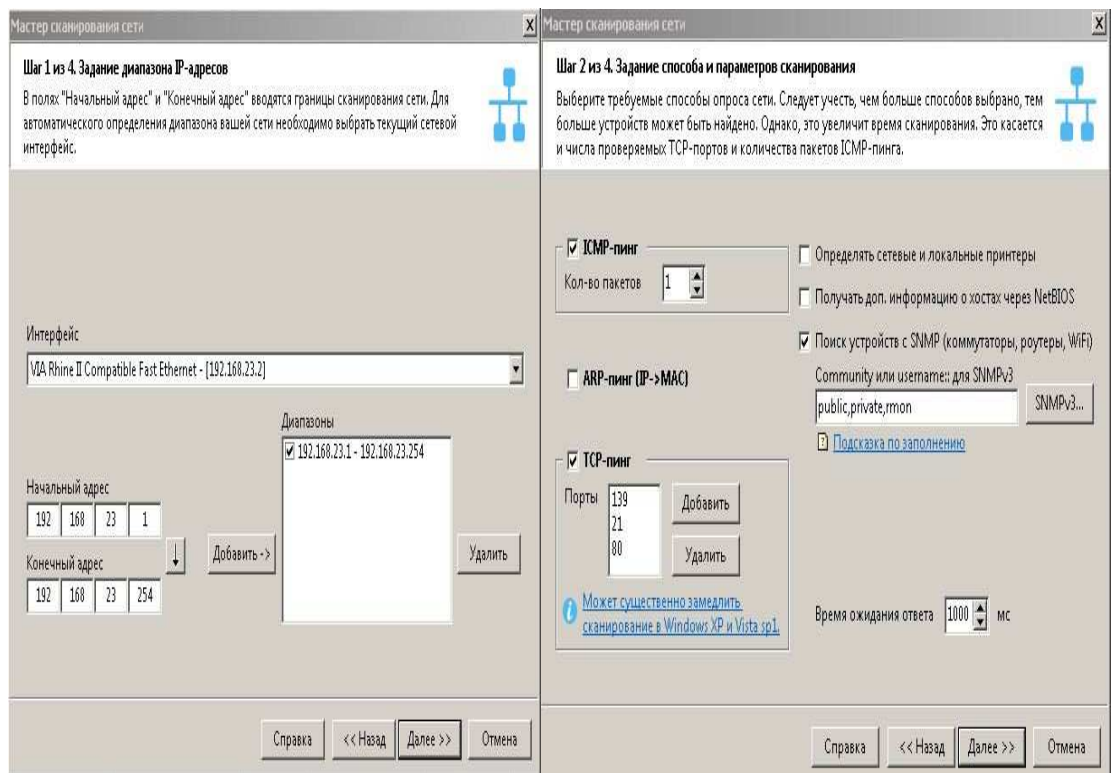


Рисунок 9.4 - Демонстрация шага 8

9 шаг. После обнаружения IP Адресов, в выпадающем окне выбраны «Хосты», IP адреса помещены в список хостов и нажата кнопка «Готово». Добавленный хост появился в левом столбце окна программы, под вкладкой хосты. Демонстрация шага 9 показана на рисунке 9.5.

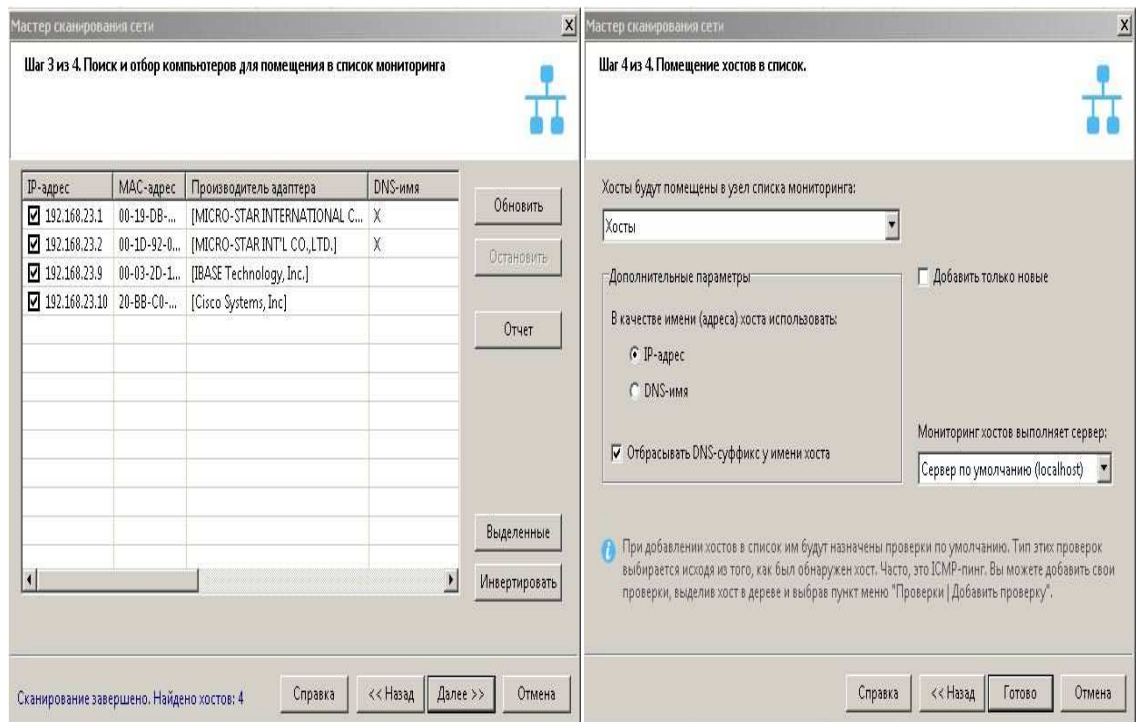


Рисунок 9.5 - Демонстрация шага 9

10 шаг. Осуществлен переход на вкладку главного меню «Проверки» и выбрана вкладка «Добавить проверку» нажав на нее курсором мыши. Демонстрация шага 10 показана на рисунке 9.6.

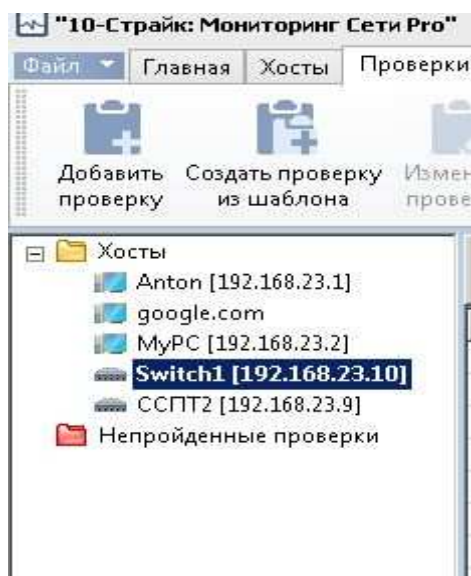


Рисунок 9.6 - Демонстрация шага 10

11 шаг. Появился помощник для создания проверки, для начала в нем, выбран тип и параметры проверки и нажата кнопка «Далее». Демонстрация шага 11 показана на рисунке 9.7.

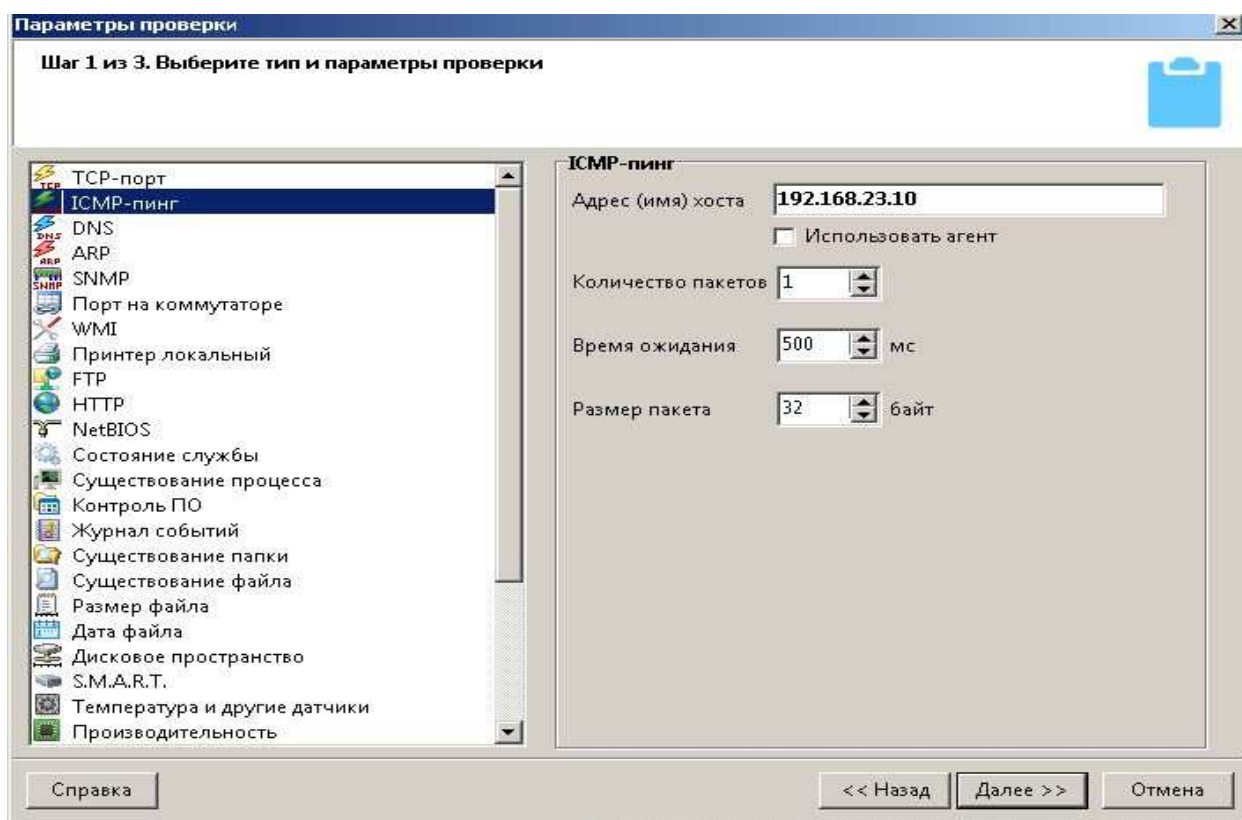


Рисунок 9.7 – Демонстрация шага 11

12 шаг. При необходимости можно задать зависимости проверок и другие параметры и нажать кнопку «Далее». Демонстрация шага 12 показана на рисунке 9.8.

Рисунок 9.8 – Демонстрация шага 12

13 шаг. Заданы действия, которые будут выполняться при соответствующих результатах проверки и нажата кнопка «Готово». Демонстрация шага 13 показана на рисунке 9.9.

Рисунок 9.9 – Демонстрация шага 13

После 13 шага появилась добавленная проверка ICMP - ping, которая представлена на рисунке 9.10.

Отображаемо...	Имя или адрес хоста...	Тип проверки	Состояние	Статус	Время отклика	Значение параметра:
Switch1	192.168.23.10	ICMP-пинг	Включена	Успешно завершила...	3 мс	-
Switch1	192.168.23.10	SNMP	Включена	Успешно завершила...	15 мс	-
Switch1	192.168.23.10	SNMP	Включена	Не прошла	-	1

Хост: 192.168.23.10
 Время смены статуса: 11.11.2016 13:35:10
Действия:

Проверка: ICMP-пинг
 Интервал проверки (сек.): 120
Действия:

Описание:
 Последнее сообщение: ICMP-пинг: ответ получен. Время отклика: 3 мс

Легенда:
 - отключена
- прошла
- не прошла
- не прошла по зависимости

Информация
 Время отклика, за последний час
Время отклика, за период
Время простоя, за период
Отчёт об авариях

Рисунок 9.10 – Добавленная проверка ICMP – ping

Так же можно посмотреть график времени отклика за последнее время, для этого выбрана внизу экрана вкладка «Время отклика». График времени отклика показан на рисунке 9.11.



Рисунок 9.11 – График времени отклика

14 шаг. Необходимо ли добавить еще проверку? Если да, необходимо, то нужно перейти к шагу 10. Если нет, то продолжить выполнять следующий шаг.

15 шаг. Осуществлен переход на вкладку главного меню «Мониторинг» и выбрана вкладка «Мониторинг Syslog» нажав на нее курсором мыши. Демонстрация шага 15 показана на рисунке 9.12.

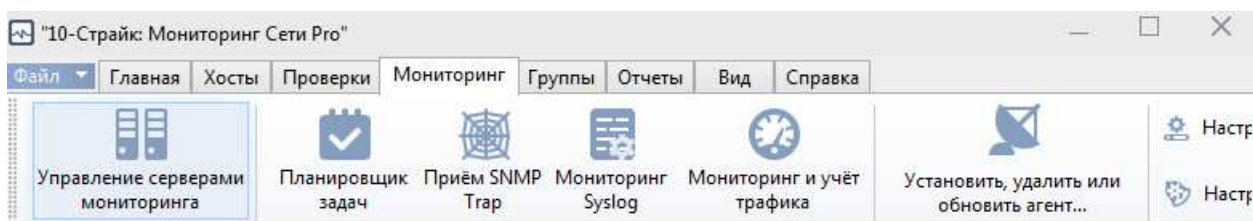


Рисунок 9.12 – Демонстрация шага 15

16 шаг. После появления диалогового окна «Мониторинг Syslog» была нажата кнопка «Включить прием записей Syslog», выбрано галочкой «Принимать все записи». Демонстрация шага 16 показана на рисунке 9.14.

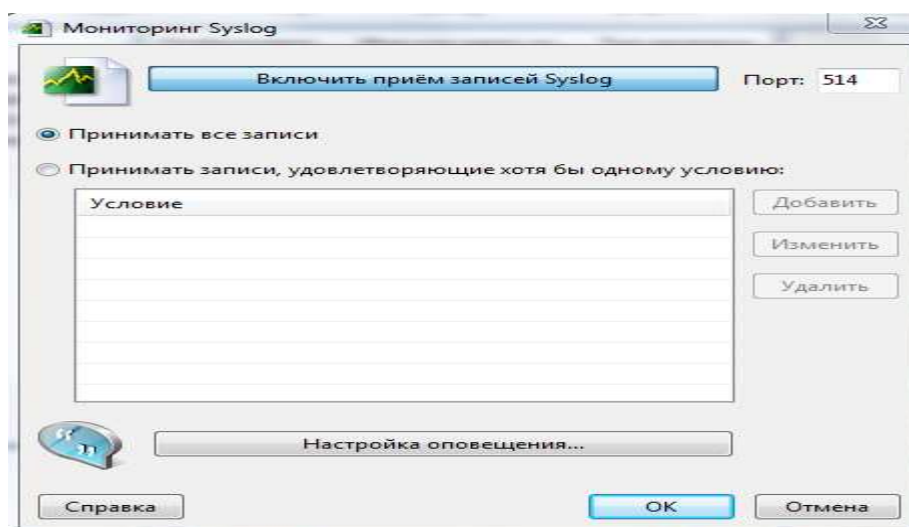


Рисунок 9.14 – Демонстрация шага 16

17 шаг. В диалоговом окне «Мониторинг Syslog» нажата кнопка «Настройка оповещения», после появления диалогового окна «Параметры оповещения», выбрана вкладка «Сообщения» и поставлена галочка «Выдать сообщение на экран этого компьютера». Демонстрация шага 17 показана на рисунке 9.15.

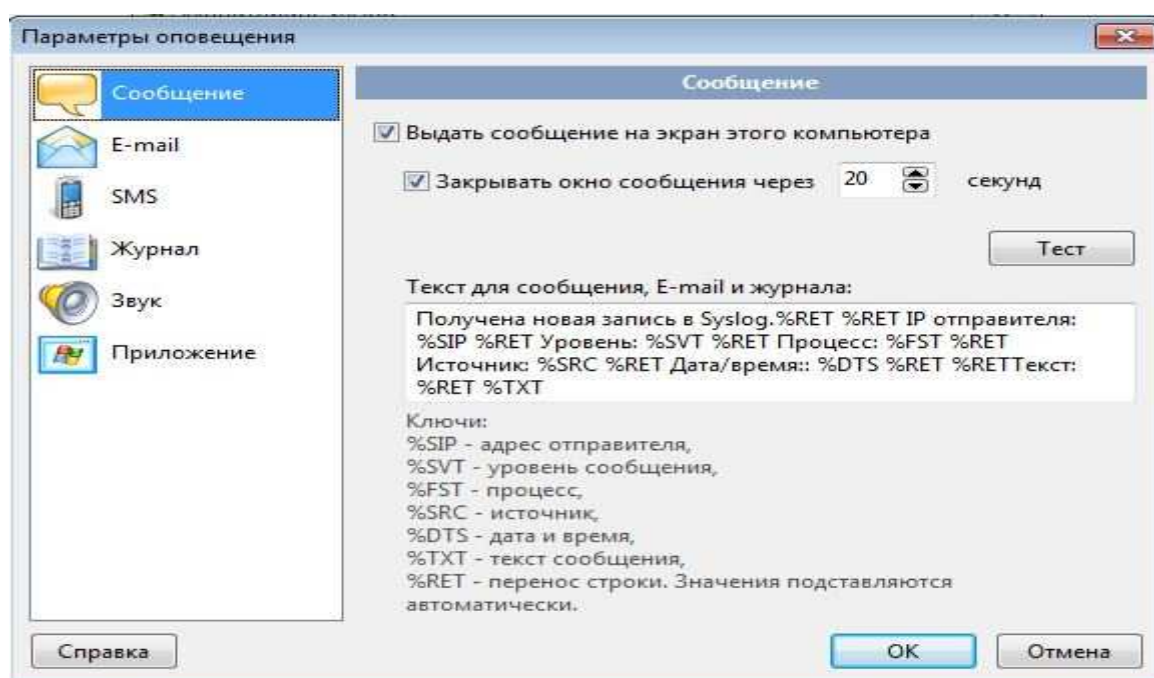


Рисунок 9.15 – Демонстрация шага 17

18 шаг. В диалоговом окне «Мониторинг Syslog» нажата кнопка «Настройка оповещения», после появления диалогового окна «Параметры оповещения», выбрана вкладка «Журнал» и поставлена галочка «Записать в журнал программы» и «Отправить запись в Syslog». Демонстрация шага 18 показана на рисунке 9.16.

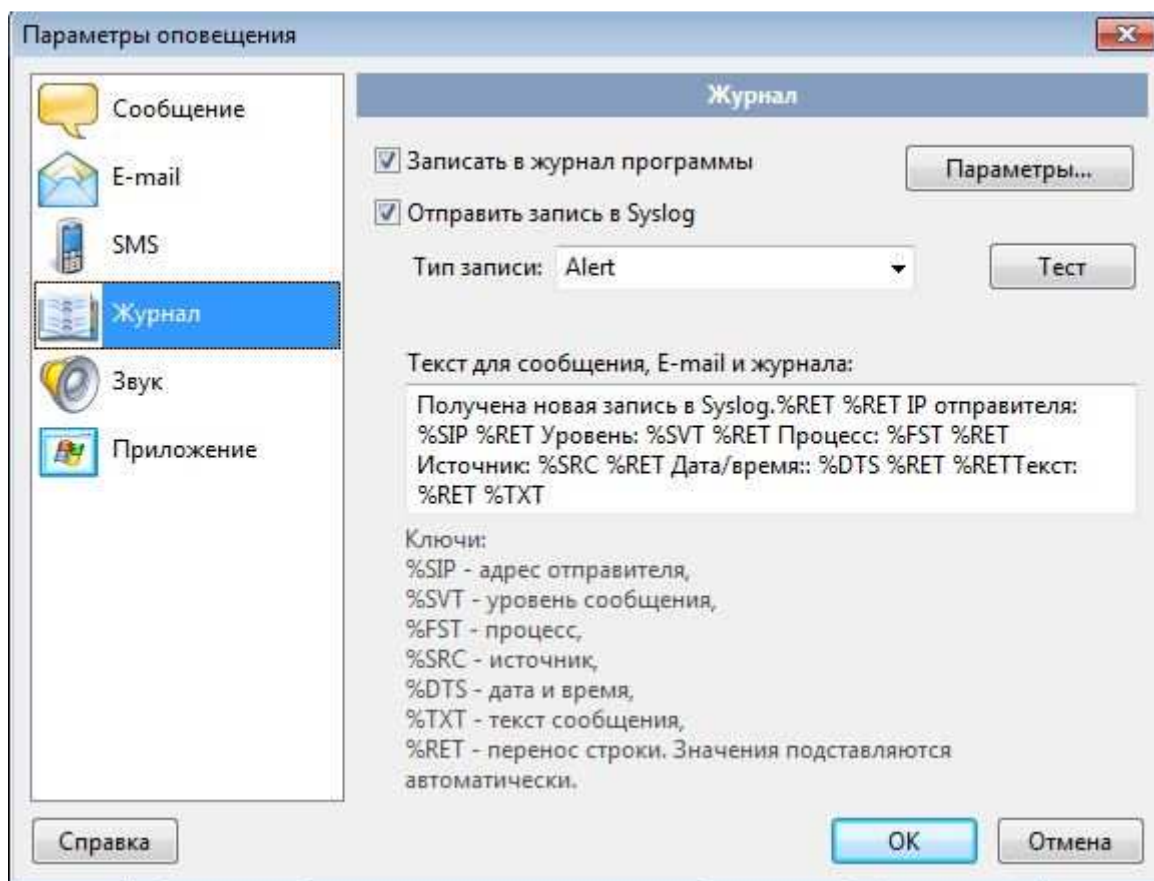


Рисунок 9.16 – Демонстрация шага 18

19 шаг. Осуществлен переход на вкладку главного меню «Мониторинг» и выбрана вкладка «Приём SNMP Trap» нажав на нее курсором мыши. Демонстрация шага 19 показана на рисунке 9.17.

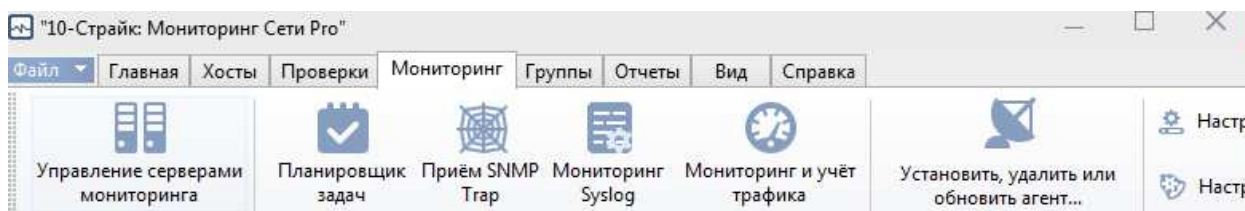


Рисунок 9.17 – Демонстрация шага 19

20 шаг. После появления диалогового окна «Ловушка SNMP» нажата кнопка «Включить прием сообщений от SNMP-устройств», выбрано

галочкой «Принимать все сообщения от SNMP-устройств». Демонстрация шага 20 показана на рисунке 9.18.

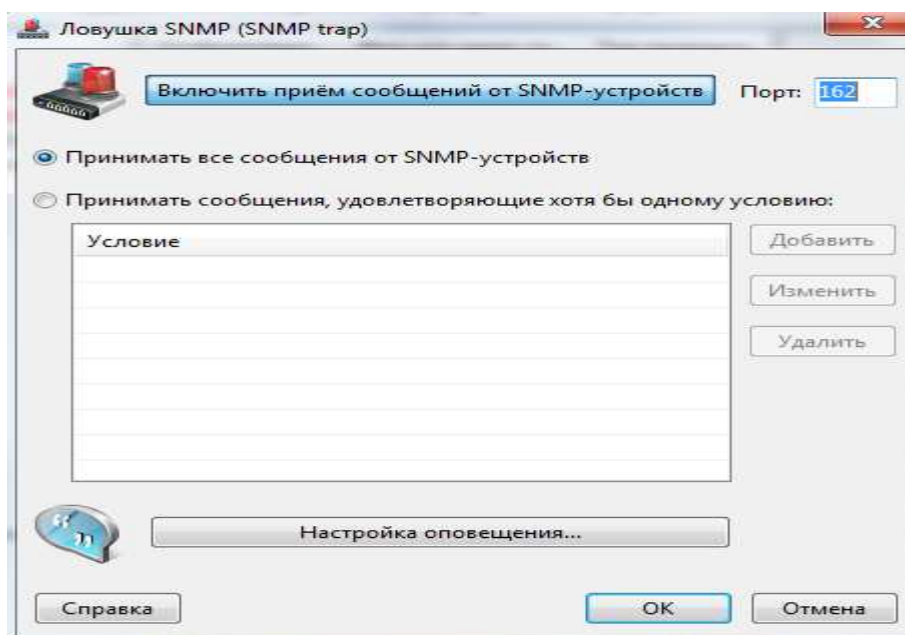


Рисунок 9.18 – Демонстрация шага 20

21 шаг. В диалоговом окне «Ловушка SNMP» нажата кнопка «Настройка оповещения», после появления диалогового окна «Параметры оповещения», выбрана вкладка «Сообщения» и поставлена галочка «Выдать сообщение на экран этого компьютера». Демонстрация шага 21 показана на рисунке 9.19.

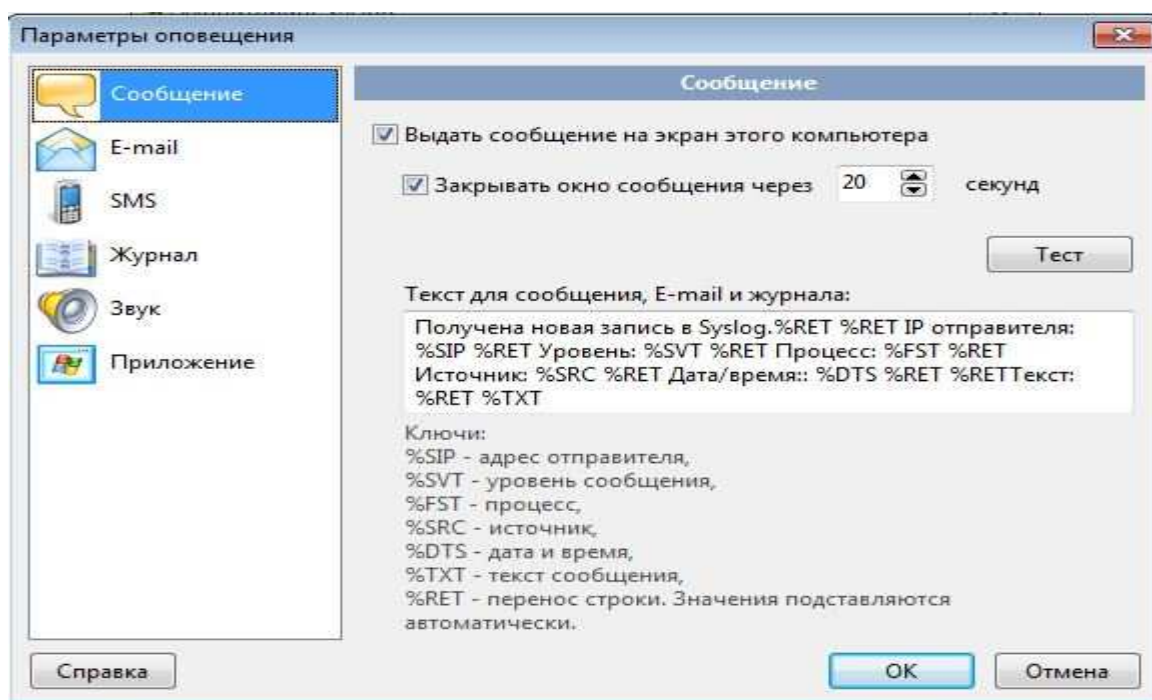


Рисунок 9.19 – Демонстрация шага 21

Шаг 22. В диалоговом окне «Ловушка SNMP» нажата кнопка «Настройка оповещения», после появления диалогового окна «Параметры оповещения», выбрана вкладка «Журнал» и поставлена галочка «Записать в журнал программы». Демонстрация шага 22 показана на рисунке 9.20.

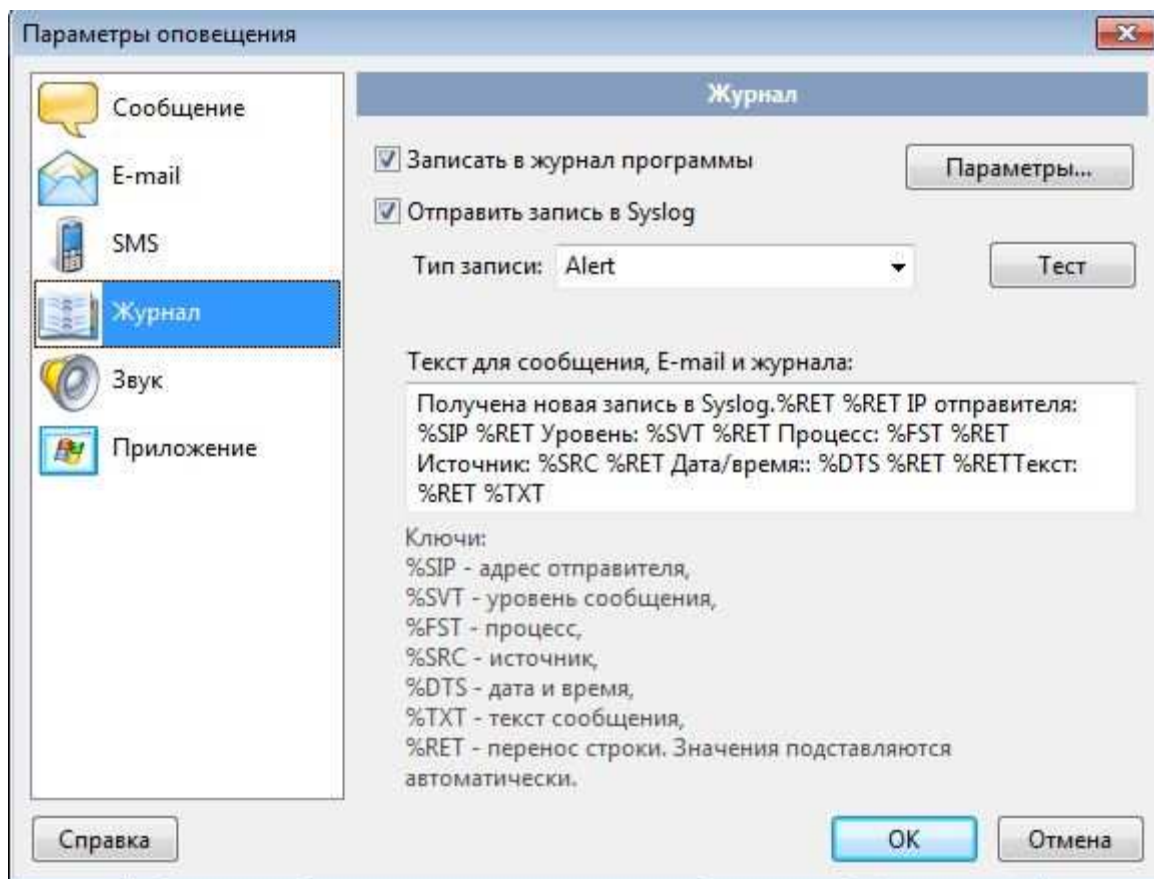


Рисунок 9.20 – Демонстрация шага 22

Так как система мониторинга сетевых компонентов необходима для контроля событий на коммутационном оборудовании. Были настроены проверки согласно перечню контролируемых событий.

Перечень контролируемых событий:

- работоспособность коммутационного оборудования;
- несанкционированное подключение к порту;
- мониторинг используемых портов;
- мониторинг не используемых портов;
- удаленное подключение администратора;
- события ACL;
- выборочная загрузка портов.

Таким образом система мониторинга сетевых компонентов имеет функции согласно перечня контролируемых событий.

Для функции проверки работоспособности коммутационного оборудования настроена проверка по ICMP – ping. Описание настройки данной проверки приведено ниже.

Для добавления данной проверки выбран хост курсором мыши и в главном меню программы выбрана вкладка «проверки» и нажата кнопка «добавить проверку». Добавление новой проверки показано на рисунке 9.21.

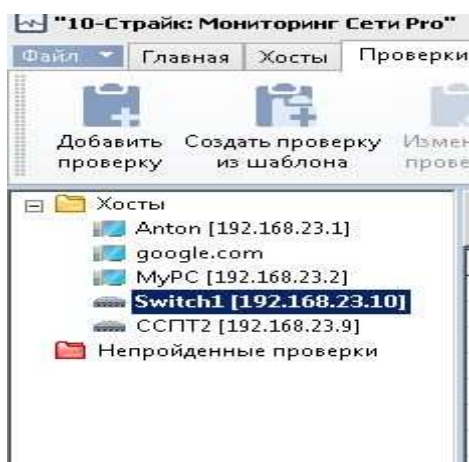


Рисунок 9.21 – Добавление новой проверки

Далее после открытия диалогового окна «Мастер проверок» выбран тип и параметры проверки, в данном случае это проверка по ICMP – ping. Добавление типа и параметра проверки показано на рисунке 9.22.

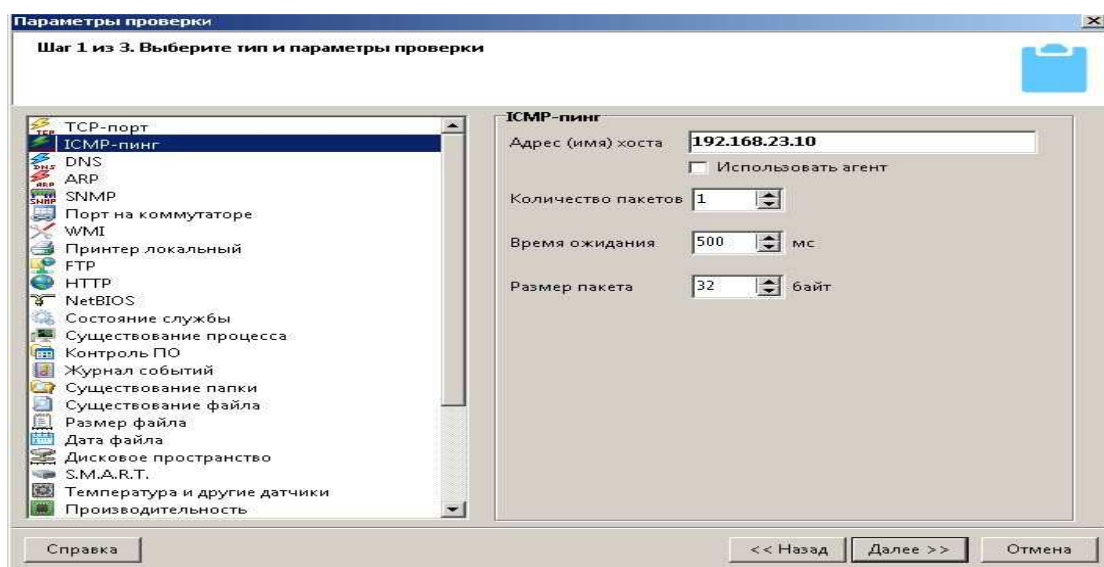
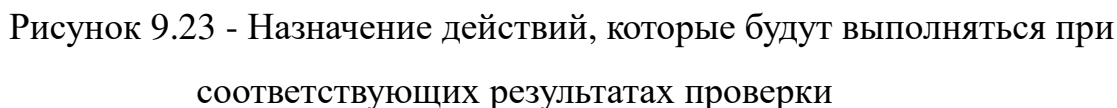


Рисунок 9.22 – Добавление типа и параметра проверки

Далее заданы действия, которые будут выполняться при соответствующих результатах проверки. Это выдача сообщения на экран, если проверка прошла и выдача сообщения на экран, если проверка не прошла. Назначение действий, которые будут выполняться при соответствующих результатах проверки показаны на рисунке 9.23.

[illegible]

66

В случае если коммутационное оборудование отключиться, то проверка не пройдет.

Настройка проверки по ICMP – ping для разного коммутационного оборудования будет одинаковой, отличаться будет только IP адрес хоста (коммутационного оборудования), на котором нужно сделать данную проверку.

Для функции проверки используемых портов на коммутационном оборудовании cisco 2960s настроена проверка по SNMP протоколу.

Для добавления данной проверки выбран хост курсором мыши и в главном меню программы выбрана вкладка «проверки» и нажата кнопка «добавить проверку». Добавление новой проверки показано на рисунке 9.25.

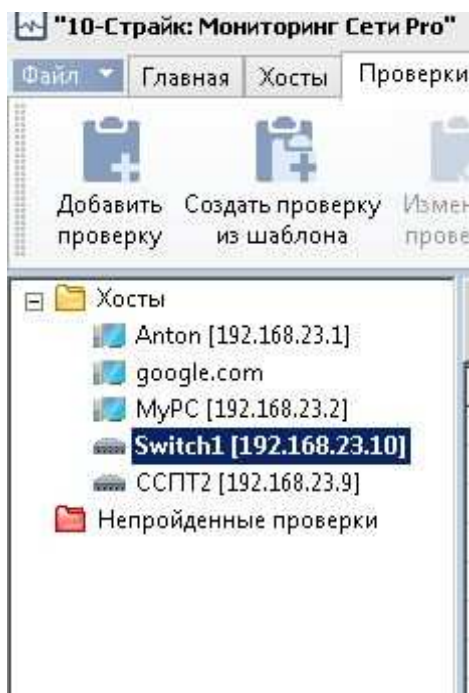


Рисунок 9.25 – Добавление новой проверки

Далее после открытия диалогового окна «Мастер проверок» выбран тип и параметры проверки в данном случае это проверка по SNMP. Для проверки работоспособности порта загружены mib файлы коммутатора cisco 2960s в корень установленного ПО в папку mibs. После чего открыт mib браузер в ПО и выбран OID который отвечает за состояние порта в данном случае это ifOperStatus. Выбор OID в mib браузере показан на рисунке 9.26.

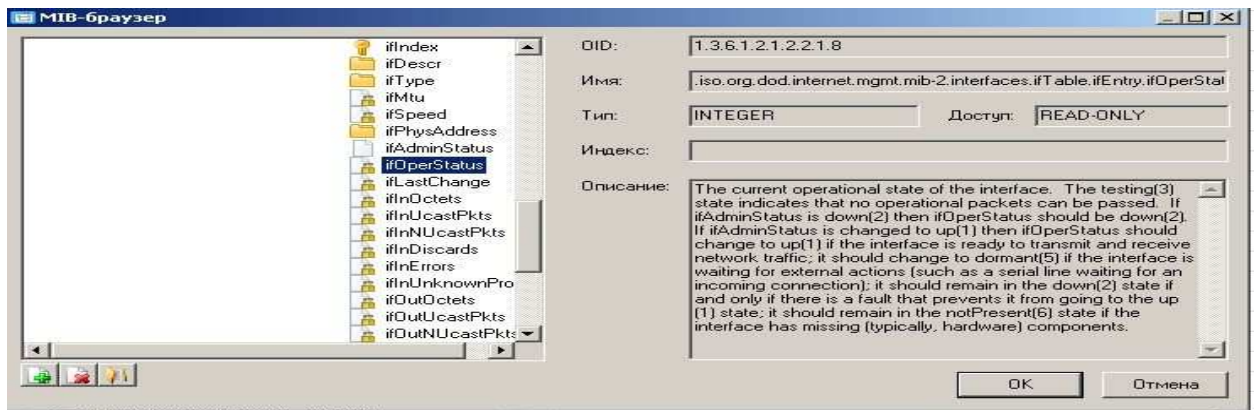


Рисунок 9.26 - Выбор OID в mib браузере

После выбора OID нажата кнопка «Ок». В окне выбора типа и параметров проверки, в строке OID появился выбранный OID ifOperStatus, для проверки конкретного порта, для примера это будет первый порт, в конце OID дописано значение 10101. Значение 10101 дописывается, потому что это условное обозначение 101XX, где 101 это обозначение гигабитных коммутаторов, а XX это номер порта. Помимо всего этого выбрана версия протокола SNMP, в данном случае 2с и имя «community myRO», которое было задано в конфигурации коммутатора на этапе 8 дипломного проектирования. Заданы условие проверки, проверка прошла если, нажата кнопка «получить» и так как первый порт имеет подключение, то в соответствии с описанием OID ifOperStatus, показанным на рисунке 9.26, получено значение равное 1. Настройка SNMP для OID ifOperStatus представленная на рисунке 9.27.

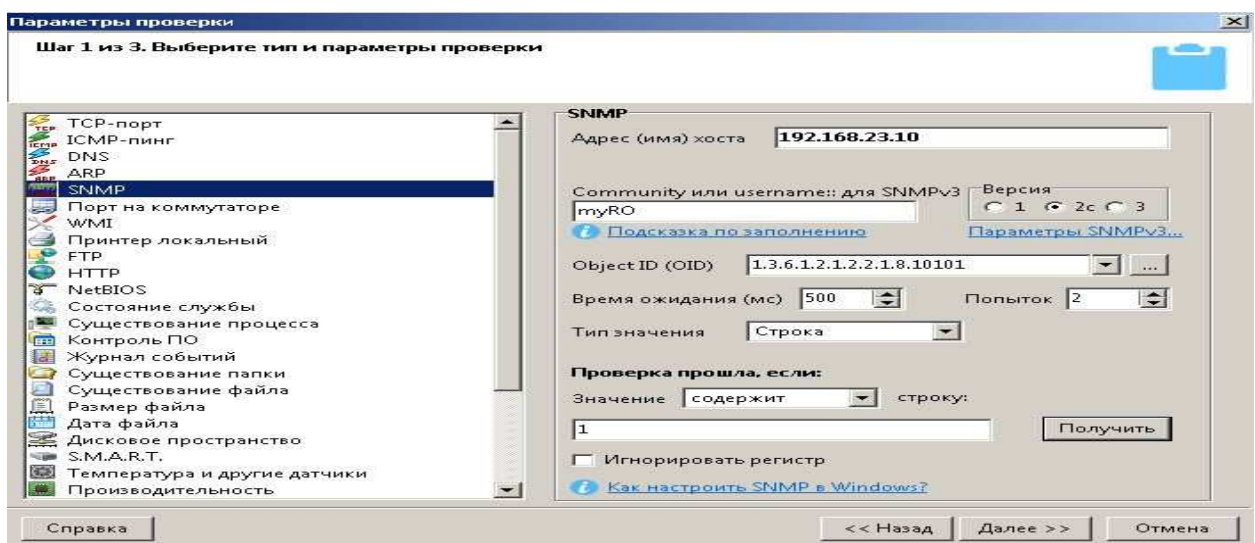


Рисунок 9.27 - Настройка SNMP для OID ifOperStatus

Для функции проверки используемых портов на межсетевом экране ССПТ-2 настроена проверка по Syslog.

В случае подключения к порту eth0 меж сетевого экрана ССПТ-2, будет выдано системное сообщение «FNPSH-I-3027-Фильтрующий интерфейс включен (eth0)». Данное сообщение получает программа мониторинга 10 Страйк: Мониторинг сети Pro, после настройки приема Syslog сообщений. Настройка получения Syslog сообщений от меж сетевого экрана ССПТ-2 проведена на 8 этапе дипломной работы. Пример получения системного сообщения «FNPSH-I-3027-Фильтрующий интерфейс включен (eth0)» показан на рисунке 9.30.

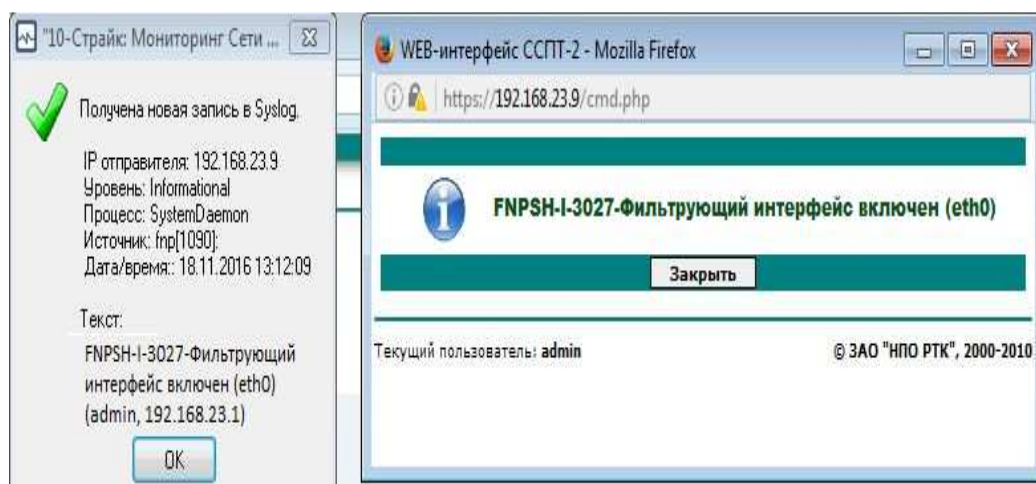


Рисунок 9.30 - Пример получения системного сообщения «FNPSH-I-3027-Фильтрующий интерфейс включен (eth0)»

Для функции проверки неиспользуемых портов на коммутационном оборудовании cisco 2960s настроена проверка по SNMP протоколу.

Данная проверка аналогична по настройкам с проверкой используемых портов. Так как 3 порт на коммутаторе cisco 2960s не используется, для примера сделана проверка на 3 порту. Задано условие проверки, проверка прошла если, нажата кнопка «получить», и так как 3 порт не имеет подключение, то в соответствии с описанием OID ifOperStatus, показанным на рисунке 9.26, получено значение равное 2. Настройка проверки на 3 порту показана на рисунке 9.31.

сообщения «FNPSH-I-3026-Фильтрующий интерфейс отключен (eth0)» показан на рисунке 9.34.

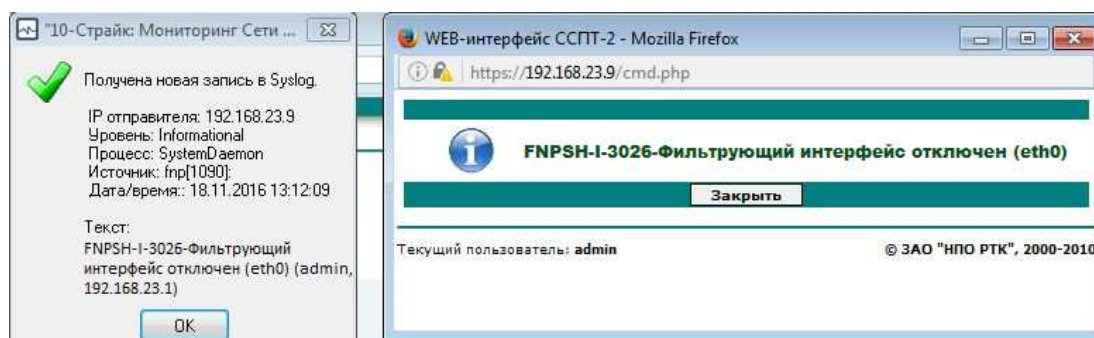


Рисунок 9.34 - Пример получения системного сообщения «FNPSH-I-3026-Фильтрующий интерфейс отключен (eth0)»

Для функции проверки удаленного подключения администратора к коммутатору cisco 2960s настроена проверка по SNMP.

Для добавления данной проверки выбран хост курсором мыши и в главном меню программы выбрана вкладка «проверки» и нажата кнопка «добавить проверку». Добавление новой проверки показано на рисунке 9.35.

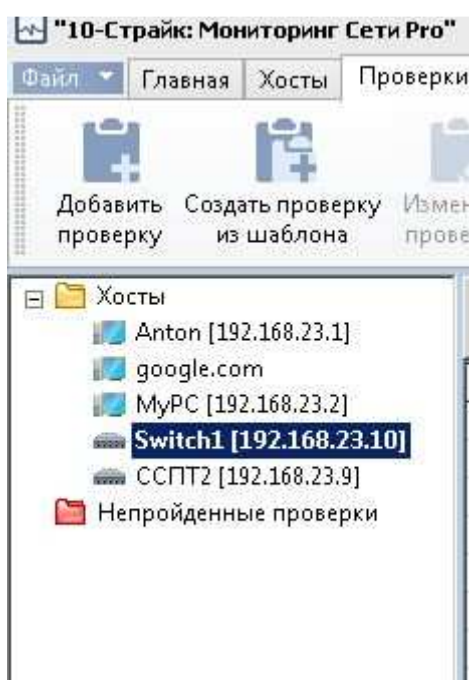


Рисунок 9.35 – Добавление новой проверки

Далее после открытия диалогового окна «Мастер проверок» выбран тип и параметры проверки в данном случае это проверка по SNMP. Для проверки удаленного подключения администратора загружены mib файлы коммутатора cisco 2960s в корень установленного ПО в папку mibs. После

чего открыт mib браузер в ПО и выбран OID который отвечает за состояние администратора в данном случае это ifAdminStatus. Выбор OID ifAdminStatus в mib браузере показан на рисунке 9.36.

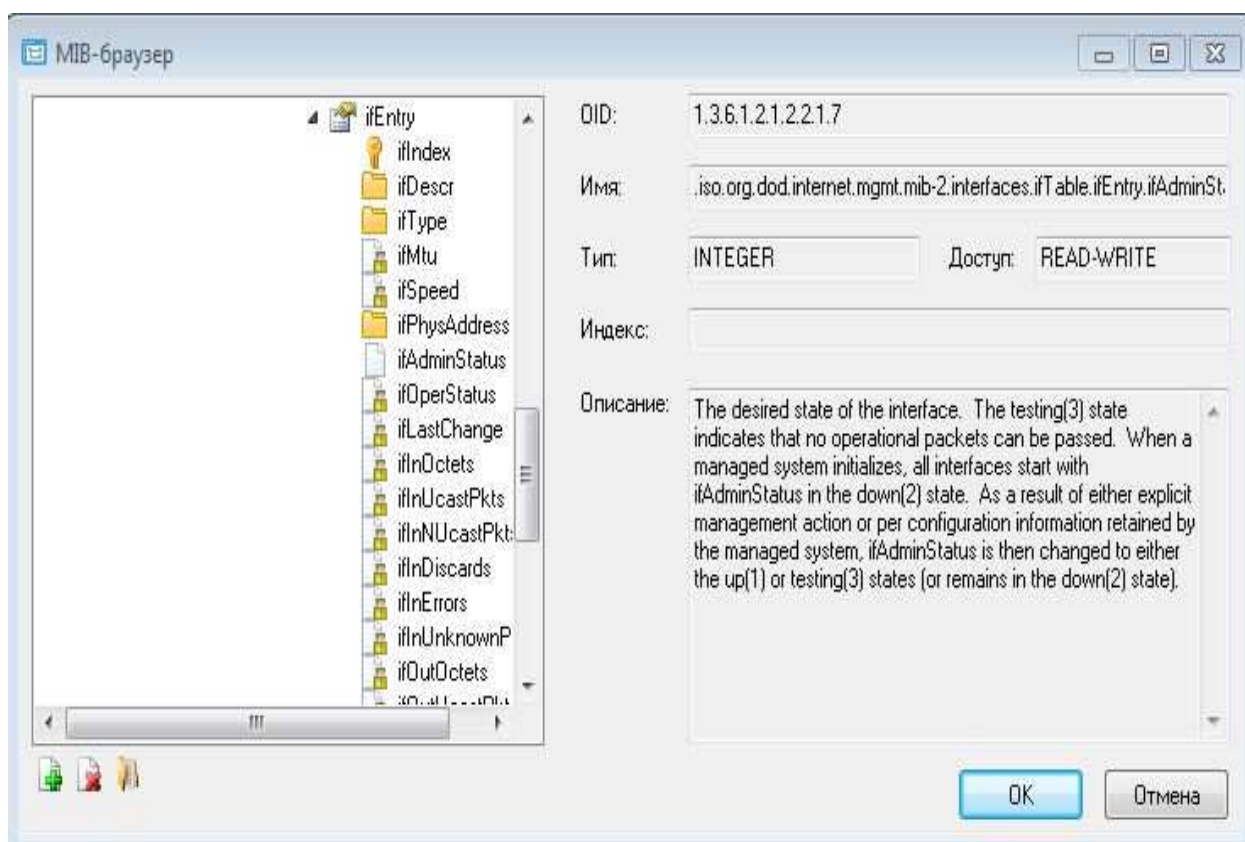


Рисунок 9.36 - Выбор OID ifAdminStatus в mib браузере

После выбора OID нажата кнопка «Ок». В окне выбора типа и параметров проверки, в строке OID появился выбранный OID ifAdminStatus, для проверки подключения администратора к коммутатору cisco 2960s помимо всего этого, выбрана версия протокола SNMP, в данном случае 2с и имя «community myRO», которое было задано в конфигурации коммутатора на этапе 8 дипломной работы. Задано условие проверки, проверка прошла если получено значение равное 1, нажата кнопка «получить» и так как администратор в данный момент подлкючен, то в соответствии с описанием OID ifAdminStatus показанным на рисунке 9.36, получено значение равное 1. Настройка SNMP для OID ifAdminStatus представленная на рисунке 9.37.

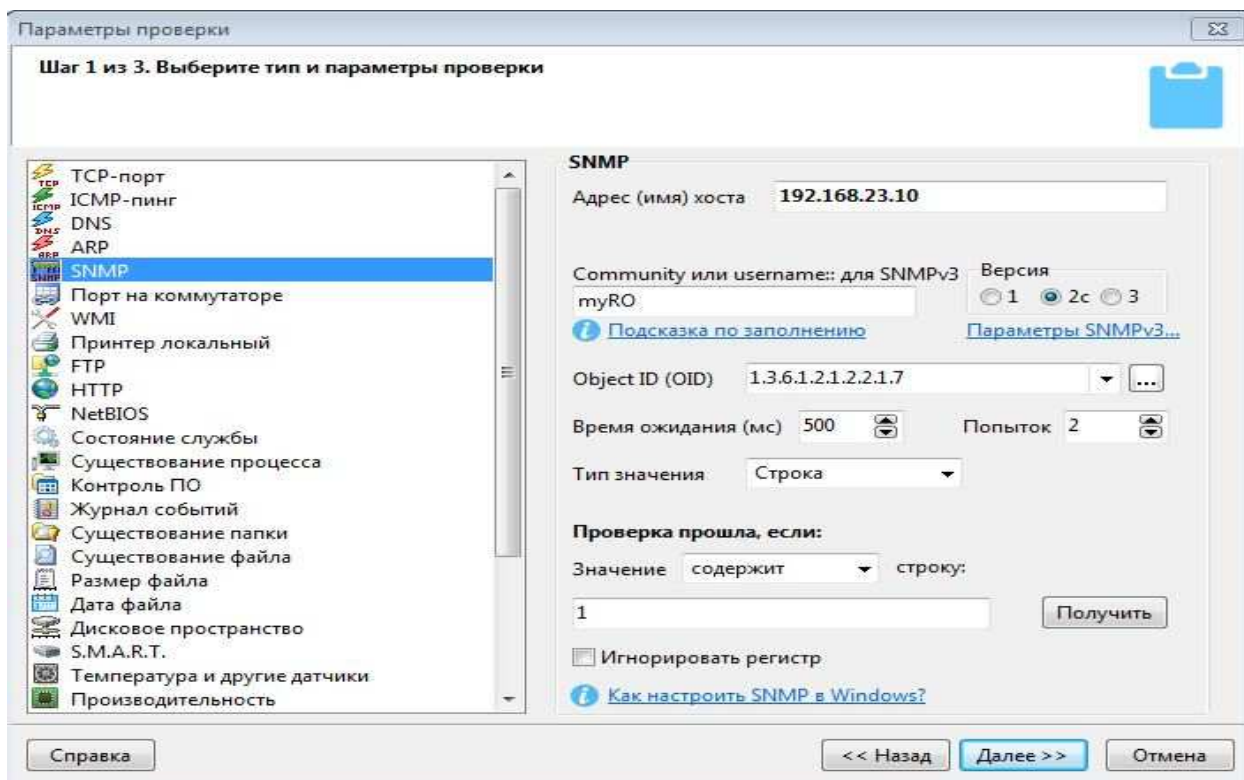


Рисунок 9.37 - Настройка SNMP для OID ifAdminStatus

Далее необходимо задать зависимости проверки и другие параметры, так как зависимостей у данной проверки нет, то этот шаг пропущен.

Далее заданы действия, которые будут выполняться при соответствующих результатах проверки. Это выдача сообщения на экран, если проверка прошла и выдача сообщения на экран, если проверка не прошла. Назначение действий, которые будут выполняться при соответствующих результатах проверки показаны на рисунке 9.38.

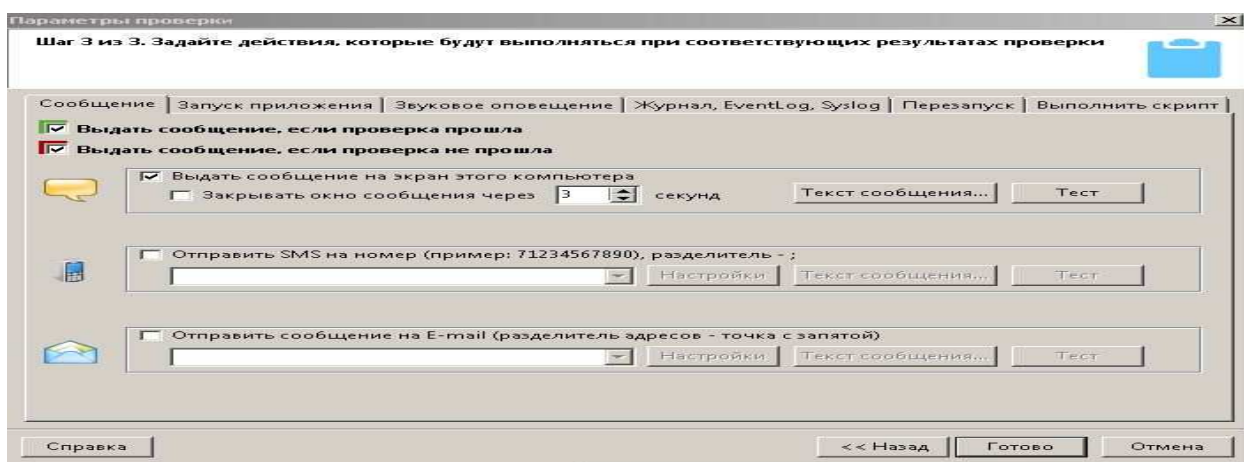


Рисунок 9.38 - Назначение действий, которые будут выполняться при соответствующих результатах проверки

Так как администратор подключен, то результатом является успешная проверка. Результат проверки по OID ifAdminStatus показан на рисунке 9.39.

Отображаемо...	Имя или адрес хо...	Тип проверки	Состояние	Статус	Время отклика	Значение пар...	Последнее с
Switch1	192.168.23.10	ICMP-пинг	Включена	Успешно з...	1 мс	-	ICMP-пинг: 1
Switch1	192.168.23.10	SNMP	Включена	Успешно з...	0 мс	-	SNMP: Полу

Хост:	192.168.23.10	Время смены статуса:	16.11.2016 10:35:05	Действия:	Сообщение
Проверка:	SNMP	Интервал проверки (сек.):	120	Действия:	Сообщение
Описание:	Последнее сообщение: SNMP: Полученное значение "1" содержит заданную строку "1"				

Легенда:
 - отключена
 - прошла
 - не прошла
 - не прошла по зависимости

Информация /
 [Время отклика, за последний час](#) /
 [Время отклика, за период](#) /
 [Время простоя, за период](#) /
 [Отчёт об авариях](#)

Рисунок 9.39 - Результат проверки по OID ifAdminStatus

В случае если администратор отключиться от коммутатора то проверка не пройдет. Результат проверки по OID ifAdminStatus с отключенным от коммутатора администратором показан на рисунке 9.40.

Отображаемо...	Имя или адрес хо...	Тип проверки	Состояние	Статус	Время отклика	Значение пар...	Последнее с
Switch1	192.168.23.10	ICMP-пинг	Включена	Успешно з...	1 мс	-	ICMP-пинг: 1
Switch1	192.168.23.10	SNMP	Включена	Не прошла	-	1	SNMP: Полу

Хост:	192.168.23.10	Время смены статуса:	16.11.2016 10:41:09	Действия:	Сообщение
Проверка:	SNMP	Интервал проверки (сек.):	120	Действия:	Сообщение
Описание:	Последнее сообщение: SNMP: Полученное значение 2 не равно заданному 1				

Легенда:
 - отключена
 - прошла
 - не прошла
 - не прошла по зависимости

Информация /
 [Время отклика, за последний час](#) /
 [Время отклика, за период](#) /
 [Время простоя, за период](#) /
 [Отчёт об авариях](#)

Рисунок 9.40 - Результат проверки по OID ifAdminStatus с отключенным от коммутатора администратором

Помимо проверки по протоколу SNMP, данная проверка была настроена и по протоколу Syslog.

Для функции контроля попыток доступа через VTY терминалы к cisco2960s, было настроено логирование, настройка проведена на 8 этапе дипломной работы. Контроль попыток подключения к коммутатору через vty терминалы очень важен. Это может заранее предупредить о попытках злоумышленника получить доступ к коммутатору. Поэтому в случае попыток доступа к коммутатору через терминалы, попытки логируются и отсылаются в ПО системы мониторинга 10 Страйк: Мониторинг сети Pro. Если администратор зайдет со своего ip адреса то будет получен следующий лог

Oct 13 21:10:44.185 EDT: %SEC-6-IPACCESSLOGP: list 117 permitted tcp

192.168.23.1(Vlan1) -> 192.168.23.10(0/0), 1 packet.

Если злоумышленник попытается зайти то будет получен следующий лог

Oct 13 21:10:54.185 EDT: %SEC-6-IPACCESSLOGP: list 117 denied tcp

192.168.23.4(Vlan1) -> 192.168.23.10(0/0), 1 packet.

Пример получения логов в программе 10 Страйк: Мониторинг сети Pro, показан на рисунке 9.41.

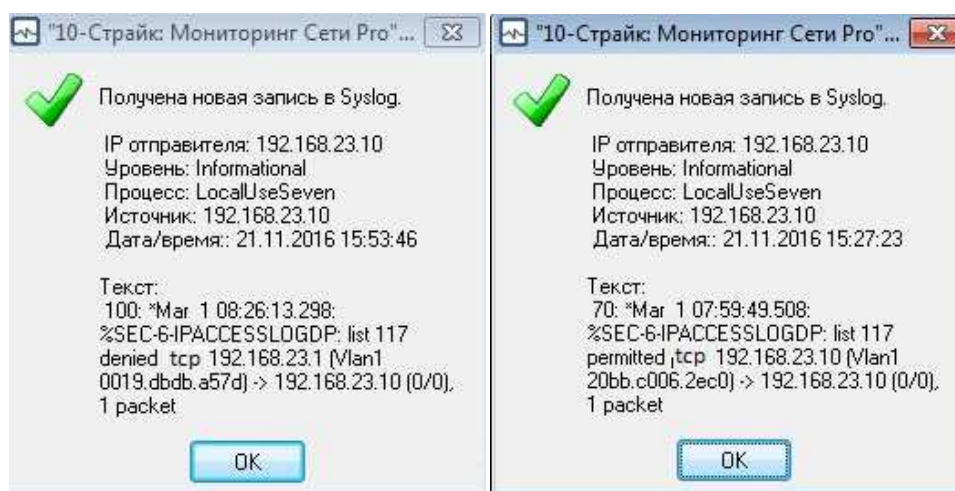


Рисунок 9.41 - Пример получения логов в программе 10 Страйк: Мониторинг сети Pro

Для функции проверки удаленного подключения администратора на межсетевом экране ССПТ-2 настроена проверка по Syslog.

В случае подключения администратора к межсетевому экрану ССПТ-2, будет выдано системное сообщение «FNPSH-I-3001-Успешная авторизация пользователя Admin». Данное сообщение получает программа мониторинга 10 Страйк: Мониторинг сети Pro, после настройки приема Syslog сообщений. Настройка получения Syslog сообщений от меж сетевого экрана ССПТ-2 проведена на 8 этапе дипломной работы. Пример получения системного сообщения «FNPSH-I-3001-Успешная авторизация пользователя Admin» показан на рисунке 9.42.

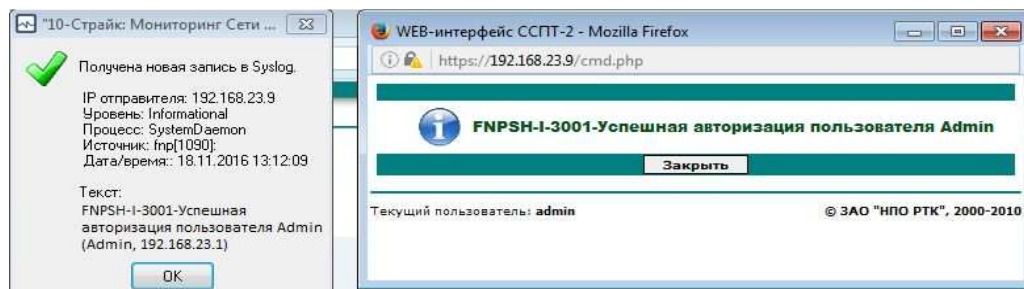


Рисунок 9.42 - Пример получения системного сообщения «FNPSH-I-3001-Успешная авторизация пользователя Admin»

Для функции проверки загрузки порта на коммутаторе cisco 2960s настроена проверка по SNMP. Описание настройки данной проверки приведено ниже.

Для добавления данной проверки выбран хост курсором мыши и в главном меню программы выбрана вкладка «проверки» и нажата кнопка «добавить проверку». Добавление новой проверки показано на рисунке 9.43.

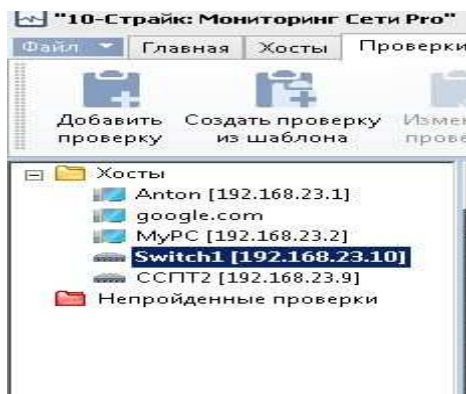


Рисунок 9.43 – Добавление новой проверки

Далее после открытия диалогового окна «Мастер проверок» выбран тип и параметры проверки в данном случае это проверка по SNMP. Для проверки загрузки порта на коммутаторе загружены mib файлы коммутатора cisco 2960s в корень установленного ПО в папку mibs. После чего открыт mib браузер в ПО и выбран OID который отвечает за состояние администратора в данном случае это ifInOctets и ifOutOctets. Выбор OID ifInOctets в mib браузере показан на рисунке 9.44.

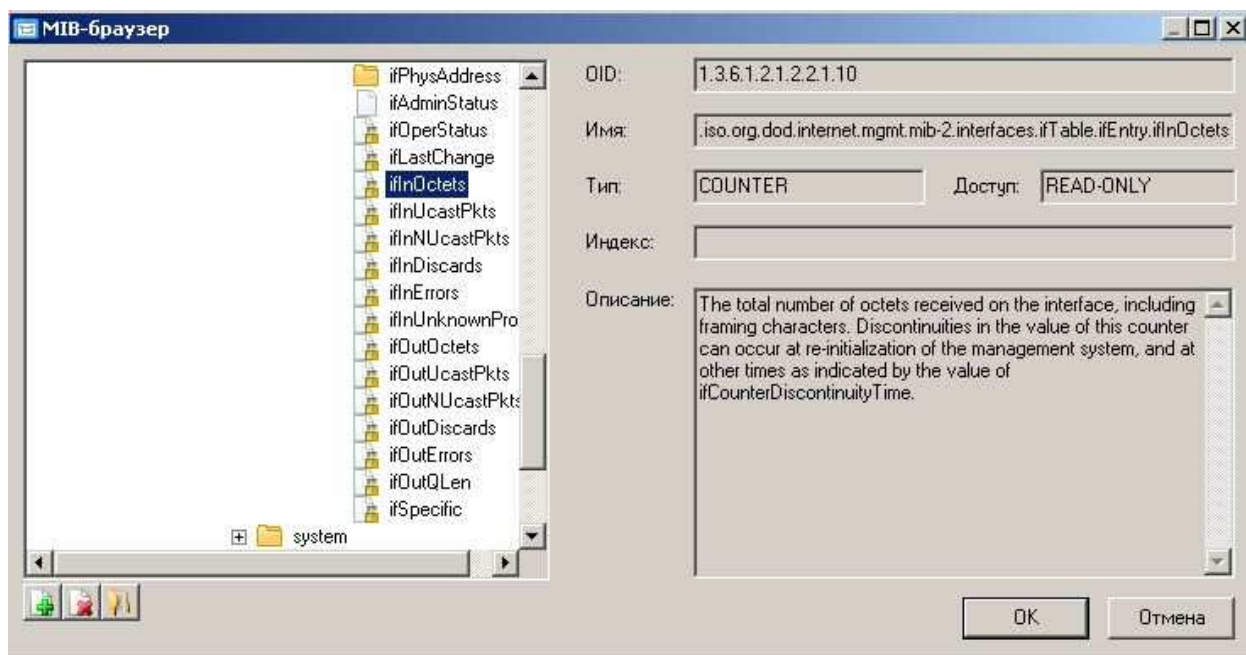


Рисунок 9.44 - Выбор OID ifInOctets в mib браузере

После выбора OID нажата кнопка «Ок». В окне выбора типа и параметров проверки, в строке OID появился выбранный OID ifInOctets, описание OID показано на рисунке 9.44, для проверки загрузки конкретного порта, для примера это будет первый порт, в конце OID дописано значение 10101. Значение 10101 дописывается, потому что это условное обозначение 101XX, где 101 это обозначение гигабитных коммутаторов, а XX это номер порта. Помимо всего этого, выбрана версия протокола SNMP, в данном случае 2с и имя «community myRO», которое было задано в конфигурации коммутатора на этапе 8 дипломной работы. Заданы условия проверки, проверка прошла если, и задан допустимый порог загрузки порта на получение пакетов. Настройка SNMP для OID ifInOctets представленная на рисунке 9.45.

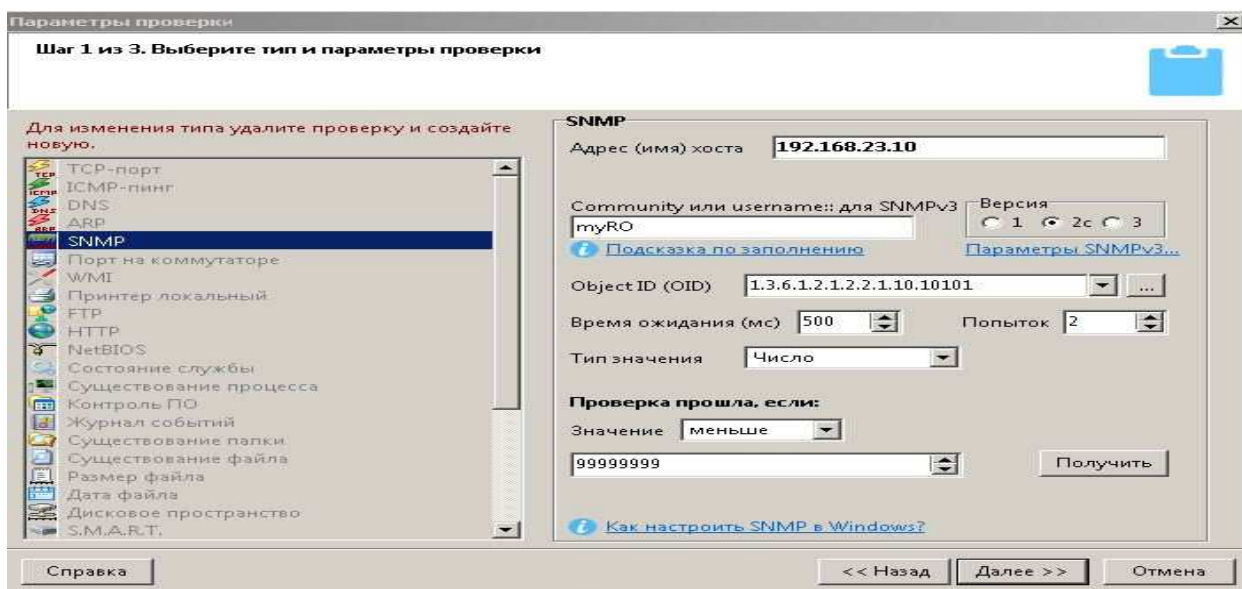


Рисунок 9.45 - Настройка SNMP для OID ifInOctets

Далее необходимо задать зависимости проверки и другие параметры, так как зависимостей у данной проверки нет, то этот шаг пропущен.

Далее заданы действия, которые будут выполняться при соответствующих результатах проверки. Это выдача сообщения на экран, если проверка прошла и выдача сообщения на экран, если проверка не прошла. Назначение действий, которые будут выполняться при соответствующих результатах проверки показаны на рисунке 9.46.

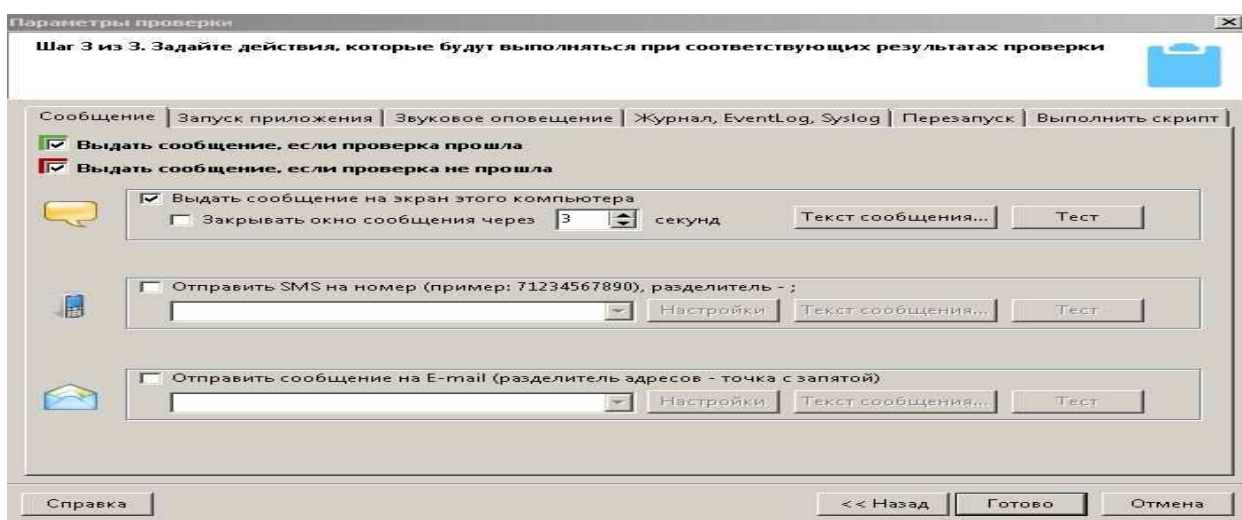


Рисунок 9.46 - Назначение действий, которые будут выполняться при соответствующих результатах проверки

Отображаемо...	Имя или адрес хо...	Тип проверки	Состояние	Статус	Время отклика	Значение параметр...
Switch1	192.168.23.10	ICMP-пинг	Включена	Успешно завершила...	1 мс	-
Switch1	192.168.23.10	SNMP	Включена	Успешно завершила...	15 мс	-
Switch1	192.168.23.10	SNMP	Включена	Не прошла	-	1
Switch1	192.168.23.10	SNMP	Включена	Успешно завершила...	15 мс	1114813

Хост: 192.168.23.10 ⌚ Время смены статуса: 11.11.2016 15:45:18 📧 Действия: Сообщение

Проверка: SNMP ⌚ Интервал проверки (сек.): 120 📧 Действия: Сообщение

Описание: ⌚ Последнее сообщение: SNMP: Полученное значение 1114813 меньше заданного 99999999

Легенда: - отключена - прошла - не прошла - не прошла по зависимости

Информация / Время отклика, за последний час / Время отклика, за период / Время простоя, за период / Отчёт об авариях

В случае если порог будет превышен то проверка не пройдет. Результат проверки по OID `ifInOctets` с превышением допустимого порога показан на рисунке 9.48.

Отображаемо...	Имя или адрес хо...	Тип проверки	Состояние	Статус	Время отклика	Значение параметр...
Switch1	192.168.23.10	ICMP-пинг	Включена	Успешно завершила...	4 мс	-
Switch1	192.168.23.10	SNMP	Включена	Успешно завершила...	0 мс	-
Switch1	192.168.23.10	SNMP	Включена	Не прошла	-	1
Switch1	192.168.23.10	SNMP	Включена	Успешно завершила...	16 мс	1149975
Switch1	192.168.23.10	SNMP	Включена	Не прошла	-	1149760

Хост: 192.168.23.10 ⌚ Время смены статуса: 11.11.2016 15:53:04 🟢 Действия:

✓ Проверка: SNMP ⏰ Интервал проверки (сек.): 120 🔴 Действия:

📄 Описание: 💬 Последнее сообщение: SNMP: Полученное значение 1149760 больше заданного 1111111

💡 Легенда: □ - отключена ■ - прошла ■ - не прошла ■ - не прошла по зависимости

Информация / Время отклика, за последний час / Время отклика, за период / Время простоя, за период / Отчёт об авариях

81

Для ifOutOctets. Выбор OID ifOutOctets в mib браузер показан на рисунке 9.49.

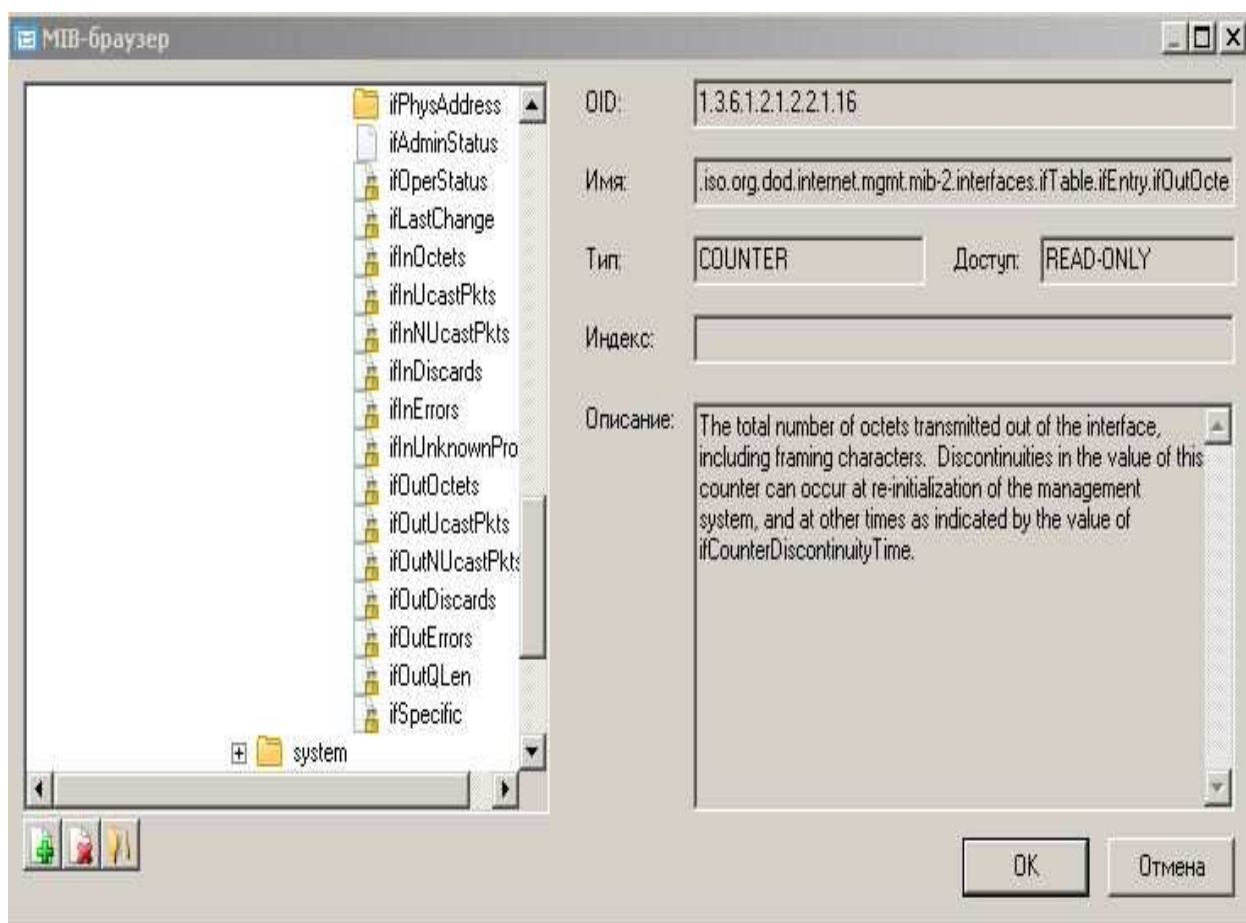


Рисунок 9.49 - Выбор OID ifOutOctets в mib браузере

После выбора OID нажата кнопка «Ок». В окне выбора типа и параметров проверки, в строке OID появился выбранный OID ifOutOctets, описание OID показано на рисунке 9.49, для проверки загрузки конкретного порта, для примера это будет первый порт, в конце OID дописано значение 10101. Значение 10101 дописывается, потому что это условное обозначение 101XX, где 101 это обозначение гигабитных коммутаторов, а XX это номер порта. Помимо всего этого, выбрана версия протокола SNMP, в данном случае 2с и имя «community myRO», которое было задано в конфигурации коммутатора на этапе 8 дипломной работы. Задано условие проверки, проверка прошла если, и задан допустимый порог загрузки порта на отдачу пакетов. Настройка SNMP для OID ifOutOctets представлена на рисунке 9.50.

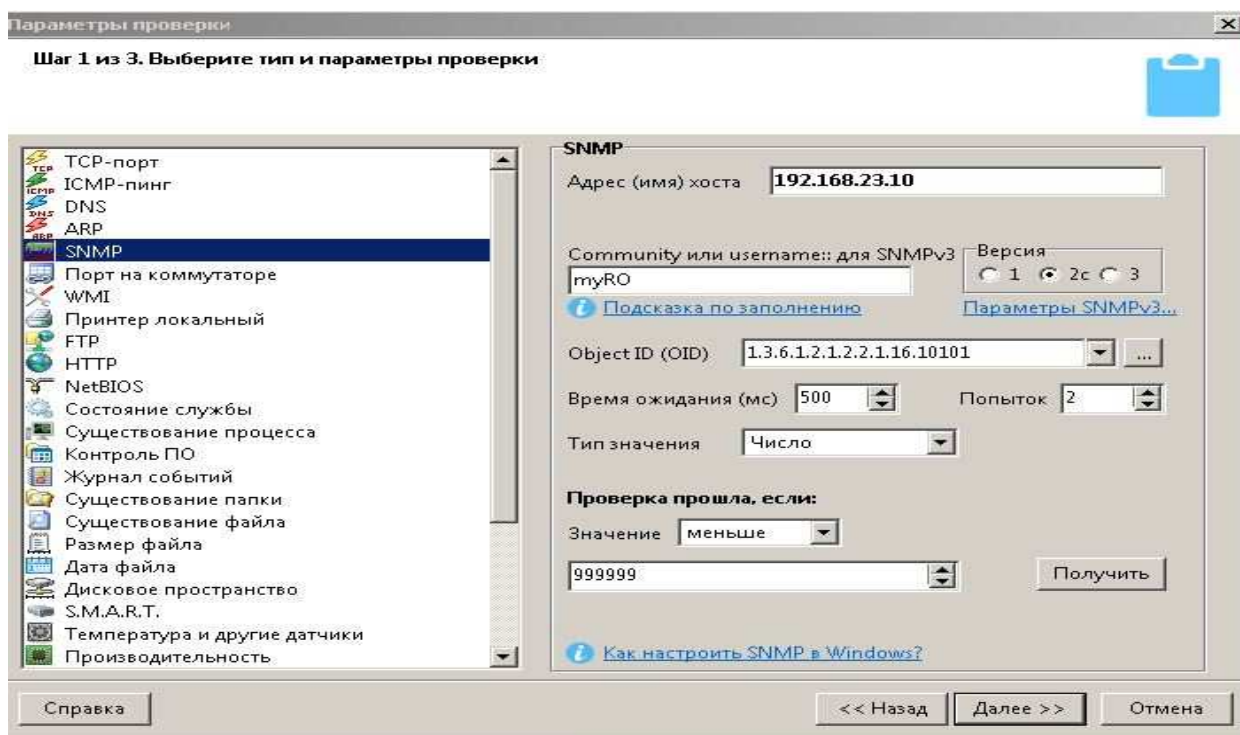


Рисунок 9.50 - Настройка SNMP для OID ifInOctets

Далее необходимо задать зависимости проверки и другие параметры, так как зависимостей у данной проверки нет, то этот шаг пропущен.

Далее заданы действия, которые будут выполняться при соответствующих результатах проверки. Это выдача сообщения на экран, если проверка прошла и выдача сообщения на экран, если проверка не прошла. Назначение действий, которые будут выполняться при соответствующих результатах проверки показаны на рисунке 9.51.

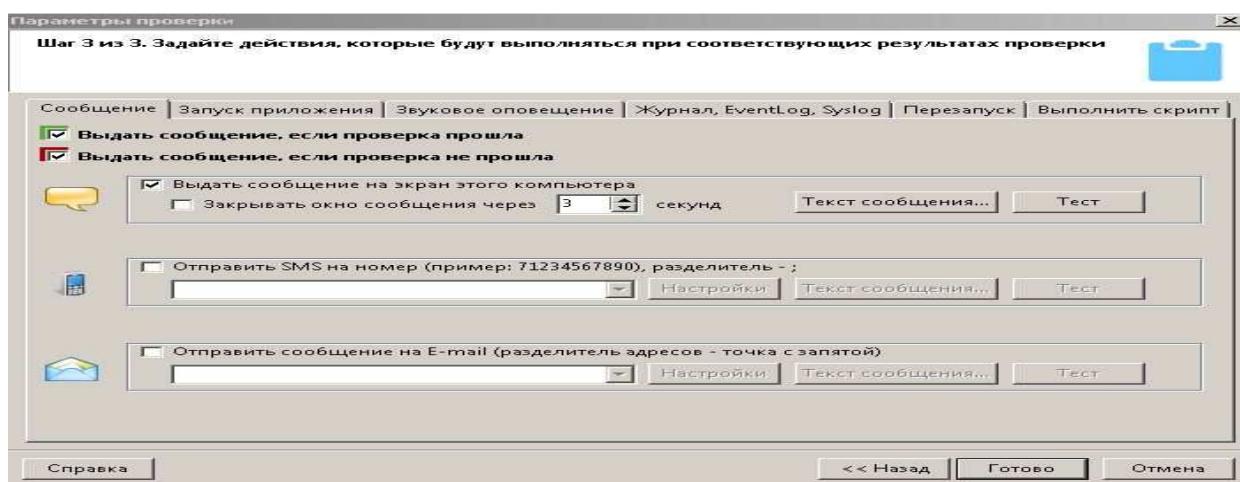


Рисунок 9.51 - Назначение действий, которые будут выполняться при соответствующих результатах проверки

Так как нагрузка порта не велика и полученное значение не превышает заданный допустимый порог, то результатом является успешная проверка. Результат проверки по OID ifOutOctets показан на рисунке 9.52.

Отображаемо...	Имя или адрес хо...	Тип проверки	Состояние	Статус	Время отклика	Значение параметр...
Switch1	192.168.23.10	ICMP-пинг	Включена	Успешно завершила...	0 мс	-
Switch1	192.168.23.10	SNMP	Включена	Успешно завершила...	16 мс	-
Switch1	192.168.23.10	SNMP	Включена	Не прошла	-	1
Switch1	192.168.23.10	SNMP	Включена	Успешно завершила...	16 мс	1175341
Switch1	192.168.23.10	SNMP	Включена	Не прошла	-	1173893
Switch1	192.168.23.10	SNMP	Включена	Успешно завершила...	15 мс	463183

Хост:	192.168.23.10	Время смены статуса:	11.11.2016 15:55:55	Действия:	Сообщение
Проверка:	SNMP	Интервал проверки (сек.):	120	Действия:	Сообщение
Описание:	Последнее сообщение: SNMP: Полученное значение 463183 меньше заданного 999999				
Легенда:	☐ - отключена ☒ - прошла ☐ - не прошла ☐ - не прошла по зависимости				

Рисунок 9.52 - Результат проверки по OID ifOutOctets

В случае если порог будет превышен то проверка не пройдет. Результат проверки по OID ifOutOctets с превышением допустимого порога показан на рисунке 9.53.

Отображаемо...	Имя или адрес хо...	Тип проверки	Состояние	Статус	Время отклика	Значение параметр...
Switch1	192.168.23.10	ICMP-пинг	Включена	Успешно завершила...	1 мс	-
Switch1	192.168.23.10	SNMP	Включена	Успешно завершила...	15 мс	-
Switch1	192.168.23.10	SNMP	Включена	Не прошла	-	1
Switch1	192.168.23.10	SNMP	Включена	Успешно завершила...	16 мс	1198262
Switch1	192.168.23.10	SNMP	Включена	Не прошла	-	1196411
Switch1	192.168.23.10	SNMP	Включена	Успешно завершила...	0 мс	469859
Switch1	192.168.23.10	SNMP	Включена	Не прошла	-	470525

Хост:	192.168.23.10	Время смены статуса:	11.11.2016 15:58:11	Действия:	Сообщение
Проверка:	SNMP	Интервал проверки (сек.):	120	Действия:	Сообщение
Описание:	Последнее сообщение: SNMP: Полученное значение 470525 больше заданного 444444				
Легенда:	☐ - отключена ☒ - прошла ☐ - не прошла ☐ - не прошла по зависимости				

Рисунок 9.53 - Результат проверки по OID ifOutOctets с превышением допустимого порога

Для функции контроля несанкционированного подключения к портам на коммутаторе cisco 2960s настроена проверка по Syslog. Описание настройки данной проверки приведено на этапе 8 дипломной работы.

По умолчанию все не используемые порты находятся в состоянии down(выключен), но в случае подключения к порту он переходит в состояние up(включен). В случае несанкционированного подключения к порту 5 коммутатора, на ПО системы мониторинга будет отправлен лог. Пример приема лога о состоянии порта 5 (up) показан на рисунке 9.54. Данный лог говорит о том, что порт 5 включен. Если злоумышленник отключится от порта 5 коммутатора, то на ПО системы мониторинга будет отправлен лог. Пример приема лога о состоянии порта 5 (down) показан на рисунке 9.55.

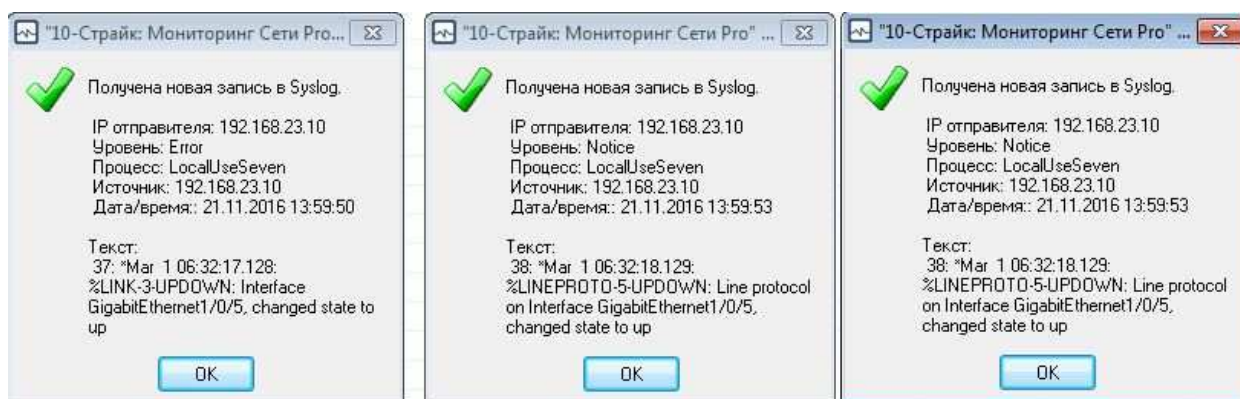


Рисунок 9.54 - Пример приема лога о состоянии порта 5 (up)

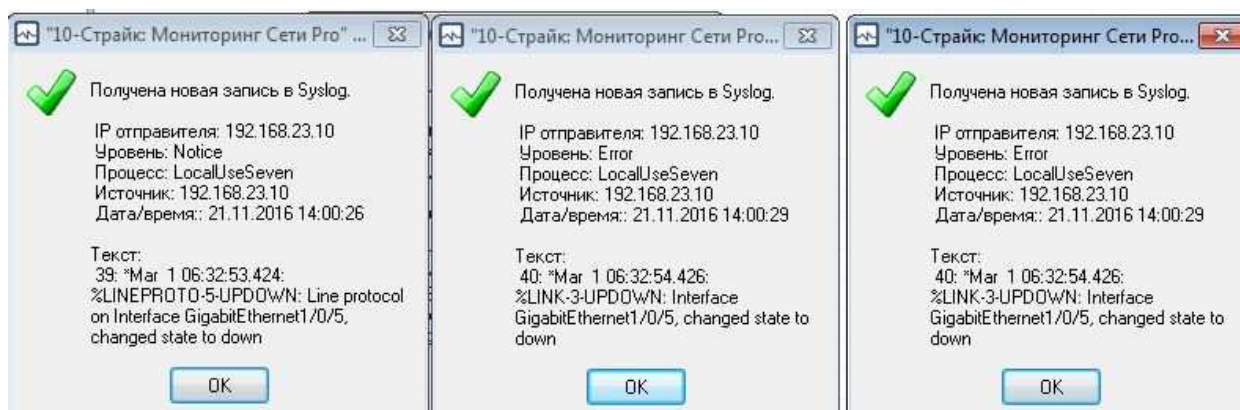


Рисунок 9.55 - Пример приема лога о состоянии порта 5 (down)

Все логи записываются в журнал syslog на ПО системы мониторинга. Пример записи логов в журнал Syslog показан на рисунке 9.56.

192.168.23.10	5	23	192.168.23.10	31:	*Mar 1 06:25:20.833: %SYS-5-CONFIG-I: Configured from console by console
192.168.23.10	6	23	192.168.23.10	32:	*Mar 1 06:25:21.834: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.23.1 Port 514 started - CLI initiated
192.168.23.10	3	23	192.168.23.10	33:	*Mar 1 06:28:42.149: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/5, changed state to up
192.168.23.10	5	23	192.168.23.10	34:	*Mar 1 06:28:43.150: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/5, changed state to up
192.168.23.10	5	23	192.168.23.10	35:	*Mar 1 06:31:26.765: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/5, changed state to down
192.168.23.10	3	23	192.168.23.10	36:	*Mar 1 06:31:27.766: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/5, changed state to down
192.168.23.10	3	23	192.168.23.10	37:	*Mar 1 06:32:17.128: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/5, changed state to up
192.168.23.10	5	23	192.168.23.10	38:	*Mar 1 06:32:18.129: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/5, changed state to up
192.168.23.10	5	23	192.168.23.10	39:	*Mar 1 06:32:53.424: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/5, changed state to down
192.168.23.10	3	23	192.168.23.10	40:	*Mar 1 06:32:54.426: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/5, changed state to down

Рисунок 9.56 - Пример записи логов в журнал Syslog

Для функции контроля несанкционированная подключения к межсетевому экрану ССПТ-2 выполнены аналогичные действия, по настройки состояния порта, которые показаны выше.

Для функции контроля событий ACL на коммутационном оборудовании cisco 2960s настроена проверка по Syslog протоколу. Настройка проверки проведена на 8 этапе дипломной работы.

В случае нарушения правил ACL, будет сформирован лог, который будет отправлен на ПО системы мониторинга 10 Страйк: Мониторинг Сети Pro. Для примера задана проверка, разрешен ping с хоста 192.168.23.1 на хост 192.168.23.10, осуществлена команда ping, получен лог на ПО системы мониторинга. Демонстрация лога, с разрешением ping с хоста 192.168.23.1 на хост 192.168.23.10, показана на рисунке 9.57.

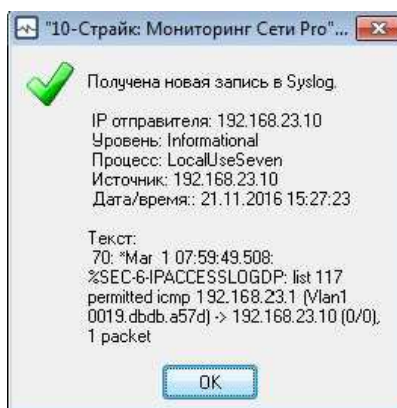


Рисунок 9.57 - Демонстрация лога, с разрешением ping с хоста 192.168.23.1 на хост 192.168.23.10

Для примера задана проверка, запрещен ping с хоста 192.168.23.1 на хост 192.168.23.10, осуществлена команда ping, получен лог на ПО системы мониторинга. Демонстрация лога, с запретом ping с хоста 192.168.23.1 на хост 192.168.23.10, показана на рисунке 9.58.

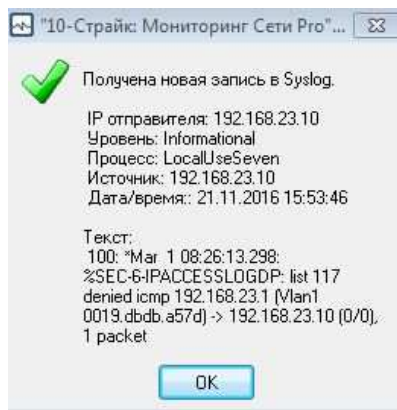


Рисунок 9.58 - Демонстрация лога, с запретом ping с хоста 192.168.23.1 на хост 192.168.23.10

Для функции контроля событий ACL на межсетевом экране ССПТ-2 настроена проверка по Syslog протоколу. Настройка проверки проведена на 8 этапе дипломной работы.

Для функции контроля событий ACL, добавлено правило фильтрации MAC. Данное правило настроено следующим образом, в главном меню WEB интерфейса выбрана вкладка правила, далее выбрана вкладка MAC, появилось окно с правилами MAC, если они есть. Если правил нет, нажата иконка «белый листок» под надписью «Регулярные MAC правила» и создано правило. Окно правил MAC показано на рисунке 9.59.

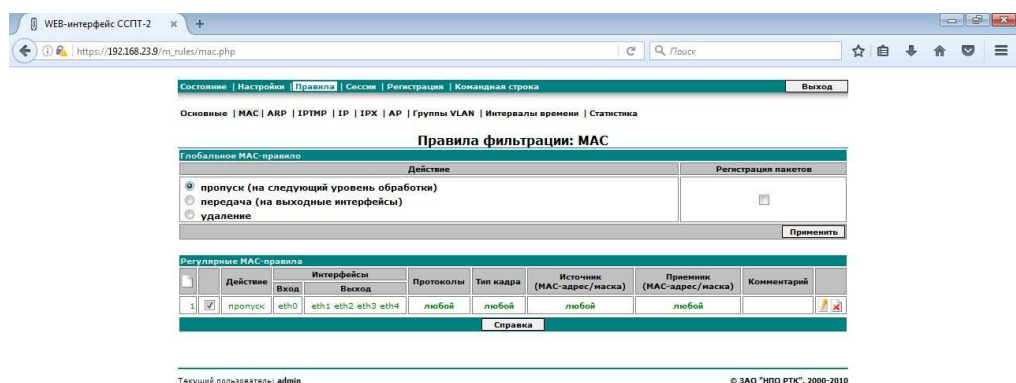


Рисунок 9.59 - Окно правил MAC

Окно добавления MAC правил показано на рисунке 9.60. В данном правиле под номером 3, запрещено MAC адресу 001d92099e9c обращаться по любому протоколу к MAC адресу 0019dbdba57d. Компьютер с MAC адресом 001d92099e9c подключен к порту eth0, а компьютер с MAC адресом 0019dbdba57d к порту eth1.

Redaction of MAC rule 3

Basic rule parameters		Interfaces		Packet registration	VLAN group
Number	Activity	Action	Input		
3	☒	☐ deletion ☐ bypass ☐ transmission	☒ eth0 ☐ eth1 ☐ eth2 ☐ eth3 ☐ eth4	☒ eth0 ☐ eth1 ☐ eth2 ☐ eth3 ☐ eth4	☐ any frames ☐ only not VLAN ☐ only VLAN: <input type="text"/>
Protocols		Signalization	Interval time		Comment
☒ any		☒	<input type="text"/>		<input type="text"/>
Ethernet frame parameters					
Frame type		Source (MAC address/mask)		Destination (MAC address/mask)	
☒ any ☐ Ethernet II ☐ IEEE 802.3-LLC ☐ IEEE 802.3-raw ☐ IEEE 802.3-SNAP		☐ any <input type="text"/> 001d92099e9c		☐ any <input type="text"/> 0019dbdba57d	
<input type="button" value="Save"/> <input type="button" value="Help"/> <input type="button" value="Close"/>					

Current user: admin © ЗАО "МНО РИ", 2008-2010

Рисунок 9.60 - Окно добавления MAC правил

Для примера осуществлена команда ping на компьютер с MAC адресом 0019dbdba57d, с компьютера, который имеет MAC адрес 001d92099e9c. Результат команды ping для MAC правила №3 показан на рисунке 9.61.

```
C:\Users\Admin>ping 192.168.23.1

Обмен пакетами с 192.168.23.1 по 32 байтами данных:
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.

Статистика Ping для 192.168.23.1:
Пакетов: отправлено = 4, получено = 0, потеряно = 4
<100% потеря>
```

Рисунок 9.61 - Результат команды ping для для MAC правила №3

В данном случае, в случае его нарушения, будет отправлено системное сообщение, сигнализация о нарушении MAC правила №3 показанное на рисунке 9.62.

```
Nov 23 15:40:23 fnp2 fnp[1150]: fnp_filt: Сигнализация фильтрации -
15:40:23.260751[drop][mac:3]eth0->[IP/ICMP]192.168.23.5[192.168.23.1
Nov 23 15:40:28 fnp2 fnp[1150]: fnp_filt: Сигнализация фильтрации -
15:40:28.102530[drop][mac:3]eth0->[ARP]001d92099e9c[0019dbdba57d
Nov 23 15:40:28 fnp2 fnp[1150]: fnp_filt: Сигнализация фильтрации -
15:40:28.118315[drop][mac:3]eth0->[IP/ICMP]192.168.23.5[192.168.23.1
Nov 23 15:40:29 fnp2 fnp[1150]: fnp_filt: Сигнализация фильтрации -
15:40:29.101060[drop][mac:3]eth0->[ARP]001d92099e9c[0019dbdba57d
Nov 23 15:40:30 fnp2 fnp[1150]: fnp_filt: Сигнализация фильтрации -
15:40:30.099732[drop][mac:3]eth0->[ARP]001d92099e9c[0019dbdba57d
Nov 23 15:40:33 fnp2 fnp[1150]: fnp_filt: Сигнализация фильтрации -
15:40:33.126796[drop][mac:3]eth0->[IP/ICMP]192.168.23.5[192.168.23.1
Nov 23 15:40:38 fnp2 fnp[1150]: fnp_filt: Сигнализация фильтрации -
15:40:38.115522[drop][mac:3]eth0->[IP/ICMP]192.168.23.5[192.168.23.1
Nov 23 15:41:57 fnp2 fnp[1150]: fnp_filt: Сигнализация фильтрации -
15:41:57.243685[drop][mac:3]eth0->[ARP]001d92099e9c[0019dbdba57d
Nov 23 15:41:58 fnp2 fnp[1150]: fnp_filt: Сигнализация фильтрации -
15:41:58.223080[drop][mac:3]eth0->[ARP]001d92099e9c[0019dbdba57d
Nov 23 15:41:59 fnp2 fnp[1150]: fnp_filt: Сигнализация фильтрации -
15:41:59.237190[drop][mac:3]eth0->[ARP]001d92099e9c[0019dbdba57d
```

Рисунок 9.62 – Системное сообщение, сигнализация о нарушении MAC правила №3

Так же для контроля событий ACL, добавлено правило фильтрации по IP. Данное правило настроено следующим образом, в главном меню WEB интерфейса выбрана вкладка правила, далее выбрана вкладка IP, появилось окно с правилами IP, если они есть. Если правил нет, нажата иконка «белый листок» под надписью «Регулярные IP правила» и создано правило. Окно правил IP показано на рисунке 9.63.

Состояние | Настройки | **Правила** | Сессии | Регистрация | Командная строка | Выход

Основные | MAC | ARP | IPTMP | IP | IPX | AP | Группы VLAN | Интервалы времени | Статистика

Правила фильтрации: IP

Глобальное IP правило

Действие	Регистрация
☒ пропуск (на следующий уровень обработки)	☐ пакеты
☐ удаление	☐ сессии

Применить

Регулярные IP правила

Действие	Интерфейсы		Протокол	Источник		Приемник		Комментарий
	Входящий	Исходящий		IP адрес/маска	Порт	IP адрес/маска	Порт	

Справка

Текущий пользователь: admin

© ЗАО "НПО РТК", 2000-2010

Рисунок 9.63 - Окно правил IP

Окно добавления IP правил показано на рисунке 9.64. В данном правиле под номером 1, запрещено диапазону ip адресов с 192.168.23.2 по 192.168.23.8 обращаться по протоколу ICMP к ip адресу 192.168.23.1.

WEB-интерфейс CCITT-2 - Mozilla Firefox

https://192.168.23.9/in_rules/ipr_edit.php?rule=0

Добавление IP правила

Общие параметры правила

Номер	Активность	Действие	Интерфейсы		Регистрация	VLAN группа	Сигнализация	Интервал времени	Комментарий
			Входящий	Исходящий					
1	☒	☒ удаление ☐ пропуск ☐ передача	☒ eth0 ☐ eth1 ☐ eth2 ☐ eth3 ☐ eth4	☒ eth0 ☒ eth1 ☒ eth2 ☒ eth3 ☒ eth4	☐ пакеты ☐ сессии	☒ любые кадры ☐ только не VLAN ☐ только VLAN ☐ VLAN группа	☒		

Параметры IP пакета

Протокол	Источник		Приемник	
	IP адрес/маска	Порт	IP адрес/маска	Порт
☐ любой icmp	☐ любой 3.23.2-192.168.23.8	☒ любой any	☐ любой 192.168.23.1	☒ любой any

Параметры IP | Дополнительные параметры

Сохранить | Справка | Закрыть

Текущий пользователь: admin

© ЗАО "НПО РТК", 2000-2010

Рисунок 9.64 - Окно добавления IP правила

Окно с добавленным правилом фильтрации по ip показано на рисунке 9.65.

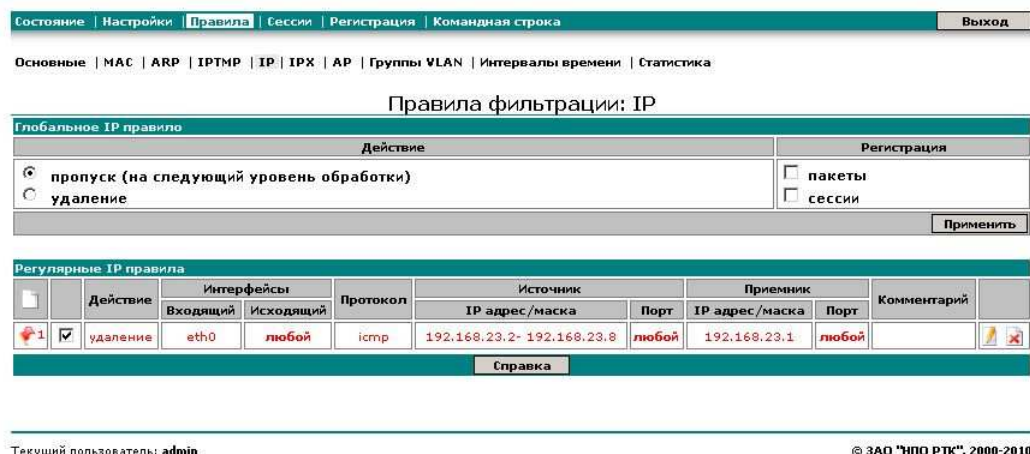


Рисунок 9.65 - Окно с добавленным правилом фильтрации по ip

Для примера осуществлена команда `ping ip 192.168.23.1` с ip 192.168.23.2, ping не проходит. Результат `ping ip 192.168.23.1` с ip 192.168.23.2 показан на рисунке 9.66.

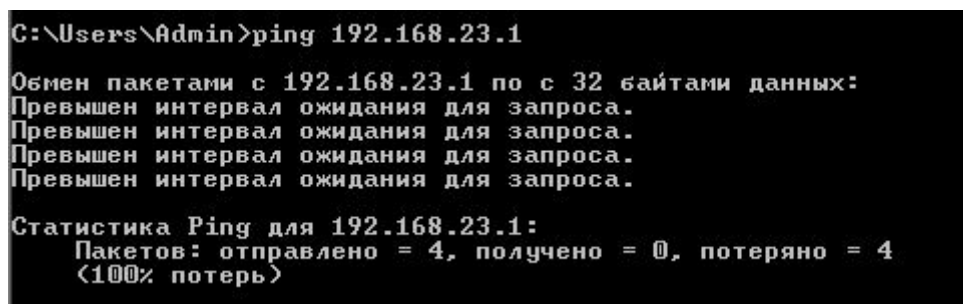


Рисунок 9.66 - Результат `ping ip 192.168.23.1` с ip 192.168.23.2

В данном случае, в случае его нарушения, отправлено системное сообщение, сигнализация о нарушении ip правила №1 показанное на рисунке 9.67.

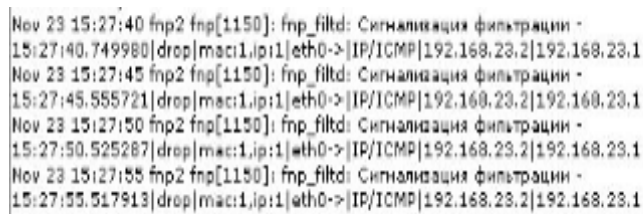


Рисунок 9.67 – Системное сообщение, сигнализация о нарушении ip правила №1

Для примера осуществлена команда `ping ip 192.168.23.1` с ip не внесенного в диапазон запрета, взят ip 192.168.23.15, так как он не попадает в

диапазон запрета. Результат ping ip 192.168.23.1 с ip 192.168.23.15 показан на рисунке 9.68.

```
C:\Users\Admin>ping 192.168.23.1

Обмен пакетами с 192.168.23.1 по 32 байтами данных:
Ответ от 192.168.23.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.23.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.23.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.23.1: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.23.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    <0% потерь>
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
```

Рисунок 9.68 - Результат ping ip 192.168.23.1 с ip 192.168.23.15

Таким образом система мониторинга сетевых компонентов выполняет следующие функции:

- функция контроля работоспособность коммутационного оборудования;
- функция контроля несанкционированное подключение к порту;
- функция мониторинга используемых портов;
- функция мониторинга не используемых портов;
- функция удаленного подключения администратора;
- функция контроля событий ACL;
- функция контроля выборочной загрузки портов.

ЗАКЛЮЧЕНИЕ

В ходе выполнения ВКР, была разработана система мониторинга сетевых компонентов, которая осуществляет контроль коммутационного оборудования с помощью протоколов контроля доступа. В случае нарушения правил доступа или нарушения конфигураций доступа, будет отправлено сообщение на АРМ администратора безопасности, для принятия решения. Результаты данной дипломной работы применены в ОКР, о чем говорится в акте внедрения.

Для создания системы мониторинга сетевых компонентов в распределенной ИСПДн, в ходе ВКР были выполнены следующие этапы:

- изучена структура информационной системы персональных данных с точки зрения обеспечения мониторинга коммутационного оборудования;
- изучены возможные методы мониторинга состояния коммутационного оборудования;
- изучен протокол SNMP для анализа состояния коммутационного оборудования;
- осуществлен выбор программного обеспечения для системы мониторинга;
- разработаны требования к коммутационному оборудованию и осуществлен выбор коммутационного оборудования;
- разработаны требования к характеристикам ПЭВМ для системы мониторинга;
- разработан перечень контролируемых событий на коммутационном оборудовании;
- разработаны типовые конфигурации файлов для коммутационного оборудования, используемого в ИСПДн;
- разработана конфигурация (настройка) программного обеспечения используемого для системы мониторинга.

Таким образом, все требования задания на выпускную квалификационную работу были выполнены в полном объеме.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

- 1 Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) "О персональных данных" (с изм. и доп., вступ. в силу с 01.09.2015);
- 2 ГОСТ 34.003-90 «Информационная технология Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения», - Введ. 1992-01-01. (ИПК Издательство стандартов, 1992г., 14 стр.);
- 3 Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями от 27 июля 2010 г., 6 апреля, 21 июля 2011 г., 28 июля 2012 г., 5 апреля, 7 июня, 2 июля, 28 декабря 2013 г., 5 мая, 21 июля 2014 г.);
- 4 ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».– Взамен ГОСТ Р 50922-96, введ. 2006–12–27. (ИПК Издательство стандартов, 2008 г., 12 стр.);
- 5 ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения». – Введ 2009-10-01.
- 6 ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования» - ИПК издательство стандартов г.Москва, 25 стр., введ 01.07.90.
- 7 ГОСТ Р 34.10-2001 «Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» - официальное издание Госстандарт России., 16 стр., введ 12.09.2001.
- 8 Catalyst 2960 and 2960-s Switch Software Configuration guide. Cisco Systems, Inc, March 2010. USA – 1018 pages.
- 9 Межсетевой экран ССПТ-2. Руководство администратора. ЗАО «НПО РТК», 2006-2012г. Санкт-Петербург – 245 с.

ПРИЛОЖЕНИЕ А
(обязательное)
Структура ИСПДн

Структура информационной системы персональных данных

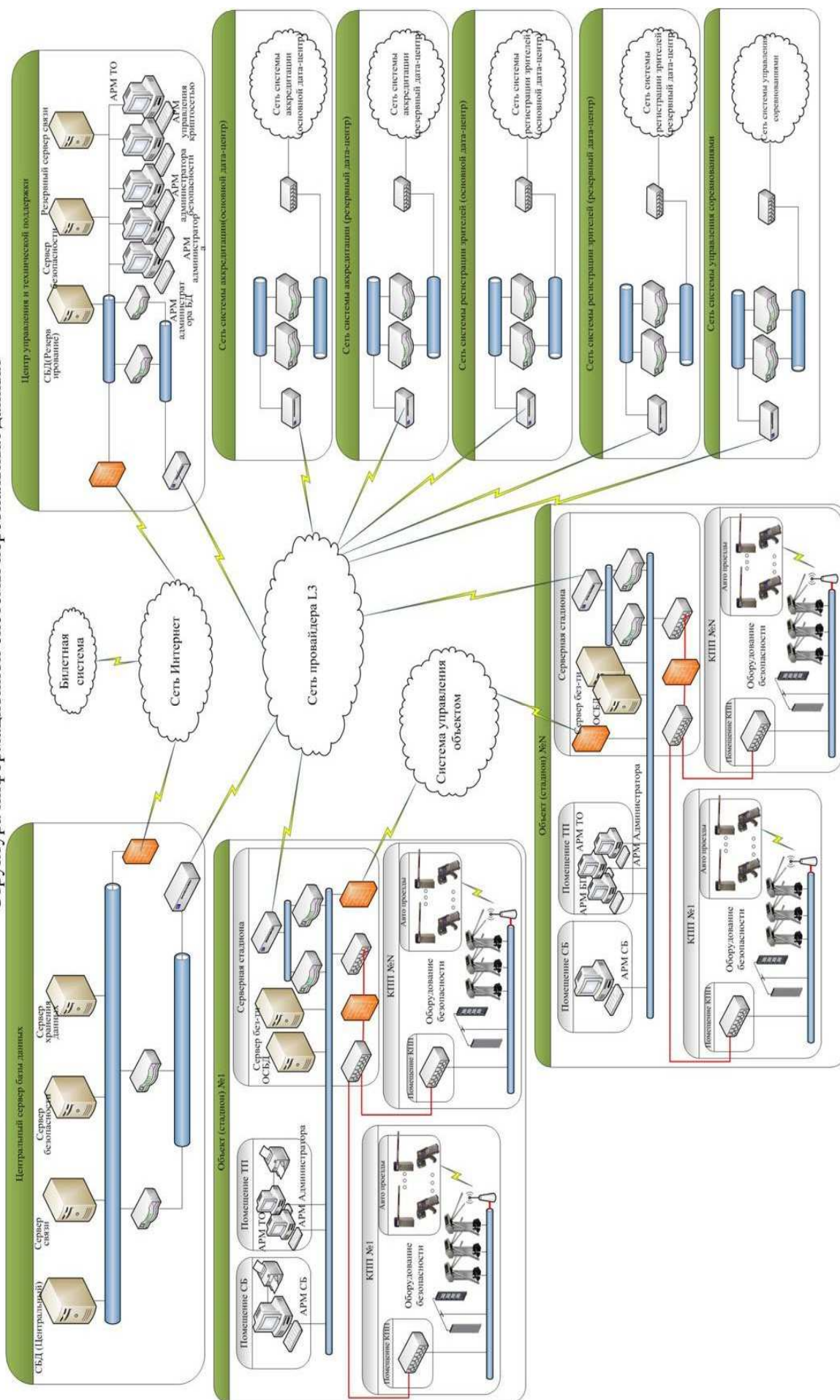


Рисунок А.1 – Структура ИСПДн

ПРИЛОЖЕНИЕ Б
(обязательное)
Структура информационных потоков в ИСПДн

Структура информационных потоков в информационной системе персональных данных

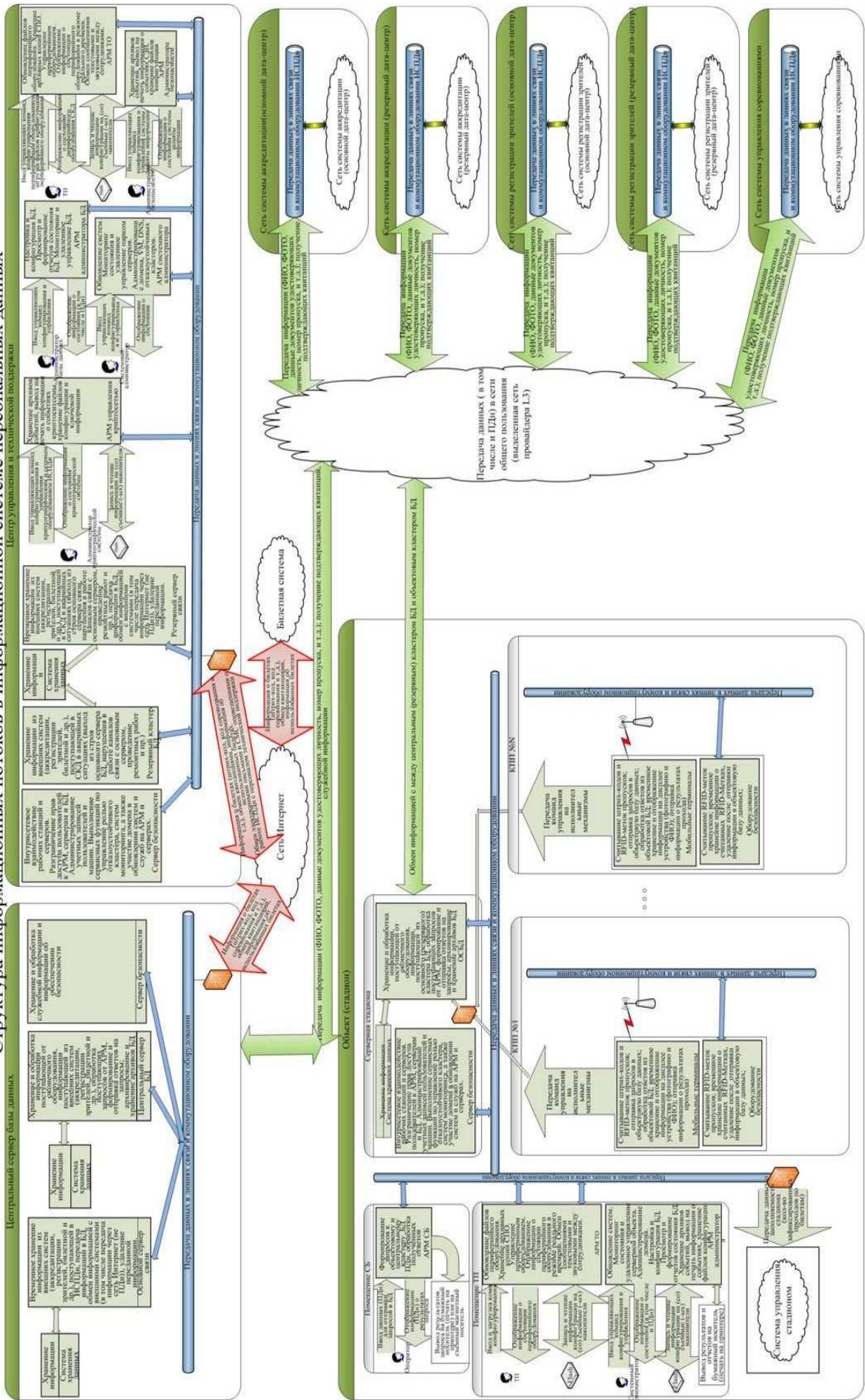


Рисунок Б.1 – Структура информационных потоков в информационной системе персональных данных

ПРИЛОЖЕНИЕ В
(обязательное)
Состав системы мониторинга

Состав системы мониторинга

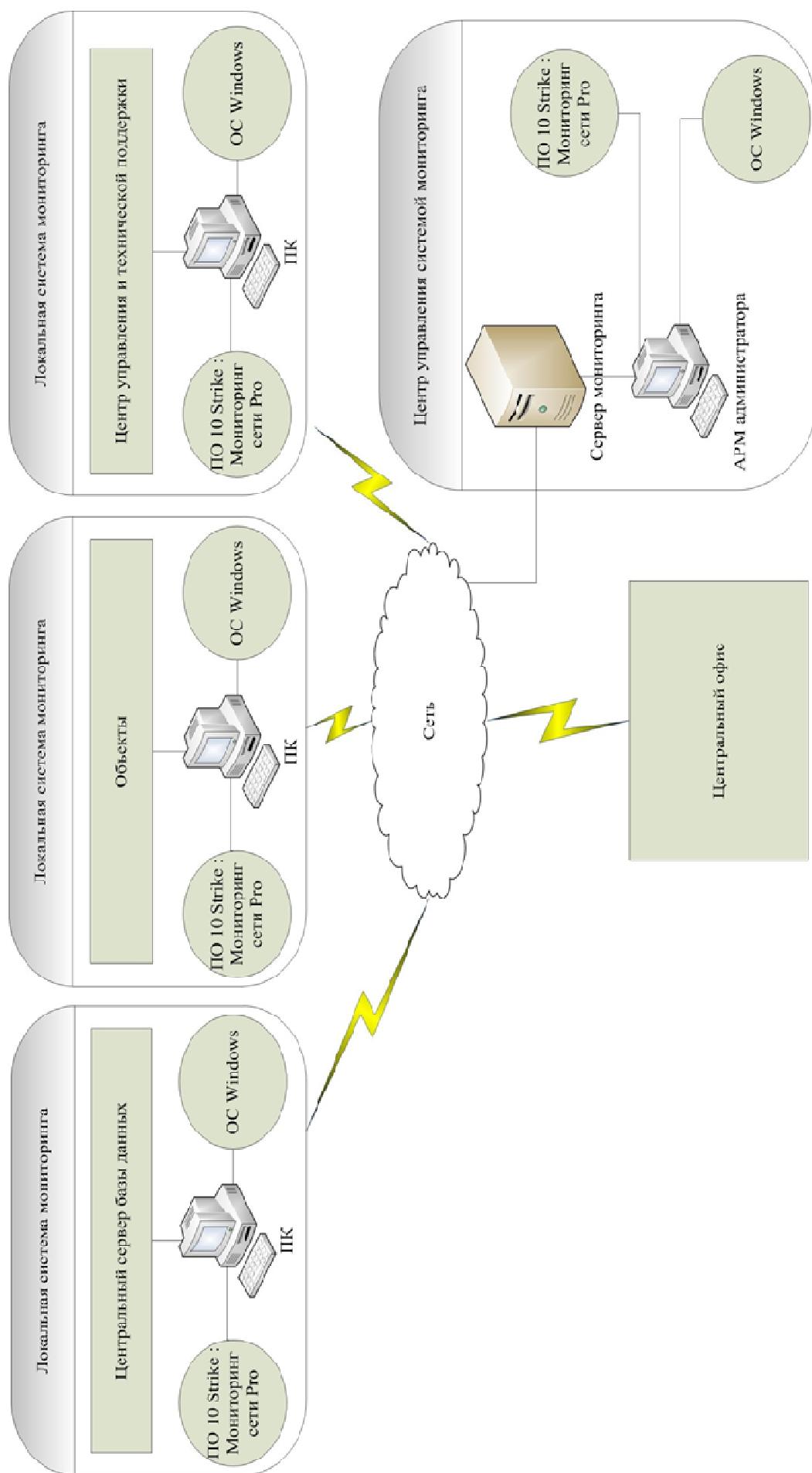


Рисунок В.1 – Состав системы мониторинга

ПРИЛОЖЕНИЕ Г

(обязательное)

Состав программного обеспечения системы мониторинга

Состав программного обеспечения системы мониторинга

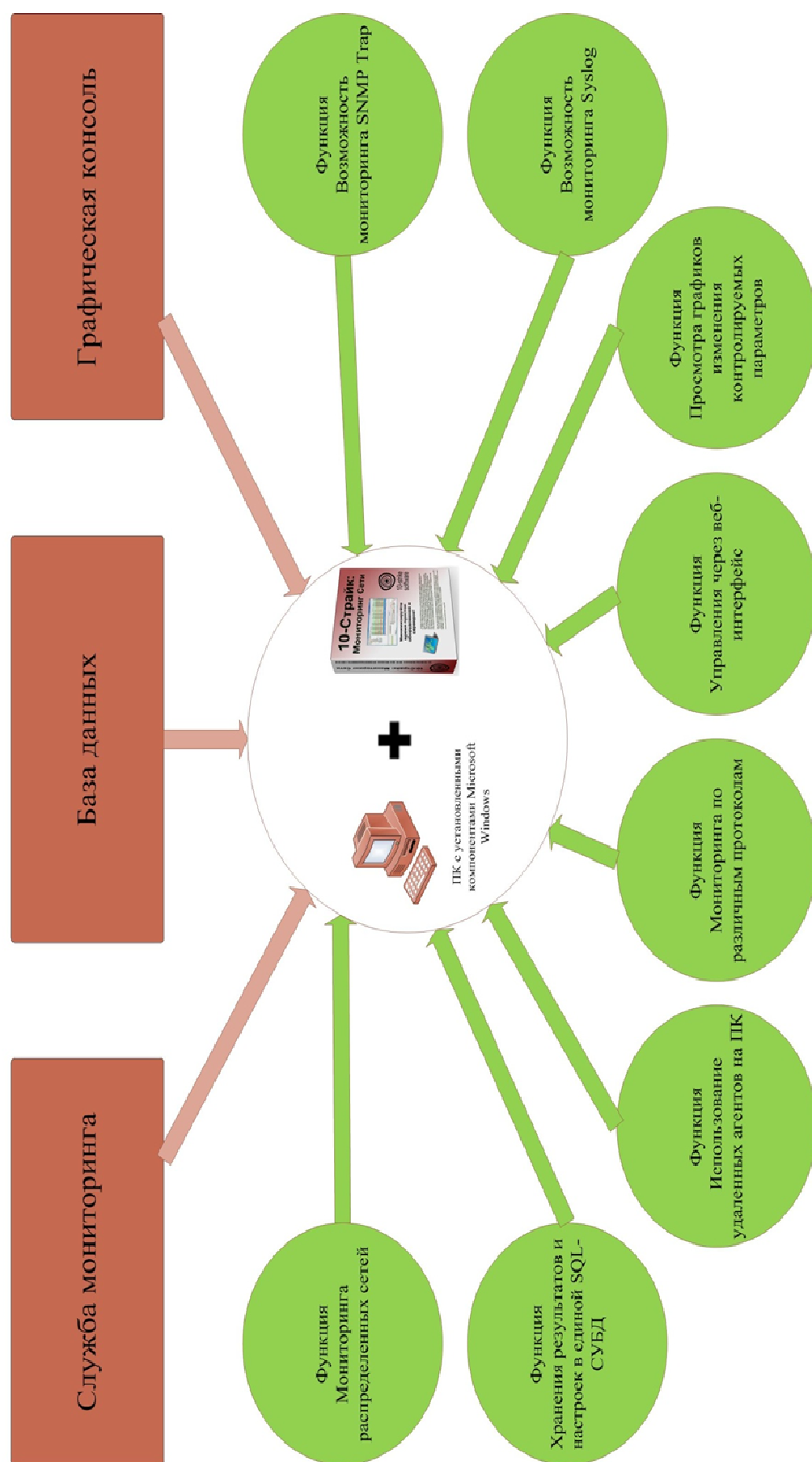


Рисунок Г.1 – Состав программного обеспечения системы мониторинга

ПРИЛОЖЕНИЕ Д

(обязательное)

Файл конфигурации для коммутатора cisco 2960-s

Был разработан файл конфигурации для коммутационного оборудования, коммутатора cisco2960s. [8]

Файл конфигураций для коммутатора cisco2960s представлен ниже.

```
Switch> enable
Switch# configure terminal
Switch(config)# enable password sergey
Switch(config)# line vty 0 15
Switch(config-line)# password sergey
Switch(config-line)# login
Switch(config-line)# exit
Switch(config)# exit
Switch# configure terminal
Switch(config)# service password-encryption
Switch(config)# hostname cisco2960s
cisco2960s(config)# interface vlan 1
cisco2960s(config-if)# ip address 192.168.23.10 255.255.255.0
cisco2960s(config-if)# exit
cisco2960s(config)# interface range gi 1/0/1 — 26
cisco2960s(config-if-range)# no shutdown
cisco2960s(config-if-range)# switchport mode access
cisco2960s(config-if-range)# exit
cisco2960s(config)# no ip http server
cisco2960s(config)# ip default-gateway 192.168.23.0
cisco2960s(config)# ip access-list standard TELNET
cisco2960s(config-std-nacl)# permit 192.168.23.1
cisco2960s(config-std-nacl)# permit 192.168.23.15
cisco2960s(config-std-nacl)# permit any
cisco2960s(config-std-nacl)# exit
cisco2960s(config)# line vty 0 15
cisco2960s(config-line)# access-class TELNET in
cisco2960s(config-line)# exec-timeout 5 0
cisco2960s(config-line)# exit
cisco2960s(config)# snmp-server community myRO RO
cisco2960s(config)# snmp-server community myRW RW
cisco2960s(config)# snmp-server trap-source Vlan1
cisco2960s(config)# snmp-server source-interface informs Vlan1
cisco2960s(config)# snmp-server host 192.168.23.1 myRO
cisco2960s(config)# snmp-server host 192.168.23.1 myRW
cisco2960s(config)# exit
```

```

cisco2960s# copy running-config startup-config
cisco2960s# wri
cisco2960s# configure terminal
cisco2960s(config)#snmp-server view test internet included
cisco2960s(config)#snmp-server group TESTGR v3 auth write test
cisco2960s(config)#snmp-server user TESTUSER TESTGR v3 auth md5 testpass
cisco2960s(config)#exit
cisco2960s# copy running-config startup-config
cisco2960s# wri
cisco2960s(config)#logging on
cisco2960s(config)#logging buffered informational
cisco2960s(config)#logging buffered 16386
cisco2960s(config)#logging 192.168.23.1
cisco2960s(config)#logging trap informational
cisco2960s(config)#access-list 117 permit ip host 192.168.23.1 any
cisco2960s(config)#access-list 117 deny ip any any log-input
cisco2960s(config)#line vty 0 15
cisco2960s(config-line)#access-class 117 in
cisco2960s(config-line)#exit
cisco2960s(config)#access-list 117 permit icmp 192.168.23.1
cisco2960s(config)#access-list 117 deny icmp 192.168.23.1
cisco2960s(config)#access-list 117 permit any any
cisco2960s(config)# interface vlan 1
cisco2960s(config-if)#access-class 117 in
cisco2960s(config-if)#exit
cisco2960s(config)# exit
cisco2960s# copy running-config startup-config
cisco2960s# wri

```

Пояснения к конфигурирующему файлу приведены ниже.

Для работы с коммутатором cisco 2960-s задан пароль на режим конфигурирования, для безопасности доступа к коммутационному оборудованию. Для этого в командной строке коммутатора с помощью команды `configure terminal`, осуществлен вход в режим конфигурирования коммутатора. Далее, чтобы задать пароль на режим конфигурирования использована команда `enable password` и задан пароль ,в данном случае пароль `sergey`.

```
Switch> enable
```

```
Switch# configure terminal
```

```
Switch(config)# enable password sergey
```

Чтобы иметь удаленное подключение к коммутатору, установлен пароль для входа по telnet, для этого осуществлен вход в режим настройки виртуальных терминалов с помощью добавления команды line vty 0 15 в командную строку коммутатора, где цифры означают количество терминалов с 0 по 15. В режиме настройки виртуальных терминалов используя команду password задан пароль, в данном случае sergey.

```
Switch(config)# line vty 0 15
```

```
Switch(config-line)# password sergey
```

Чтобы включить удаленное подключение к коммутатору, использована команда login, не выходя из режима настройки виртуальных терминалов, после чего осуществлен выход из данного режима используя команду exit.

```
Switch(config-line)# login
```

```
Switch(config-line)# exit
```

```
Switch(config)# exit
```

Для того, чтобы пароль на вход в режим управления коммутатором был защищен, осуществлен вход в режим конфигурирования коммутатора с помощью команды configure terminal и использована команда service password-encryption, которая шифрует заданный пароль на режим управления коммутатором.

```
Switch# configure terminal
```

```
Switch(config)# service password-encryption
```

Чтобы коммутатор отличался от других, себе подобных. Было задано имя коммутатора, для этого в режиме конфигурирования коммутатора использована команда hostname, которая изменяет стандартное имя коммутатора, в данном случае имя заменено на cisco2960s.

```
Switch(config)# hostname cisco2960s
```

Чтобы можно было обращаться к коммутатору был задан IP-адрес коммутатора, с помощью команды ip address. Для этого в командной строке коммутатора осуществлен вход в режим конфигурирования, выбран интерфейс vlan1, с использованием команды interface vlan 1, так как он

является управляющим интерфейсом. После чего задан ip адрес коммутатора с помощью команды ip address, в данном случае ip адрес 192.168.23.10

```
cisco2960s(config)# interface vlan 1  
cisco2960s(config-if)# ip address 192.168.23.10 255.255.255.0  
cisco2960s(config-if)# exit
```

Чтобы произвести начальные настройки всех портов коммутатора осуществлен вход в режим конфигурирования коммутатора, осуществлен вход в диапазон портов с 1 по 26 на коммутаторе, с помощью команды interface range gi 1/0/1 - 26 и заданы начальные настройки.

```
cisco2960s(config)# interface range gi 1/0/1 — 26  
cisco2960s(config-if-range)# no shutdown  
cisco2960s(config-if-range)# switchport mode access  
cisco2960s(config-if-range)# exit
```

Так как веб интерфейс для конфигурирования не нужен, то с помощью команды no ip http server он выключен.

```
cisco2960s(config)# no ip http server
```

Для того чтобы задать подсеть коммутатора, осуществлен вход в режиме конфигурирования используя команду ip default- gateway.

```
cisco2960s(config)# ip default-gateway 192.168.23.0
```

Для контроля событий настроен ACL для доступа к коммутатору только с определенных адресов. Для этого осуществлен вход в режим конфигурирования коммутатора и использована команда ip access-list standard TELNET, которая создаст стандартный access-list с именем TELNET. В access-list добавлены правила доступа с определенных адресов с помощью использования команд permit 192.168.23.1 и permit 192.168.23.15 и разрешить все остальное с помощью команды permit any.

```
cisco2960s(config)# ip access-list standard TELNET  
cisco2960s(config-std-nacl)# permit 192.168.23.1  
cisco2960s(config-std-nacl)# permit 192.168.23.15  
cisco2960s(config-std-nacl)# permit any  
cisco2960s(config-std-nacl)# exit
```

Чтобы правила работали, осуществлен вход в режим конфигурирования терминалов используя команду line vty 0 15 в командной строке коммутатора

и использована команда access-class TELNET in которая применяет данное правило на вход.

```
cisco2960s(config)# line vty 0 15  
cisco2960s(config-line)# access-class TELNET in
```

Для того, чтобы по истечении указанного времени соединение закрывалось задан таймаут неактивности используя команду exec-timeout 5 0.

```
cisco2960s(config-line)# exec-timeout 5 0  
cisco2960s(config-line)# exit
```

Чтобы производить мониторинг коммутационного оборудования включен протокол SNMP, для этого в режиме конфигурирования коммутатора создано сообщество с названием myRO для read only(RO) и myRW для read write(RW), используя команды snmp-server community myRO RO и snmp-server community myRW RW. Чтобы задать источник SNMP ловушки использована команда snmp-server source-interface informs Vlan1. Так же для того чтобы хост был доступен, ему разрешен доступ с помощью команд snmp-server host 192.168.23.1 myRO и snmp-server host 192.168.23.1 myRW.

```
cisco2960s(config)# snmp-server community myRO RO  
cisco2960s(config)# snmp-server community myRW RW  
cisco2960s(config)# snmp-server trap-source Vlan1  
cisco2960s(config)# snmp-server source-interface informs Vlan1  
cisco2960s(config)# snmp-server host 192.168.23.1 myRO  
cisco2960s(config)# snmp-server host 192.168.23.1 myRW  
cisco2960s(config)# exit
```

Далее конфигурация сохранена с помощью команды copy running-config startup-config или wri.

```
cisco2960s# copy running-config startup-config  
cisco2960s# wri
```

Для настройки протокола SNMPv3 настроена view, с использованием команды snmp-server view test internet included, где test это имя view, internet это oid-дерево и included это включение. После чего создана группа для view с использованием команды snmp-server group TESTGR v3 auth write test. После того как группа была создана, с использованием команды snmp-server

user TESTUSER TESTGR v3 auth md5 testpass создан пользователь. После чего файл конфигураций снова сохранен.

```
cisco2960s# configure terminal
cisco2960s(config)#snmp-server view test internet included
cisco2960s(config)#snmp-server group TESTGR v3 auth write test
cisco2960s(config)#snmp-server user TESTUSER TESTGR v3 auth md5 testpass
cisco2960s(config)#exit
cisco2960s# copy running-config startup-config
cisco2960s# wri
```

Для того, чтобы собирать логи использована команда «logging on», которая включает сбор логов. Помимо этого включена запись логов в буфер с использованием команды «logging buffered informational», с использованием команды «logging buffered 16386» задан размер буфера. Для того, чтобы программа мониторинга собирала логи, указан ip адрес компьютера, где установлена программа мониторинга, с использованием команды « logging 192.168.23.1».

```
cisco2960s(config)#logging on
cisco2960s(config)#logging buffered informational
cisco2960s(config)#logging buffered 16386
cisco2960s(config)#logging 192.168.23.1
```

Чтобы информационные сообщения записывались включена запись сообщений с использованием команды «logging 192.168.23.1» и заданы правила ACL, для доступа к терминалам.

```
cisco2960s(config)#logging trap informational
cisco2960s(config)#access-list 117 permit ip host 192.168.23.1 any
cisco2960s(config)#access-list 117 deny ip any any log-input
cisco2960s(config)#line vty 0 15
cisco2960s(config-line)#access-class 117 in
cisco2960s(config-line)#exit
cisco2960s(config)#access-list 117 permit icmp 192.168.23.1
cisco2960s(config)#access-list 117 deny icmp 192.168.23.1
cisco2960s(config)#access-list 117 permit any any
cisco2960s(config)# interface vlan 1
cisco2960s(config-if)#access-class 117 in
cisco2960s(config-if)#exit
cisco2960s(config)# exit
```

```
cisco2960s# copy running-config startup-config
```

```
cisco2960s# wri
```

После проделанной работы снова сохранен файл конфигураций с использованием команды `wri` или `copy running-config startup-config`.

ПРИЛОЖЕНИЕ Е

(обязательное)

Файл конфигурации для межсетевого экрана ССПТ-2

Был разработан файл конфигурации для коммутационного оборудования, межсетевого экрана ССПТ-2. [9]

Конфигурации для межсетевого экрана ССПТ-2 настроены через web интерфейс, для наглядности. Настройка конфигураций приведена ниже.

Для того чтобы произвести настройку межсетевого экрана ССПТ-2, необходимо в ОС Windows зайти в браузер нажав на него два раза левой кнопкой мыши, и в строке поиска прописан стандартный ip адрес межсетевого экрана, и нажата кнопка «Ввод». Появилось окно входа в web интерфейс межсетевого экрана ССПТ-2, которое показано на рисунке Е.1.



Рисунок Е.1- Окно входа в web интерфейс межсетевого экрана ССПТ-2

Далее в левом верхнем углу нажата кнопка «вход», после чего появилось окно ввода имени пользователя и пароля, которое показано на рисунке Е.2.

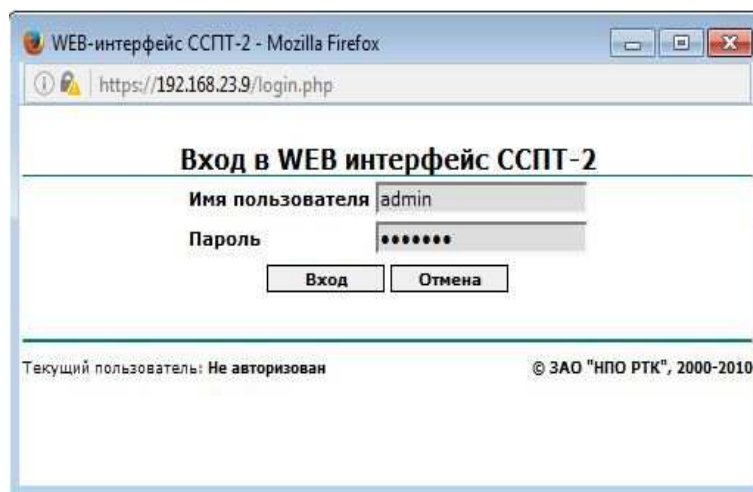


Рисунок Е.2 – Окно ввода имени пользователя и пароля

Введено имя пользователя и пароль после чего нажата кнопка «вход». В данном случае имя пользователя и пароль администратора, для настройки межсетевого экрана, так как он имеет полный доступ к межсетевому экрану. После нажатия вход, открылось главное меню межсетевого экрана, которое показано на рисунке Е.3.

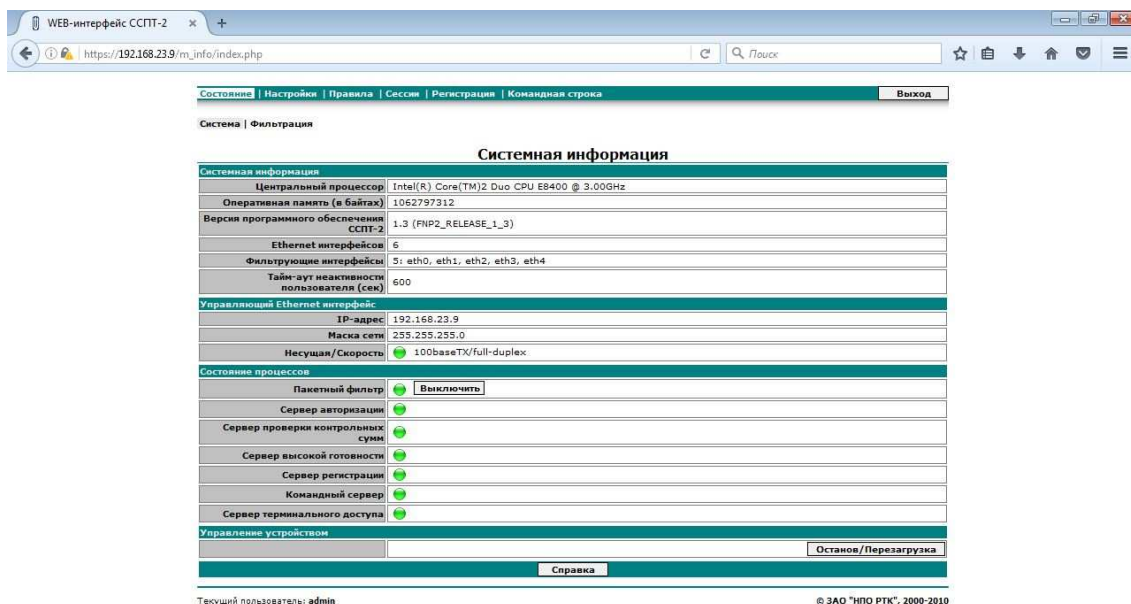


Рисунок Е.3- Главное меню межсетевого экрана ССПТ-2

Так как необходимо настроить конфигурацию, для того, чтобы можно было производить мониторинг межсетевого экрана, включена выгрузка системных сообщений Syslog. Чтобы включить выгрузку системных сообщений Syslog, выбрана вкладка «регистрация». После перехода по вкладке «регистрация», появилось окно «Регистрация:настройки», которое показано на рисунке Е.4.

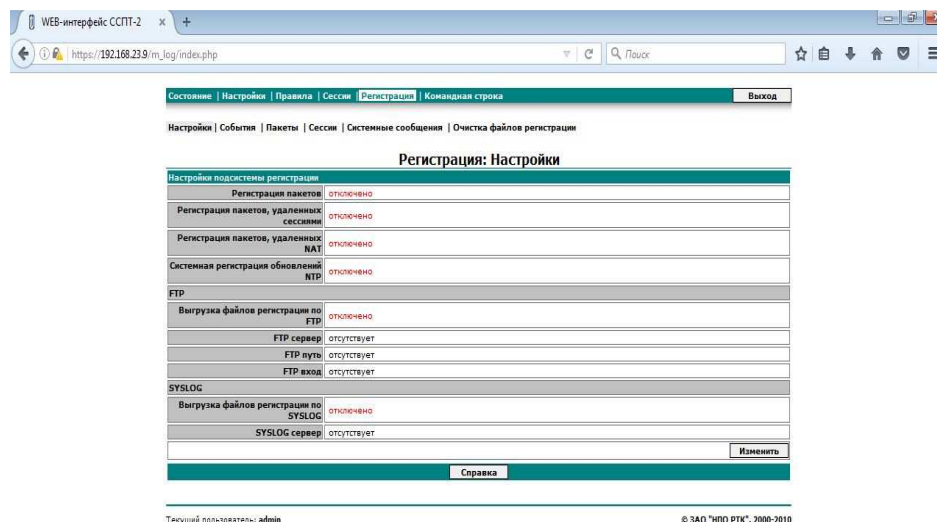


Рисунок Е.4 – Окно «Регистрация:настройки»

Для редактирования настроек в правом нижнем углу нажата кнопка «изменить», после чего появилось окно «редактирование настроек подсистемы регистрации», которое показано на рисунке Е.5.

WEB-интерфейс ССПТ-2 - Mozilla Firefox
https://192.168.23.9/m_log/sets_edit.php

Редактирование настроек подсистемы регистрации

Настройки подсистемы регистрации

Регистрация пакетов	☐
Регистрация пакетов, удаленных сессиями	☐
Регистрация пакетов, удаленных NAT	☐
Системная регистрация обновлений NTP	☐
Выгрузка файлов регистрации по FTP	☐
FTP сервер	отсутствует
FTP путь	отсутствует
FTP вход	отсутствует
FTP пароль	
FTP пароль (повторно)	
Выгрузка файлов регистрации по SYSLOG	☐
SYSLOG сервер	отсутствует

Сохранить Справка Отмена

Текущий пользователь: admin © ЗАО "НПО РТК", 2000-2010

Рисунок Е.5 – Окно «Редактирование настроек подсистемы регистрации»

Далее установлены флажки в полях «регистрация пакетов» и «выгрузка файлов регистрации по Syslog». В поле «Syslog сервер» прописан IP адрес получателя Syslog сообщений. Заполненная форма представлена на рисунке Е.6.

WEB-интерфейс ССПТ-2 - Mozilla Firefox
https://192.168.23.9/m_log/sets_edit.php

Редактирование настроек подсистемы регистрации

Настройки подсистемы регистрации

Регистрация пакетов	☒
Регистрация пакетов, удаленных сессиями	☐
Регистрация пакетов, удаленных NAT	☐
Системная регистрация обновлений NTP	☐
Выгрузка файлов регистрации по FTP	☐
FTP сервер	отсутствует
FTP путь	отсутствует
FTP вход	отсутствует
FTP пароль	
FTP пароль (повторно)	
Выгрузка файлов регистрации по SYSLOG	☒
SYSLOG сервер	192.168.23.1

Сохранить Справка Отмена

Текущий пользователь: admin © ЗАО "НПО РТК", 2000-2010

Рисунок Е.6 – Заполненная форма

После того как были заполнены необходимые поля, нажата кнопка «сохранить», и система осуществляет вывод информационного окна о системных событиях. Окно о системных событиях представлено на рисунке Е.7.

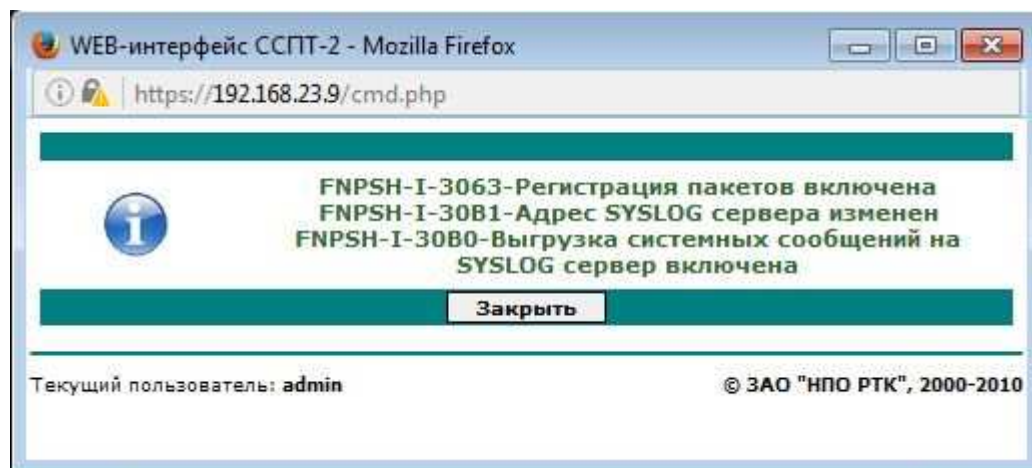


Рисунок Е.7 – Окно о системных событиях

Для того чтобы показать как работать через командную строку, я через командную строку web интерфейса ввел те команды, которые делают все то, что было проделано выше. Для этого в главном меню web интерфейса перешел в раздел «Командная строка». Для того чтобы включить выгрузку системных сообщений написана команда без кавычек «log export syslog enable» и нажата кнопка «выполнить». Демонстрация ввода данной команды показана на рисунке Е.8.

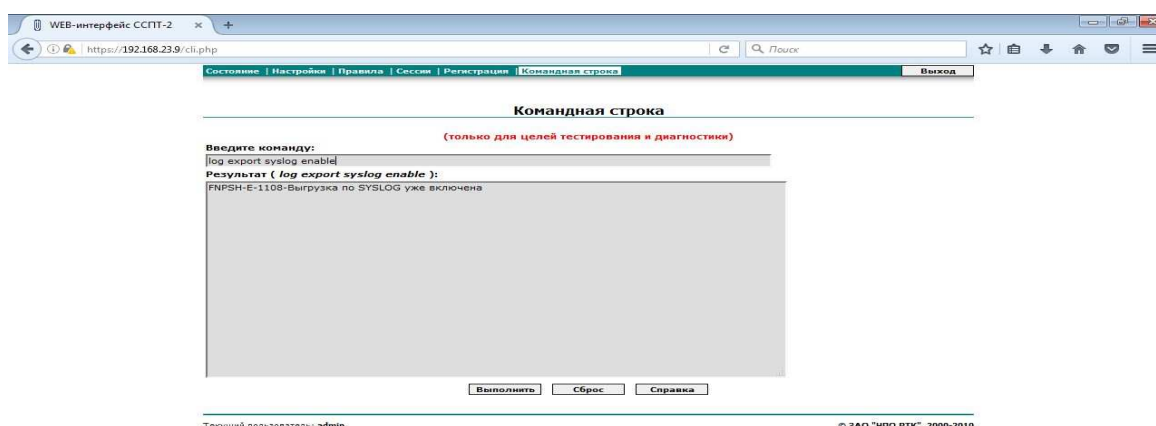


Рисунок Е.8 – Демонстрация ввода команды «log export syslog enable»

Для того чтобы задать адрес выгрузки системных сообщений написана команда без кавычек «log export syslog server 192.168.23.1» и нажата кнопка

«выполнить». После ввода данных команд, так же было выдано оповещение о статусе данных команд в окне «результат». Демонстрация ввода данной команды показана на рисунке Е.9.

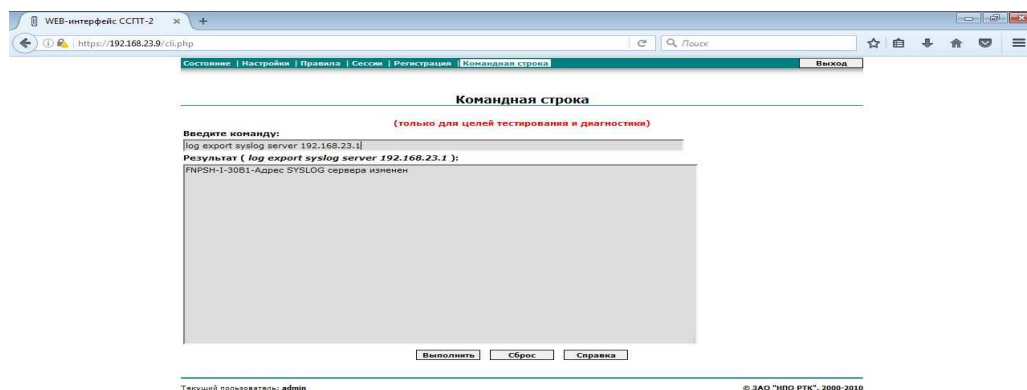


Рисунок Е.9 – Демонстрация ввода команды «log export syslog server 192.168.23.1»

ПРИЛОЖЕНИЕ Ж
(обязательное)
Порядок настройки системы мониторинга

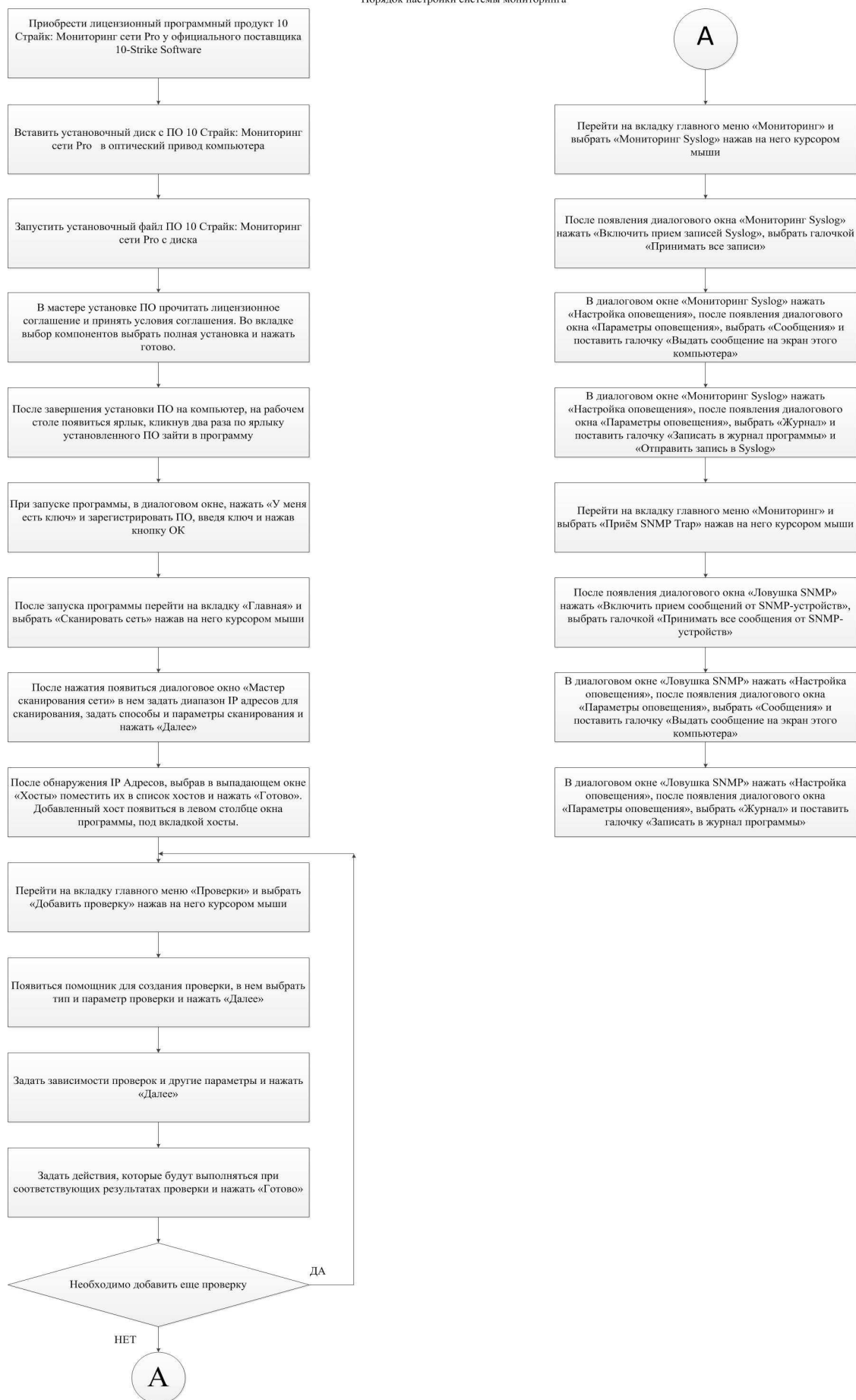


Рисунок Ж.1 – Порядок настройки системы мониторинга

ПРИЛОЖЕНИЕ И

(обязательное)

Структура информационного обмена при мониторинге сетевых компонентов

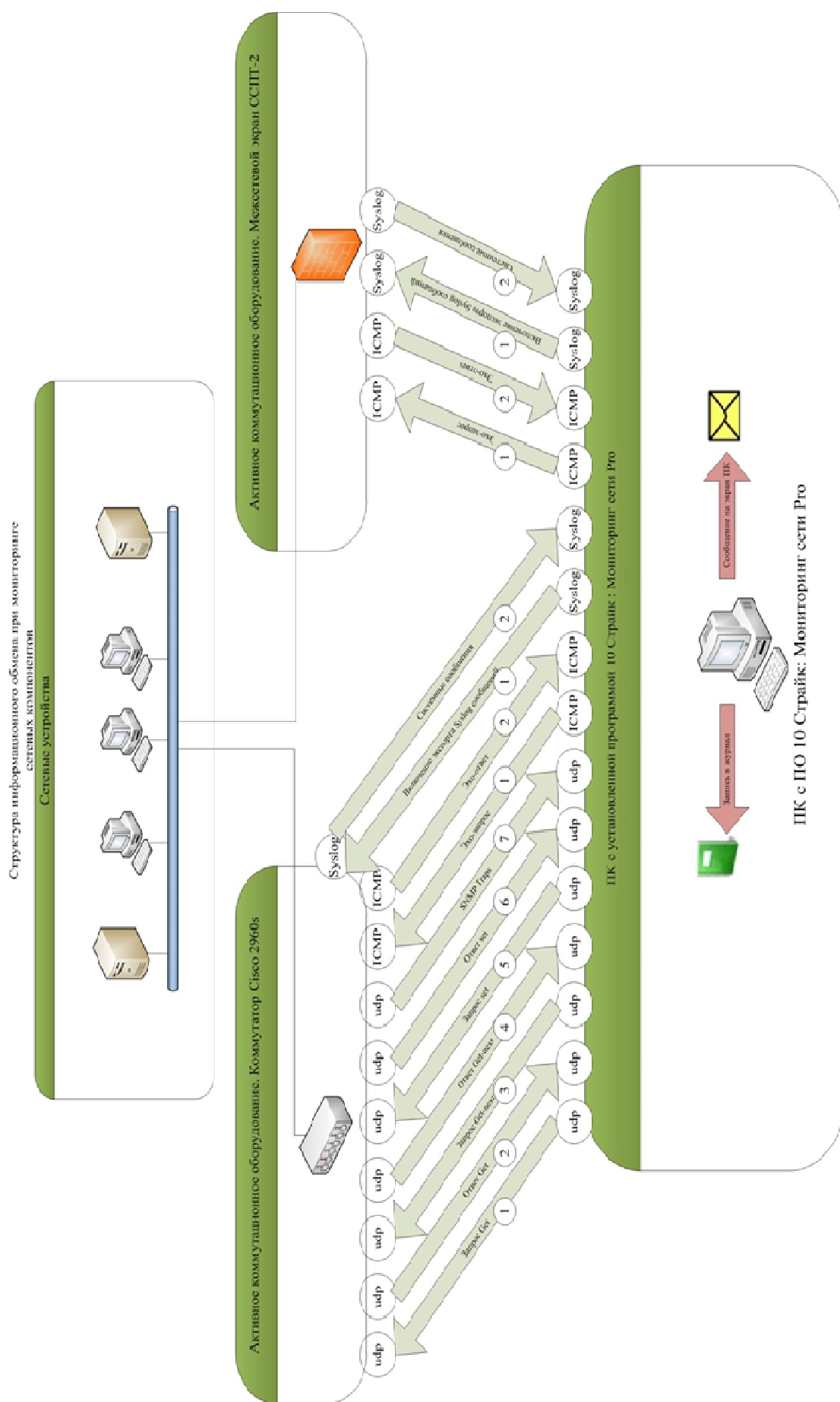


Рисунок И.1 – Структура информационного обмена при мониторинге сетевых компонентов

ПРИЛОЖЕНИЕ К
(обязательное)
Результат проверки системы «Антиплагиат»

ПРОТОКОЛ

проверки на оригинальность в системе «Антиплагиат.ВУЗ» выпускной квалификационной работы на тему «Система мониторинга сетевых компонентов в распределенной информационной системе персональных данных» студента 6 курса С.В. Посоркина направления подготовки 10.05.02 «Информационная безопасность телекоммуникационных систем». Специализация – разработка защищённых телекоммуникационных систем.

Скриншот результата проверки ВКР в системе «Антиплагиат.ВУЗ» представлен на рисунке К.1.

Руководитель ВКР: начальник отдела защиты информации НИКИРЭТ – филиал ФГУП ФНПЦ ПО «Старт» им. М.В. Проценко Мещеряков А.А.

Информация о документе:

Имя исходного файла: Диплом_Посоркин_С_В_на Антиплагиат.docx
Имя компании: Пензенский гос. Университет
Тип документа: Прочее
Имя документа: Группа 11ПТ1 ВКР Посоркин С.В.
Дата проверки: 29.12.2016 23:16
Модули поиска: Кольцо вузов, Интернет (Антиплагиат), Модуль поиска ЭБС "Лань", Университетская библиотека онлайн, Модуль поиска ЭБС БиблиоРоссика, Диссертации и авторефераты РГБ, Пензенский гос. Университет

Текстовые статистики:

Индекс читаемости: сложный
Неизвестные слова: в пределах нормы
Макс. длина слова: в пределах нормы
Большие слова: в пределах нормы

Оригинальные блоки: 90,93%

Заимствованные блоки: 9,07%

Заимствование из "белых" источников: 0%

Итоговая оценка оригинальности: **90,93%**

Рисунок К.1 – Результат проверки системы «Антиплагиат»

«___»_____ 20__г.

_____ А.А. Мещеряков