Министерство образования Красноярского края
Краевое государственное бюджетное профессиональное образовательное учреждение
«Красноярский колледж радиоэлектроники и информационных технологий»

ОТЧЕТ ПО ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ

09.02.02 Компьютерные сети
код и наименование специальности

Главное управление ФССП России по Красноярскому краю
место прохождения практики

ПМ.03 эксплуатация объектов сетевой инфраструктуры
код и наименование профессионального модуля и междисциплинарного курса

Студент 9КС-1.19, 1450 _____ И.В. Сецко
номер группы, зачетной книжки | подпись, дата | инициалы, фамилия

Руководитель от предприятия _____ В.В. Латышев
подпись, дата | инициалы, фамилия

М.П.

оценка _____

Руководитель от колледжа _____ Харитонова Е.В.
подпись, дата | инициалы, фамилия

Красноярск, 2022 г.

АННОТАЦИЯ

Данный документ является пояснительной запиской к производственной практике ПМ 0.3 «эксплуатация сетевого оборудования».

Целью практики является приобретение навыков работы с эксплуатацией сетевого оборудования.

Пояснительная записка состоит из четырех основных разделов:

1. изучение сетевой инфраструктуры предприятия
2. обеспечение сетевой безопасности;
3. мониторинг локальной сети организации;
4. разработка предложения по развитию инфраструктуры сети.

В первом разделе описываются сегменты сети, а также прилегающее оборудование.

Во втором разделе описывается набор утилит, используемый для безопасности в сети.

В третьем разделе рассказывается о утилите для мониторинга сети.

В четвертом разделе представлено предложение по развитию инфраструктуры сети.

Пояснительная записка состоит из 26 страниц, 15 рисунков, 2 приложений.

ВВЕДЕНИЕ

В начале 1980-х годов персональные компьютеры стали объединять в сети для обмена данными и совместного использования файлов и ресурсов. К середине 1980-х годов эти сети становятся крупными и сложными. Для управления ими создаются отделы информационного обеспечения.

Управление сетью (Network management) – целенаправленное воздействие на сеть, осуществляемое для организации её функционирования по заданной программе. Оно включает следующие процедуры:

1. включение и отключение системы, каналов передачи данных, терминалов;
2. диагностика неисправностей;
3. сбор статистики;
4. подготовка отчётов и т.п.

С точки зрения модели OSI управление сетью подразделяется на управление:

1. конфигурацией;
2. отказами;
3. безопасностью;
4. трафиком;
5. учётом.

Традиционные методы управления основаны на использовании правил. Они предписывают системе управления в компьютерной сети предпринимать определённые действия (например, выдать предупреждающее сообщение на управляющую консоль) при наступлении определённых событий (превышение интенсивностью трафика заранее определённого порогового значения и др.).

Задачей данной практике является изучение ЛВС и ее назначения.

Целями данной практике являются раскрытие изученной сети, ее администрирование, способы мониторинга за ней, раскрытие ее безопасности, структуры, а также предложение по развитию ее.

1 Изучение сетевой инфраструктуры предприятия (объекта практики).

1.1 Общие сведения

На практике была изучена ЛВС и приняты меры по устранению возможных сбоев; были выбраны способы решения задач профессиональной деятельности; обеспечен сбор данных для анализа использования и функционирования программно-технической части компьютерной сети; информация о способах профилактики сети, а также ее компонентах; была обеспечена защиту при подключении к сети «Интернет».

Локальная вычислительная сеть (ЛВС) в информационном отделе ФССП России нужна для совместного использования ресурсов (принтер, файловое хранилище, обмен данными, общий доступ в Интернет и помощь или консультация сотрудникам по проблемам касающиеся информационных технологий.)

1.2 Наименование сегментов сети

ЗЛВС (закрытая локально вычислительная сеть) – общая сеть сотрудников предприятия, сеть для сотрудников кадрового и финансового отделов, ни разделены в отдельные VLAN с целью их выделения;

ДМЗ ЗЛВС (демилитаризованная зона) – в любой сети подразумевается под собой общедоступные сервисы, в частности туда входят: общедоступные для ЗЛВС файлообменный ресурс, сервер терминального интернета;

ОЛВС (открытая ЛВС) – предназначенная для расположения абонентских станций, предназначенных для организации открытого доступа в сеть интернет;

ДМЗ ОЛВС (демилитаризованная ОЛВС) – предназначена для размещения общедоступных сервисов (для ЗЛВС тоже): прокси, файлообменый сервис.

Элементом сети выступающем в роли программного шлюза для организации доступа в интернет является аппаратный межсетевой экран «Diamond».

В каждом из территориальных отделов судебных Приставов оборудована ЛВС, они все являются частью ЗЛВС в основе, которой лежит маршрутизатор «Cisco 8e1».

Соответственно ЛВС каждого отдела включает в себя VLAN для размещения серверного оборудования, VLAN для размещения компьютеров пользователя локальной сети отдела и VLAN для размещения VOIP телефонов.

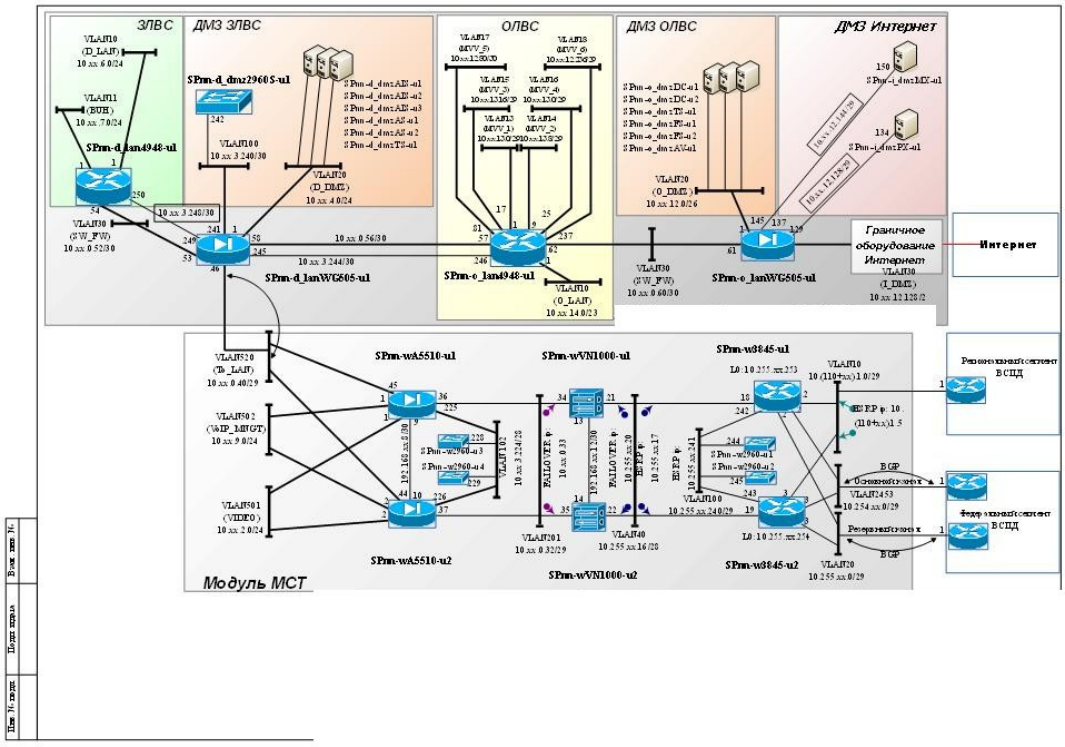
Защита и шифрование данных между территориальными отделами и управления осуществляется при помощи программного-аппаратного комплекса VipNet.

Организация канала связи между ЛВС управления и ЛВС территориальных отделов возложена на региональный сегмент ВСПД организованный при помощи 2 (основного и резервного) каналов связи. Подобным образом организована связь между ЛВС управления и федеральным сегментом ВСПД.

Для разграничения доступа между сегментами ЛВС, используются маршрутизатор cisco 345, межсетевые экраны cisco 5510, коммутаторы cisco 2960.

1.3 Анализ сети предприятия

Сеть выполнена опираясь на быстродействие, функционал, повсеместную работу с другими отделами, а также хорошо защищена (рисунок А1).



На каждом ПК в организации установлена специально разработанная операционная система «ГосЛинукс», что делает работу в сети безопасной и осуществляет пристальную сохранность важным данным, базам данных и.т.д. Также используются межсетевые экраны, которые дают защиту от нежелательного сетевого доступа извне. Программный комплекс VipNet, а также его оборудование надежно шифрует данные находящиеся в базах данных. Маршрутизаторы обеспечивают высокую скорость принятия и передачи данных. Серверное помещение соответствует всем ГОСТам. Также используется ip-телефония, для удобной работы с другими отделами и связи граждан по вопросам к судебным приставам (рисунок Б1).

1.4 Анализ оборудования и программного обеспечения предприятия

Оборудование состоит из: маршрутизаторов «cisco 345» (рисунок 1); межсетевых экранов «cisco 5510» (рисунок 2), «Diamond»; программного комплекса VipNet и его прикладного оборудования (рисунок 3); Операционной системы ГосЛинукс; антивирусом Kaspersky Security Center; а также при помощи Ensemble Sync Director осуществляется мониторинг сети.

Рисунок 1 - Маршрутизатор «Cisco 345»

Рисунок 2 - Межсетевой экран «Cisco 5510»

Рисунок 3 - межсетевой экран «VipNet»

1.5 Программные приложения и услуги

Сетевой инфраструктуре требуются соответствующие программные приложения или службы, которые должны быть установлены на компьютерах и регулировать трафик данных. В большинстве случаев службы системы доменных имен (DNS) также являются протоколом обмена динамической конфигурации хоста (DHCP) и службы Windows (WINS), которые являются частью базового пакета услуг. Эти приложения должны быть настроены соответствующим образом и постоянно быть доступными.

Для подключения компьютеров к сети Интернет необходимы дополнительные устройства, предпочтительно в виде шлюзов безопасности (брандмауэров). Если нужны беспроводные устройства связи, то в качестве соответствующих интерфейсов требуются точки беспроводного доступа. Если пользователь хочет получить быстрый обзор всех устройств в сети, он может сделать это со специальными IP-сканерами.

Пользователи также могут получить исчерпывающий обзор всех объектов в своей собственной сети с помощью службы каталогов Active Directory. Здесь все хранится в объектах, связанных с сетью, например принтеры, модемы, пользователи или группы.

В сети предприятия используются такие приложения как внутренняя почта для связи между сотрудниками или массовой рассылки важной

информации, касперский для защиты устройств сети, 1с используемый в качестве базы данных (рисунок 4), и ряд других программ и услуг разработанных специально для ФССП.

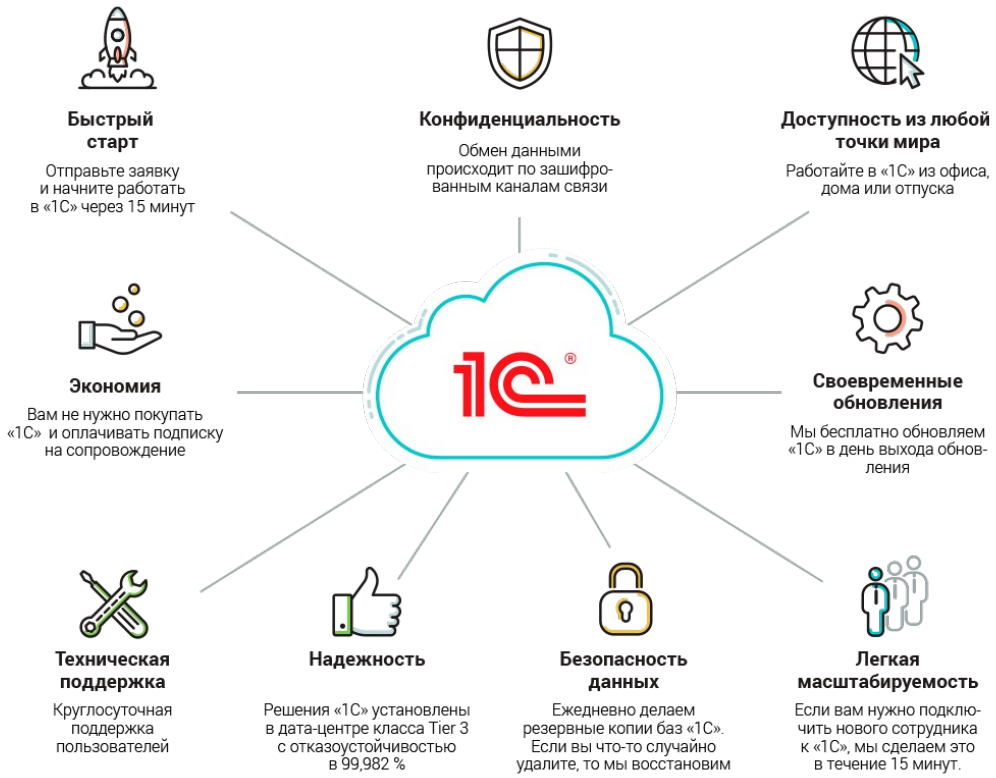


Рисунок 4 - 1с

2 Обеспечение сетевой безопасности

2.1 Администрирование учетных записей и групп в сети

Учетные записи есть, как и локальные так и имеются базы данных. При помощи учетных локальных записях разграничивается доступ к ведомственным файлообменным серверам. Учетным записям определенного структурного подразделения предоставляется доступ как к общедоступному файлообменному серверу, так и к серверам ограниченной доступности в зависимости от структурного подразделения.

Из-за организации, в которой проходил практику часть материала не возможно предоставить, в связи с подписанием бумаг о неразглашении информации во всеобщий доступ, поэтому для примера часть материала будет взята из интернета.

На рисунке ниже показана примерная работа файлообменного сервера, тоесть есть определенного количество серверов, которые доступны ограниченному числу человек в зависимости от отдела (рисунок 4).

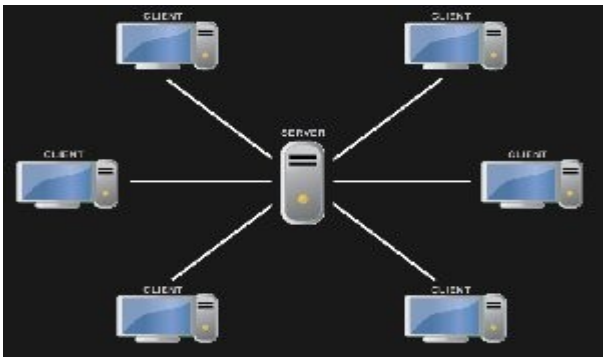


Рисунок 5 - примерная работа файлообменого сервера

2.2 Организация безопасного доступа к сети программными средствами операционных систем

Доступ к интернету и рабочим сетям осуществляется через «белый список», а именно подразумевает доступ к набору интернет сайтов, необходимых для осуществления деятельности сотрудников (рисунок 5). В

случае необходимости неограниченного доступа в сеть интернет используются специальные абонентские станции, находящиеся в отдельном сегменте сети.

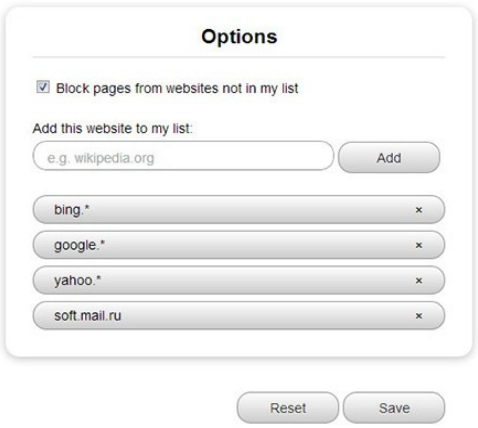


Рисунок 6 - пример работы белого списка

2.3 Обеспечение защиты от несанкционированного доступа к информации

Для обеспечения защиты от несанкционированного доступа к информации у ФССП используется ГосЛинукс, в котором не имеются права администратора у обычных сотрудников и быть не может. Функции безопасности, заложенные в операционной системе, позволят обрабатывать персональные данные без дополнительных средств защиты информации, а также применять ЭЦП (электронно цифровую подпись) для издания документов в электронном виде (рисунок).

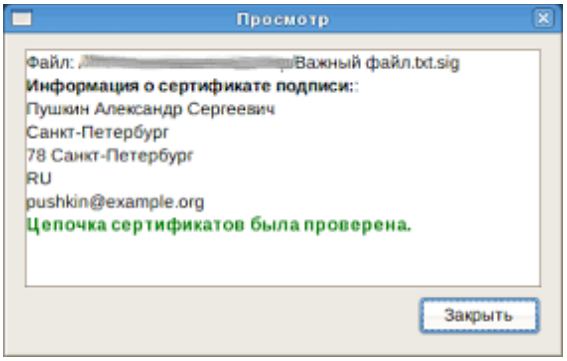


Рисунок 7 - проверка электронной подписи

2.4 Обеспечение безопасности межсетевого воздействия

Для обеспечения безопасности межсетевого воздействия используются отечественные межсетевые экраны «Diamond» (рисунок 7).

Рисунок 8 - Межсетевой экран «Diamond»

Назначение

Многофункциональный комплекс сетевой защиты является мощным инструментом по фильтрации сетевого трафика в контролируемой сети, позволяя задавать любые правила фильтрации, также позволяет обеспечить защиту конфиденциальной информации при передаче ее по общественным сетям.

Преимущества

«Diamond VPN/FW» легко интегрируется с системой контроля доступа «Diamond ACS», что позволяет осуществлять централизованное управление и контроль работы устройства из любой точки сети через единый графический интерфейс. МКСЗ «Diamond VPN/FW» содержит средства контроля за целостностью своей программной части, утилиты по ее экстренному восстановлению и созданию резервных копий.

Также используется программный комплекс «VipNet» (рисунок 8).

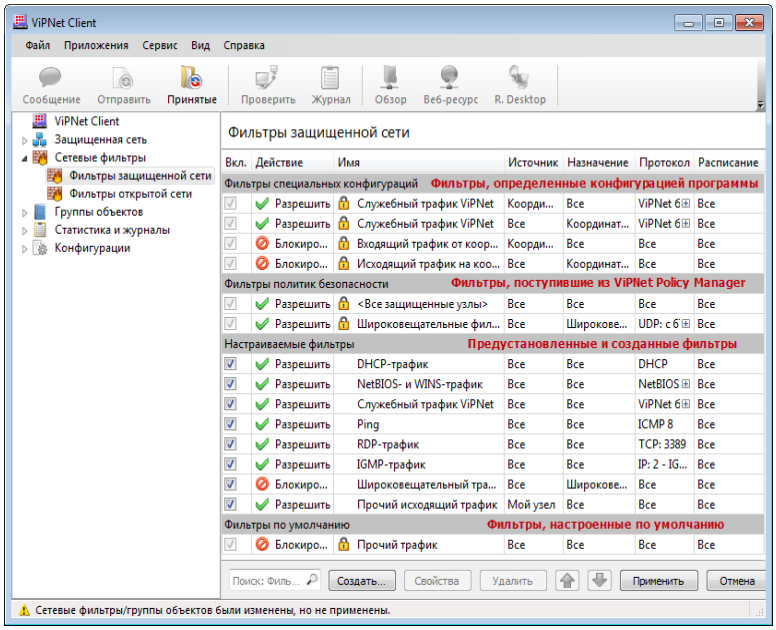


Рисунок 9 - пример работы VipNet клиента

Соединение с ресурсами, сервисами, а также другими пользователями осуществляется через каналы, функционирующие по принципу «точка-точка». Это позволяет надежно защитить информацию от других пользователей, в том числе внутри корпоративной сети. Шифрование трафика защитит работу с внутренними ресурсами и сервисами вашей организации при передаче данных через Интернет. ViPNet Client поддерживает работу на виртуальных машинах.

Преимущества

1. Высокая производительность шифрования и фильтрации трафика позволяет в реальном времени осуществлять защиту трафика служб голосовой и видеосвязи в сетях TCP/IP, а также обеспечивать одновременную работу с ресурсами разных сегментов корпоративной сети.

2. Равный доступ к ресурсам корпоративных информационных систем независимо от места и способа подключения пользователя к телекоммуникационной сети (при использовании решения ViPNet Network Security).

3. Защита канала не влияет на работу сторонних приложений на компьютере пользователя.

4. Ключи шифрования, политики безопасности и обновления ПО ViPNet доставляются на компьютер через надежный защищенный канал.

2.5 Осуществление антивирусной защиты ЛВС

Осуществление антивирусной защиты производится антивирусом Kaspersky Security Center (рисунок 9).

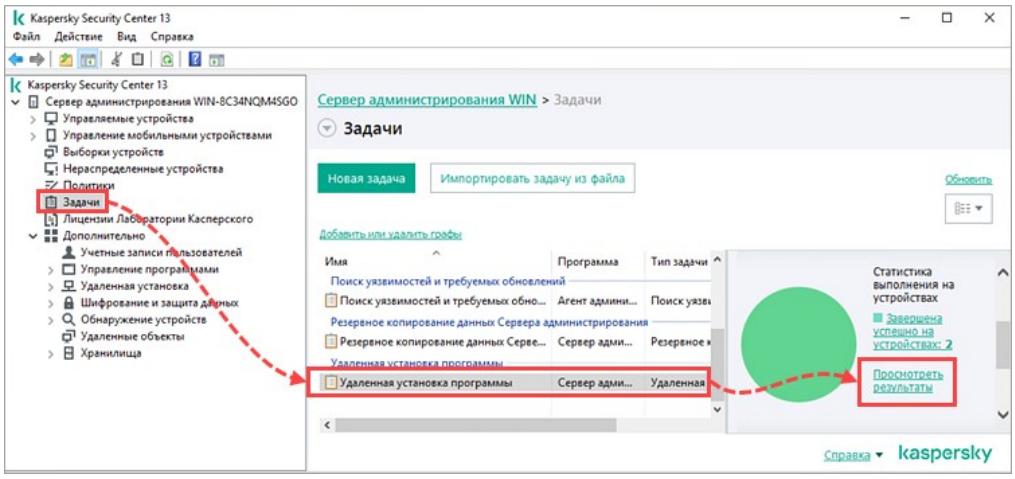


Рисунок 10 - пример работы антивируса

Kaspersky Security Center упрощает управление безопасностью и IT-системами. Гибкая, масштабируемая консоль, доступная в том числе в виде веб-версии. Она обеспечивает всестороннее управление IT-системами и средствами безопасности и облегчает распределение обязанностей между администраторами.

Kaspersky Security Center предлагает следующие преимущества:

1. Мощная консоль управления с дополнительным гибким веб-интерфейсом, доступным в любом месте с любого стационарного или мобильного устройства;

2. Возможность просматривать параметры безопасности и управлять защитой во всей корпоративной среде, включая облачные, физические и виртуальные машины, а также мобильные устройства;

3. Простое развертывание и управление безопасностью с помощью готовых к использованию унифицированных политик.

Неважно, сколько у вас рабочих станций (пятьдесят или пятьдесят тысяч) и какая инфраструктура (централизованная, распределенная или смешанная) – Kaspersky Security Center позволяет без лишних усилий устанавливать, настраивать и администрировать средства комплексной защиты.

2.6 Обеспечение своевременного копирования, архивирования и резервирования данных

Отдельного ПО у ФССП как такого не предназначено. Осуществляется инкрементное резервное копирование при помощи операционной системы ГосЛинукс. Инкрементная резервная копия - это копия всех данных базы данных, которые изменились со времени последней успешной операции полного резервного копирования. Ее называют также кумулятивной резервной копией, поскольку каждая следующая инкрементная резервная копия будет содержать информацию всех предыдущих. Предшественником инкрементной резервной копии всегда является последняя успешная полная резервная копия того же объекта (рисунок 10).

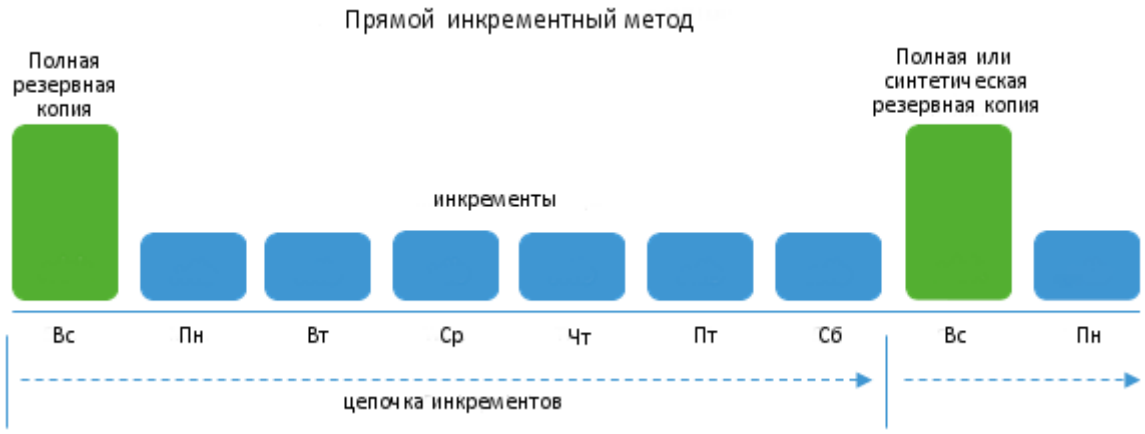


Рисунок 11 - наглядный рисунок, демонстрирующий этот способ

Все это сохраняется на файлообменный сервер, предназначенный для хранения резервных копий, создается раз в неделю полная резервная копия, раз в день создается неполная резервная копия, а именно новые настройки.

3

Мониторинг сети

Мониторинг сети осуществляется при помощи Ensemble Sync Director (рисунок 11).

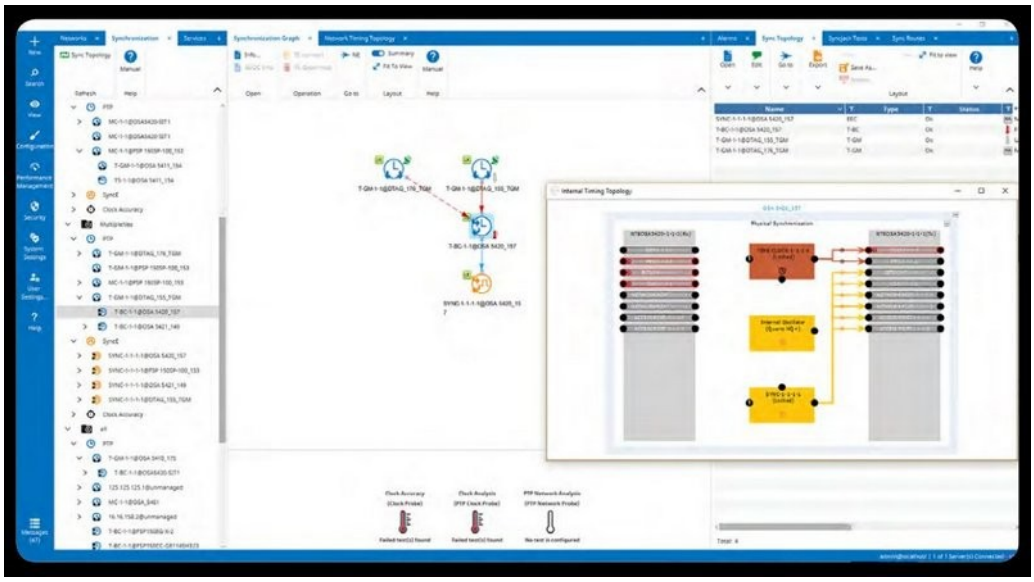


Рисунок 12 - пример работы в Ensemble Sync Director

Ensemble Sync Director - это передовая платформа управления для распределения и обеспечения синхронизации для сетевых элементов синхронизации частоты, фазы и времени. По мере роста важности синхронизации и точного времени во многих инфраструктурных сетях централизованная видимость и управление этой критически важной средой синхронизации становятся необходимыми для работы сети. Реализованный в соответствии с архитектурой клиент-сервер, Ensemble Sync Director обеспечивает гибкость, доступность, масштабируемость и производительность, необходимые для удовлетворения растущих потребностей в синхронизации сетей и приложений. Интуитивно понятное приложение графического интерфейса пользователя «точка-щелчок» в сочетании с выделением ресурсов на основе мастеров устраняет сложность и, следовательно, обеспечивает экономичную работу сетей синхронизации. Мониторинг топологии синхронизации и изменений состояния позволяет сетевым операторам инициировать соответствующие действия.

4 Разработка предложений по развитию инфраструктуры сети

Предлагаю организовать мониторинг сети при помощи системы «Nagios» (рисунок 12)

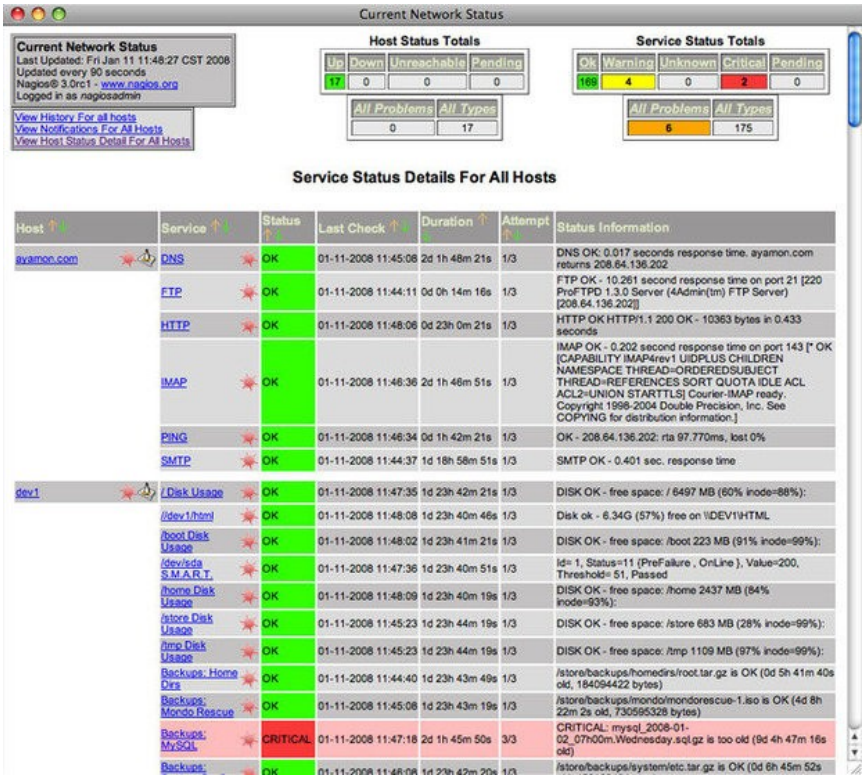


Рисунок 13 - интерфейс клиента Nagios

Nagios — это состоявшаяся программная система для мониторинга сети, которая уже многие годы находится в активной разработке. Написанная на языке C, она позволяет делать почти все, что может понадобится системным и сетевым администраторам от пакета прикладных программ для мониторинга. Веб-интерфейс этой программы является быстрым и интуитивно понятным, в то время его серверная часть — чрезвычайно надежной..

Как и Cacti, очень активное сообщество поддерживает Nagios, поэтому различные плагины существуют для огромного количества аппаратных средств и программного обеспечения. От простейших ping-проверок до интеграции со сложными программными решениями, такими как, например,

написанным на Perl бесплатным программным инструментарием WebInject для тестирования веб-приложений и веб сервисов. Nagios позволяет осуществлять постоянный мониторинг состояния серверов, сервисов, сетевых каналов и всего остального, что понимает протокол сетевого уровня IP. К примеру, вы можете контролировать использование дискового пространства на сервере, загруженность ОЗУ и ЦП, использования лицензии FLEXlm, температуру воздуха на выходе сервера, задержки в WAN и Интеренет-канале и многое другое.

Очевидно, что любая система мониторинга серверов и сети не будет полноценной без уведомлений. У Nagios с этим все в порядке: программная платформа предлагает настраиваемый механизм уведомлений (работает в качестве домена (фонового процесса) на выделенном сервере, периодически отправляя ICMP запросы на хост мониторинга. Полученная информация обрабатывается на сервере и отображается администратору в рамках WEB – интерфейса.) по электронной почте, через СМС и мгновенные сообщения большинства популярных Интернет-мессенджеров, а также схему эскалации, которая может быть использована для принятия разумных решений о том, кто, как и при каких обстоятельствах должен быть уведомлен, что при правильной настройке поможет вам обеспечить многие часы спокойного сна (рисунок 13).

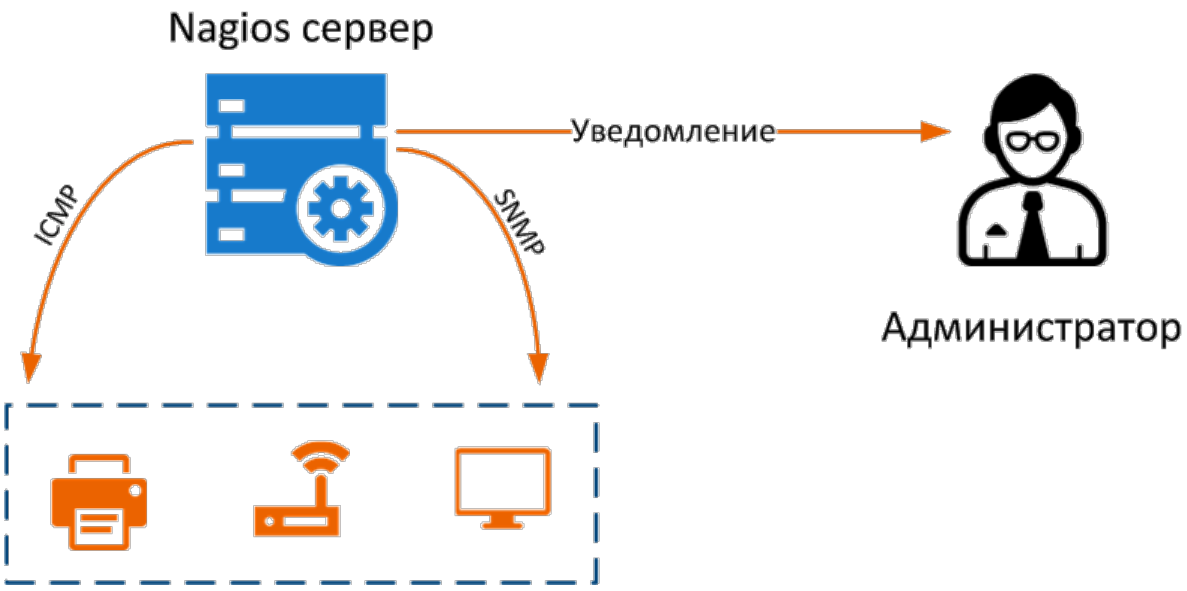


Рисунок 14 - принцип работы уведомлений Nagios

А веб-интерфейс может быть использован для временной приостановки получения уведомлений или подтверждения случившейся проблемы, а также внесения заметок администраторами.

Кроме того, функция отображения демонстрирует все контролируемые устройства в логическом представлении их размещения в сети, с цветовым кодированием, что позволяет показать проблемы по мере их возникновения.

Недостатком Nagios является конфигурация, так как ее лучше всего выполнять через командную строку, что значительно усложняет обучение новичков. Хотя люди, знакомые со стандартными файлами конфигурации Linux/Unix, особых проблем испытать не должны.

Возможности Nagios огромны, но усилия по использованию некоторых из них не всегда могут стоить затраченных на это усилий. Но преимущества системы раннего предупреждения, предоставляемые этим инструментом для столь многих аспектов сети, сложно переоценить.

ЗАКЛЮЧЕНИЕ

В данной работе была изучена локально вычислительная сеть ФССП России по Красноярску и Красноярскому краю.

Структура, сетевая операционная система, кабельная система и локально вычислительная сеть были изучены, обеспечивают совместную обработку информации, совместное использование файлов, централизованное управление компьютерными устройствами, контроль за доступом к информации, централизованное копирование всех данных и совместный доступ в интернет.

Конфигурация сети, которая удовлетворяет критериям быстродействия, надежности, информационной безопасности, отказоустойчивости, расширяемости сети и стоимости.

БИБЛИОГРАФИЧЕСКОЕ ОПИСАНИЕ

1. Кузин, А.В. Компьютерные сети: учеб. пособие / А.В. Кузин, Д.А. Кузин. – 4-е изд. – М.: ФОРУМ: ИНФРА-М, 2017. – 190 с.

2. Максимов, Н.В. Компьютерные сети: уч. Пособие для студентов учреждений среднего проф. образования. /Н.В. Максимов,
И.И. Попов – М.: ФОРУМ, 2015, - 464 с.

3. Новожилов, Е.О. Компьютерные сети: учеб. пособие для студ. Учреждений сред. Проф. образования / Е.О. Новожилов, О.П. Новожилов. – 5-е изд. – М.: издательский центр «Академия», 2017. – 224с.

4. Олифер, В. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов.5-е изд. [Текст] /В.Олифер – С-Пб.: Питер, 2016, – 992 с.

5. Пескова, С.А. Сети и телекоммуникации: учеб. пособие для студ. высш. учеб. заведений. – 3-е изд. [Текст] / С. А. Пескова, А. В. Кузин,
А. Н. Волков – М.: Издат. центр «Академия», 2012, – 352 с.

ПРИЛОЖЕНИЕ А

(информационное)

Схема сети

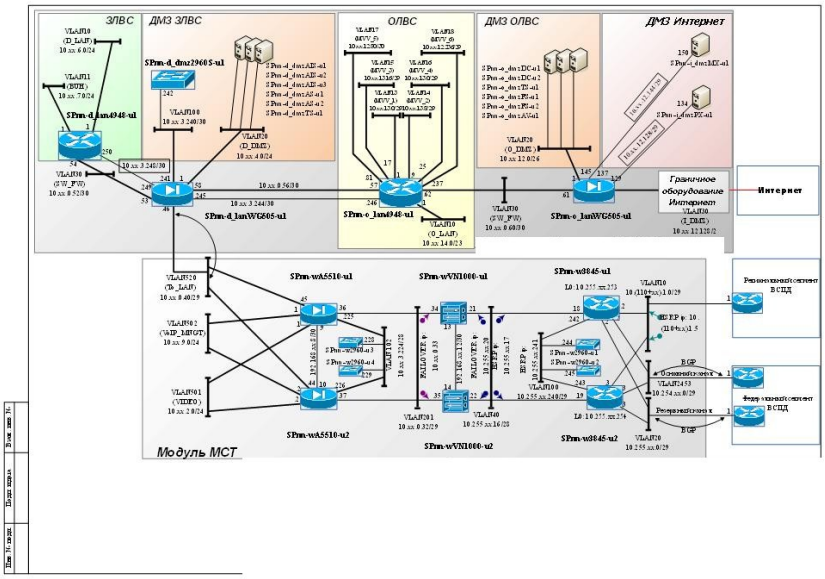


Рисунок А.1

ПРИЛОЖЕНИЕ Б

(информационное)

Схема ведомственной телефонной сети

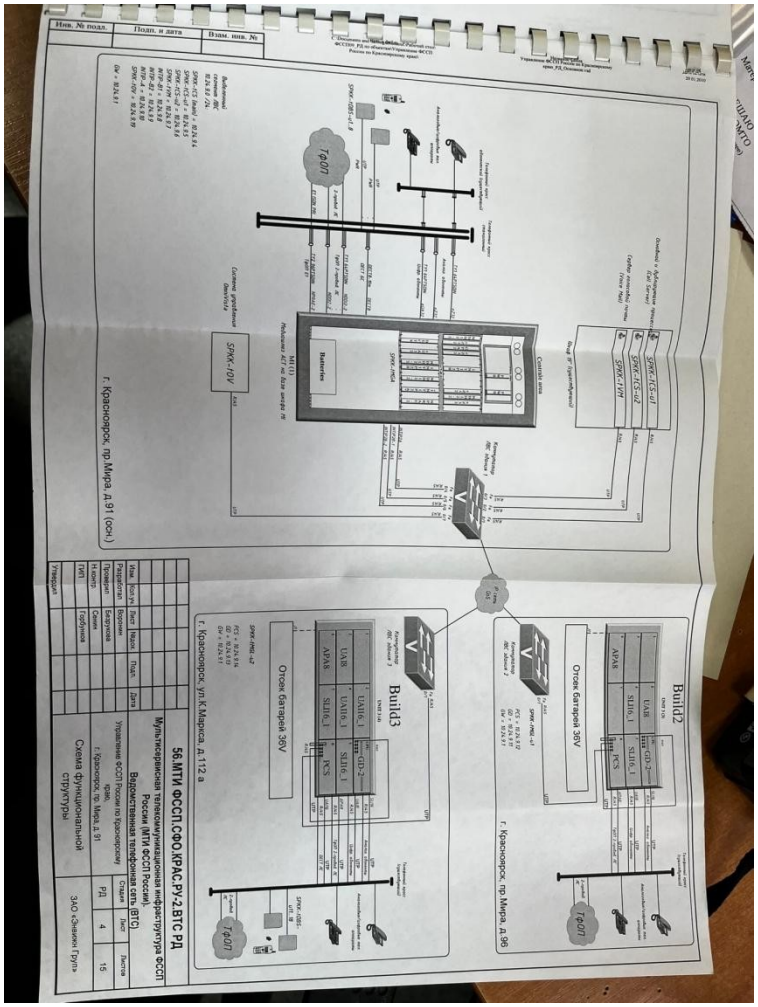


Рисунок Б.1