ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение высшего образования

«Иркутский государственный университет путей сообщения»

Сибирский колледж транспорта и строительства

Методические рекомендации по проведению практических работ

МДК 03.01 ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

для специальности
09.02.06 Сетевое и системное администрирование

базовая подготовка среднего профессионального образования

Иркутск 2023

РАССМОТРЕНО:
ЦМК специальности 09.02.06 «Сетевое и системное администрирование»

Председатель ЦМК:
Саквенко Т.В.
Протокол №9 от « 23 » мая 2023 г.

Разработчик: Панина В.Е. преподаватель Сибирского колледжа транспорта и строительства ФГБОУ ВО «Иркутский государственный университет путей сообщения».

Практическое задание №1

Цель: Научиться оформлять документацию для компьютерной сети.

Ход работы

Задание 1.

Начертить при помощи MS Visio план этажа по варианту.

Задание 2.

Расположить в каждом кабинете рабочие места с ПК и определить местоположение информационных розеток.

Задание 3.

Выбрать помещение для серверной комнаты. Обосновать выбор.

Задание 4.

Расположить сетевое оборудование в серверной комнате и, если это необходимо, в других помещениях этажа.

Задание 5.

Схематично изобразить протяжку проводов от серверной комнаты до каждой информационной розетки.

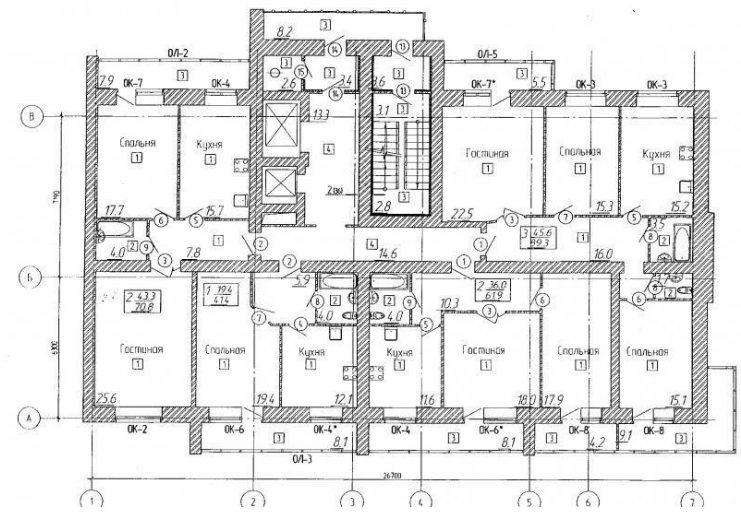
Задание 6.

Написать легенду для плана этажа, обозначив все оборудование.

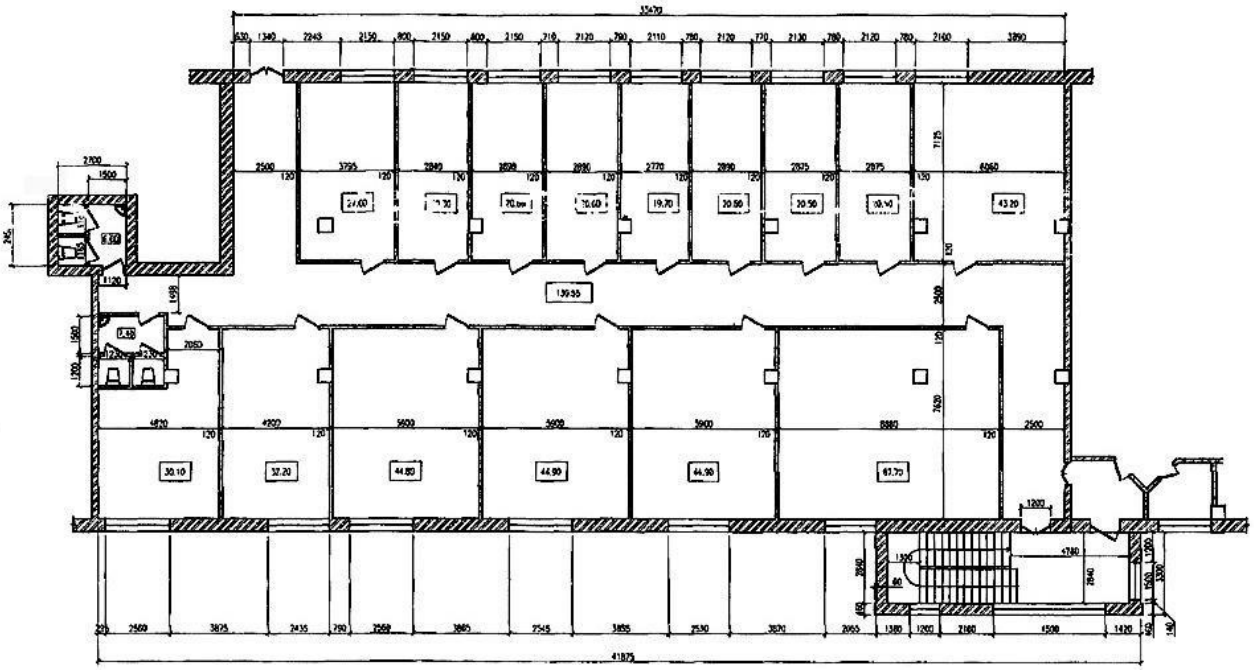
Задание 7.

Рассчитать стоимость протяжки такой сети, включив: кабель, коннекторы, кабель-канал, информационные розетки, сетевое оборудование.

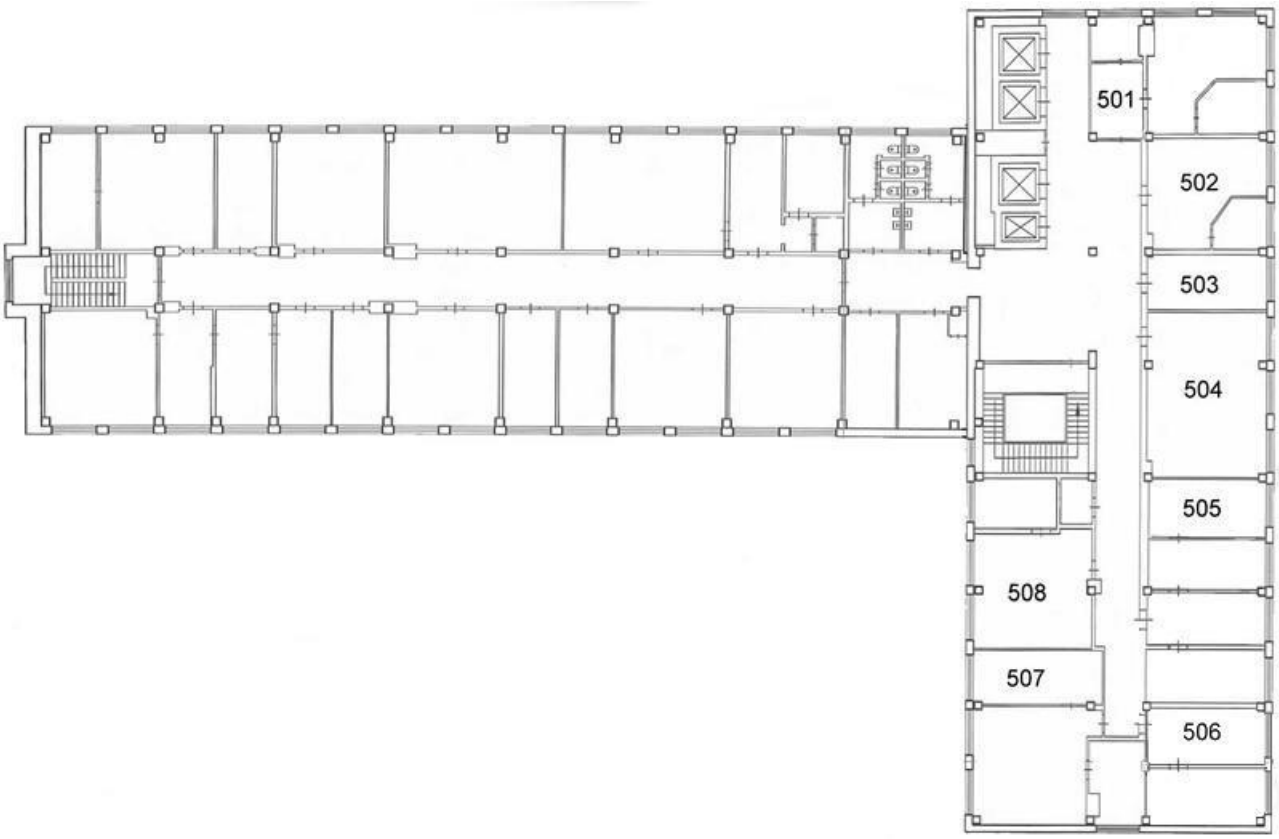
Вариант 1.



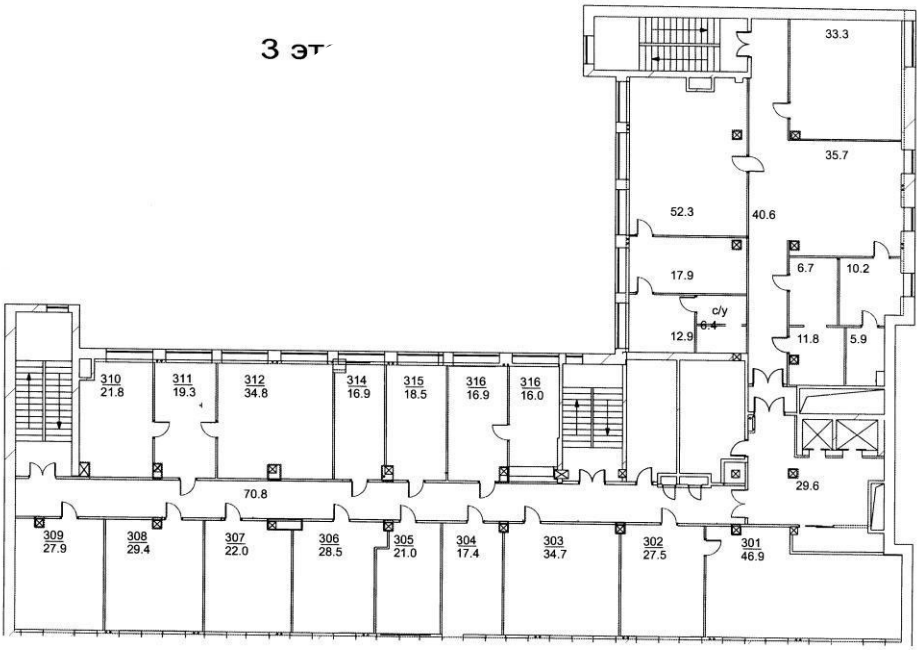
Вариант 2.



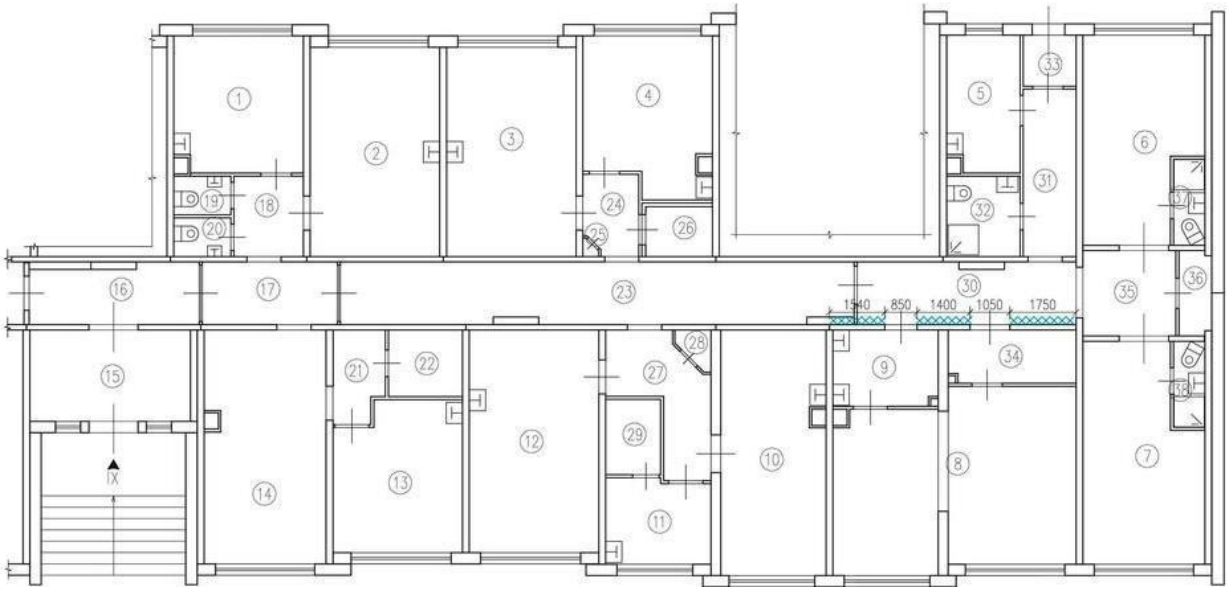
Вариант 3.



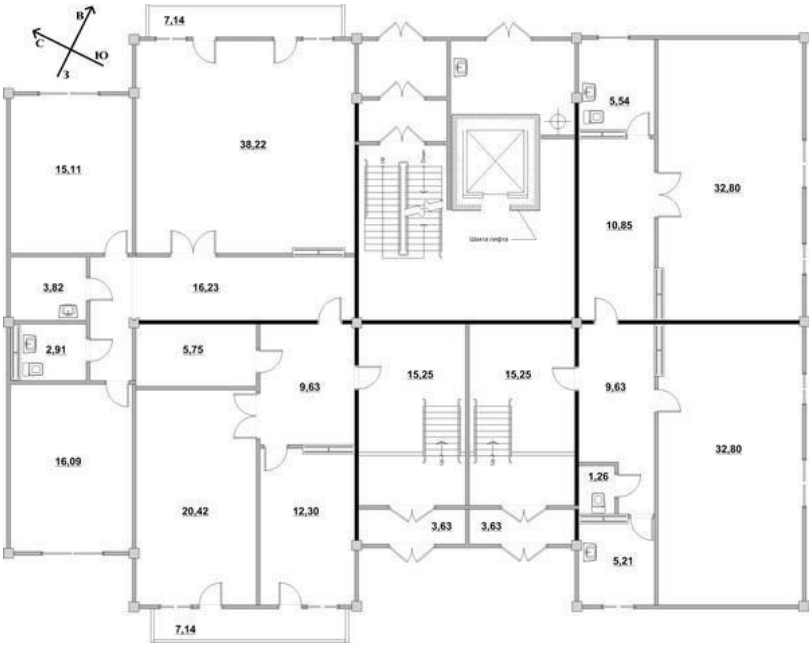
Вариант 4.



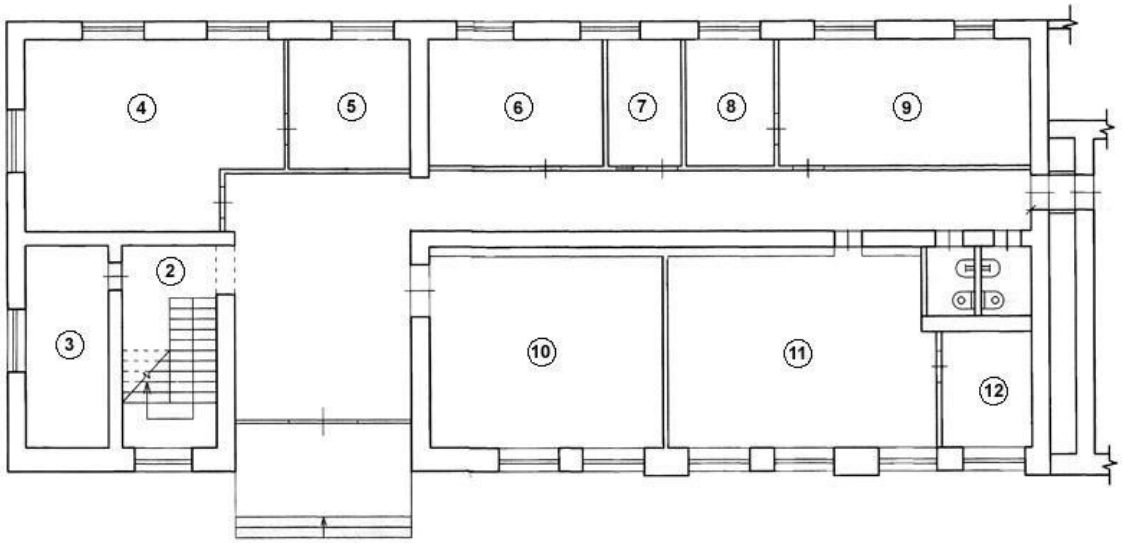
Вариант 5.



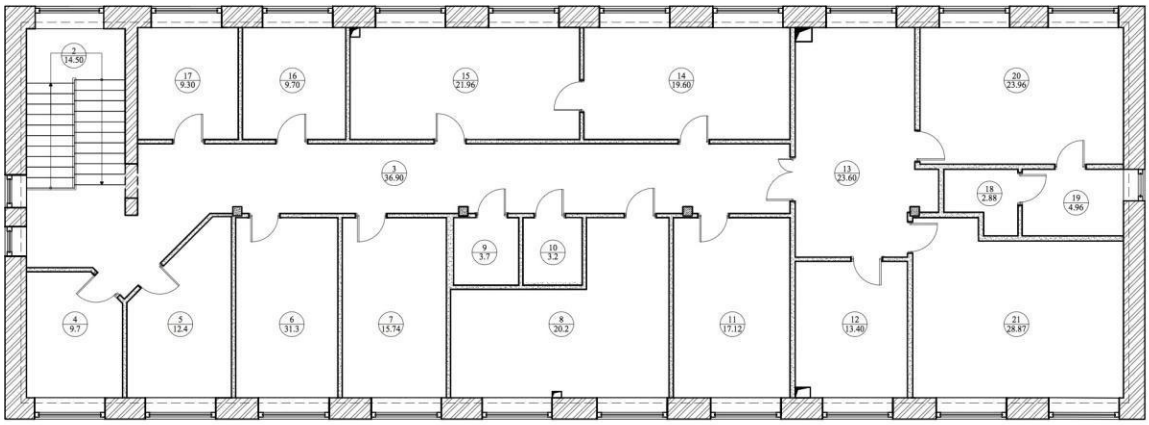
Вариант 6.



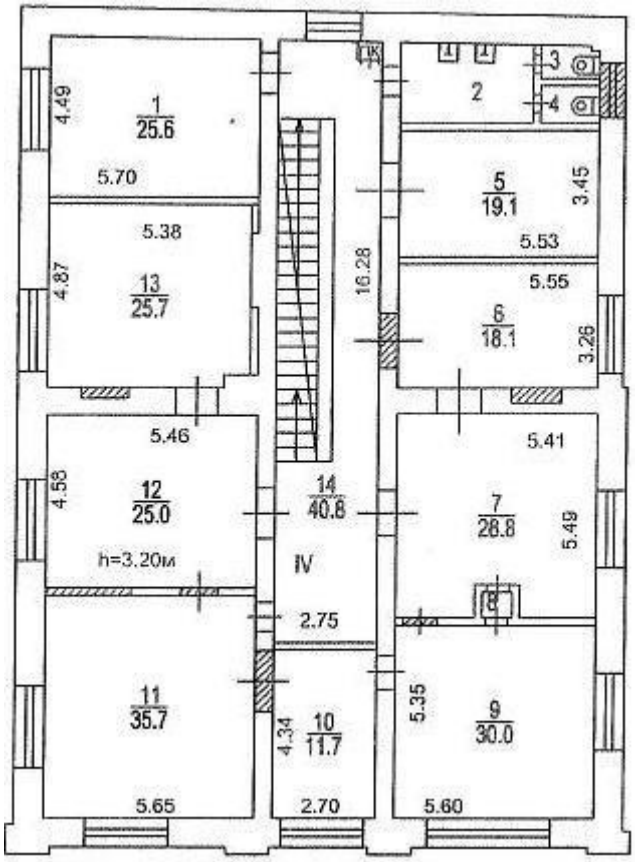
Вариант 7.



Вариант 8.



Вариант 9.



Вариант 10.

Практическое задание №2

Цель: Провести технический осмотр оборудования сети в кабинете 401.

Ход работы

1. Проверить работоспособность информационных розеток в кабинете;
2. Проверить работоспособность патч-кордов от ПК до информационной розетки;
3. Проверить работоспособность портов коммутатора;
4. Проверить работоспособность сетевой карты ПК.
5. Составить отчет-таблицу в следующем виде:

№	Тест	Примечание

Вопросы для контроля:

1) Для чего проводится технический осмотр оборудования?
2) Как часто необходимо проводить технический осмотр?

Практическое задание №3

Цель: Установить и настроить ПО для резервного копирования Cobian BackUp.

Ход работы.

1. Скачать программу cobian backup с официального сайта: http://www.cobiansoft.com/index.htm.
2. Установить утилиту с правами администратора.
3. Выбрать тип установки – автоматически запускаемая служба. Запускать под учетной записью Local System.
4. Создать новое задание (Ctrl+A);
5. Выбрать имя – название группы и номер ПК;
6. Установить тип копирования – полный;
7. В файлах выбрать свою папку;
8. Установить расписание: по понедельникам, один раз в две недели в 00:15.
9. Поставить высокий приоритет и количество полных хранимых копий – 2.
10. Тип сжатия – zip, не делить на несколько файлов.
11. Вид шифрования – AES 256 бит, секретная фраза – Компьютерныесети.

Повторить все то же, для добавочного типа копирования.

Вопросы для контроля:

1) Что значит полное копирование?
2) Чем полное копирование отличается от добавочного?

Практическое задание №4

Цель: Провести восстановление информации утилитой Recuva.

Ход работы.

1. Записать на флеш-накопитель файлы из своей папки (одну картинку и один текстовый файл).
2. Удалить с флешки эти файлы.
3. Скачать утилиту Recuva.
4. Запустить от имени администратора и выбрать все типы файлов.
5. Выбрать расположение вашей флешки и запустить сканирование.
6. Результат сканирования приложить к отчету.
7. Записать на флеш-накопитель файлы из своей папки (одну картинку и один текстовый файл).
8. Произвести быстрое форматирование флешки.
9. Запустить восстановление файлов утилитой Recuva.
10. Записать на флеш-накопитель файлы из своей папки (одну картинку и один текстовый файл).
11. Произвести полное форматирование флешки.
12. Запустить восстановление файлов утилитой Recuva.
13. В выводе описать результаты восстановления при разных способах удаления.

Вопросы для контроля:

1. Чем быстрое форматирование отличается от полного?
2. В каком случае не удастся восстановить удаленную с флешки информацию?

Практическое задание №5

Цель: Изучить типы массивов RAID.

Ход работы.

Экономичность. Следует пояснить, что под *экономичностью* мы подразумеваем в данном случае коэффициент использования пространства жёстких дисков. Для уровней JBOD и RAID0 он равен единице, для "зеркальных" уровней RAID1x равен 1/2, а для всех других вычисляется по формуле (N-X)/N, где X=1 для RAID5, X=2 для RAID5EE и RAID6. При наличии диска (дисков) горячего резерва HotSpare значение X следует увеличить ещё на количество таких дисков.

Поясню на примере. Для внешней системы хранения данных ProStor® M-6160FA-512, имеющей в составе 16 жёстких дисков, 15 из которых объединены в RAID6, а ещё один объявлен как HotSpare, коэффициент использования будет (16–2–1)/16, то есть 81%. Для массива RAID0 на той же стойке этот коэффициент будет равен 100%, а для RAID1 – 50%. Естественно, ни о какой дешевизне в таком контексте речи быть не может, поэтому не следует анализировать нашу диаграмму на предмет поиска самых бюджетных вариантов.

Раз уж об этом зашла речь, "RAID для бедных" – это, как правило, программные реализации RAID0, RAID1, RAID10, RAID5 на двух, четырёх, максимум - шести дисках. Они чаще всего применяются в домашних станциях и не слишком критических серверных задачах и, конечно, тоже имеют право на существование.

Кстати, термин RAID, предложенный учеными Калифорнийского Университета Беркли в 1987 году, первоначально расшифровывался как Redundant Array of Inexpensive Disks (избыточный массив недорогих дисков). В последующем его изменили на Redundant Array of Independent Disks (избыточный массив независимых дисков) – это более точно отражает его суть и не вводит в заблуждение насчёт стоимости, так как для работы в массиве, естественно, рекомендуется использовать аппаратный контроллер и самые качественные диски, которые дешёвыми не являются.

Скорость. Практически безальтернативным средством долговременного хранения больших объёмов данных до недавнего времени являлись магнитные жесткие диски. Магнитные ленты, различные оптические и магнито-оптические дисковые технологии и флэшки в силу присущих им специфических ограничений составить им конкуренцию не могли. Достойным соперником в будущем могут стать твердотельные диски SSD, но их время ещё не наступило (технологию SSD обсудим чуть позже)).

Итак, "узким" местом любой компьютерной системы являются скоростные характеристики механических частей жёстких дисков: скорость вращения шпинделя

и среднее время позиционирования головок. От первой характеристики (при её умножении на плотность записи) зависит так называемая внутренняя скорость чтения и записи данных. От второй – степень затрат времени на перемещение головок, во время которого, естественно, ни запись, ни чтение не производятся.

Реальными путями увеличения производительности дисковой подсистемы, очевидно, являются: минимизация перемещения головок накопителей и параллельное чтение данных с нескольких накопителей одновременно. На практике первый путь реализуется увеличением размера кластера операционной системы, оптимизацией размещения данных на диске и регулярной дефрагментацией. Для реализации второго пути в 1987 было разработано описание набора архитектур массивов дисков, отличающихся отказоустойчивостью и повышенной производительностью, получившее название RAID.

Самыми быстрым согласно нашей диаграмме является уровень RAID0 (RAID00). Теоретически, производительность такого массива должна расти линейно по мере увеличения числа входящих в него дисков, однако на практике, конечно же, всё обстоит не настолько радужно. К тому же следует помнить, что с увеличением числа входящих в RAID0 дисков скорость растёт арифметически, а вероятность отказа – геометрически. В некотором роде компромиссом скорости и надёжности являются все уровни RAIDx0, среди которых упомянем RAID10, RAID1E0, RAID50 и RAID60.

Надёжность. Стопроцентной надежности не бывает в принципе, поэтому в данном случае мы будем рассматривать уровни RAID с точки зрения их устойчивости к отказам отдельных дисков. В этом смысле самым "ненадежным", как мы только что выяснили, является самый быстрый уровень RAID0. Выход из строя любого жёсткого диска в массиве RAID0 вызывает полную потерю его данных.

Самыми надёжными на сегодняшний день можно считать уровни RAID6 и RAID15. В любом случае, не следует забывать про резервное копирование.

JBOD (Just a Bunch of Disks) – это простое объединение (spanning) жестких дисков, которое уровнем RAID формально не является. Томом JBOD может быть массив из одного диска или объединение нескольких дисков. Контроллеру RAID для работы с таким томом не требуется проведение каких-либо вычислений. На нашей диаграмме диск JBOD служит в качестве «ординара» или отправной точки – его значения надежности, производительности и стоимости совпадают с соответствующими показателями единичного жесткого диска.

RAID 0 (“Striping”) избыточности не имеет, а информацию распределяет сразу по всем входящим в массив дискам в виде небольших блоков («страйпов»). За счет этого существенно повышается производительность, но страдает надежность. Как и в случае JBOD, за свои деньги мы получаем 100% емкости диска.

Поясню, почему уменьшается надежность хранения данных на любом составном томе – так как при выходе из строя любого из входящих в него винчестеров полностью и безвозвратно пропадает вся информация. В соответствии с теорией вероятностей математически надежность тома RAID0 равна произведению

надежностей составляющих его дисков, каждая из которых меньше единицы, поэтому совокупная надежность заведомо ниже надежности любого диска.

Хороший уровень – **RAID 1** (“Mirroring”, «зеркало»). Он имеет защиту от выхода из строя половины имеющихся аппаратных средств (в общем случае – одного из двух жестких дисков), обеспечивает приемлемую скорость записи и выигрыш по скорости чтения за счет распараллеливания запросов. Недостаток заключается в том, что приходится выплачивать стоимость двух жестких дисков, получая полезный объем одного жесткого диска.

Изначально предполагается, что жесткий диск – вещь надежная. Соответственно, вероятность выхода из строя сразу двух дисков равна (по формуле) произведению вероятностей, т.е. ниже на порядки! К сожалению, реальная жизнь – не теория! Два винчестера берутся из одной партии и работают в одинаковых условиях, а при выходе из строя одного из дисков нагрузка на оставшийся увеличивается, поэтому на практике при выходе из строя одного из дисков следует срочно принимать меры – вновь восстанавливать избыточность. Для этого с любым уровнем RAID (кроме нулевого) рекомендуют использовать диски горячего резерва **HotSpare**. Достоинство такого подхода – поддержание постоянной надежности. Недостаток – еще большие издержки (т.е. стоимость 3-х винчестеров для хранения объема одного диска).

Зеркало на многих дисках – это уровень **RAID 10**. При использовании такого уровня зеркальные пары дисков выстраиваются в «цепочку», поэтому объем полученного тома может превосходить емкость одного жесткого диска. Достоинства и недостатки – такие же, как и у уровня RAID1. Как и в других случаях, рекомендуется включать в массив диски горячего резерва HotSpare из расчета один резервный на пять рабочих.

RAID 5, действительно, самый популярный из уровней – в первую очередь благодаря своей экономичности. Жертвуя ради избыточности емкостью всего одного диска из массива, мы получаем защиту от выхода из строя любого из винчестеров тома. На запись информации на том RAID5 тратятся дополнительные ресурсы, так как требуются дополнительные вычисления, зато при чтении (по сравнению с отдельным винчестером) имеется выигрыш, потому что потоки данных с нескольких накопителей массива распараллеливаются.

Недостатки RAID5 проявляются при выходе из строя одного из дисков – весь том переходит в критический режим, все операции записи и чтения сопровождаются дополнительными манипуляциями, резко падает производительность, диски начинают греться. Если срочно не принять меры – можно потерять весь том. Поэтому, (см. выше) с томом RAID5 следует обязательно использовать диск Hot Spare.

Помимо базовых уровней RAID0 - RAID5, описанных в стандарте, существуют комбинированные уровни RAID10, RAID30, RAID50, RAID15, которые различные производители интерпретируют каждый по-своему.

Суть таких комбинаций вкратце заключается в следующем. RAID10 – это сочетание единички и нолика (см. выше). RAID50 – это объединение по “0” томов 5-го уровня. RAID15 – «зеркало» «пятерок». И так далее.

Таким образом, комбинированные уровни наследуют преимущества (и недостатки) своих «родителей». Так, появление «нолика» в уровне **RAID 50** нисколько не добавляет ему надежности, но зато положительно отражается на производительности. Уровень **RAID 15**, наверное, очень надежный, но он не самый быстрый и, к тому же, крайне неэкономичный (полезная емкость тома составляет меньше половины объема исходного дискового массива).

RAID 6 отличается от RAID 5 тем, что в каждом ряду данных (по-английски *stripe*) имеет не один, а *два* блока контрольных сумм. Контрольные суммы – «многомерные», т.е. независимые друг от друга, поэтому даже отказ двух дисков в массиве позволяет сохранить исходные данные. Вычисление контрольных сумм по методу Рида-Соломона требует более интенсивных по сравнению с RAID5 вычислений, поэтому раньше шестой уровень практически не использовался. Сейчас он поддерживается многими продуктами, так как в них стали устанавливать специализированные микросхемы, выполняющие все необходимые математические операции.

Согласно некоторым исследованиям, восстановление целостности после отказа одного диска на томе RAID5, составленном из дисков SATA большого объема (400 и 500 гигабайт), в 5% случаев заканчивается утратой данных. Другими словами, в одном случае из двадцати во время регенерации массива RAID5 на диск резерва Hot Spare возможен выход из строя второго диска... Отсюда рекомендации лучших RAIDоводов: 1) **всегда** делайте резервные копии; 2) используйте **RAID6**!

Недавно появились новые уровни RAID1E, RAID5E, RAID5EE. Буква “E” в названии означает *Enhanced*.

RAID level-1 Enhanced (RAID level-1E) комбинирует mirroring и data striping. Эта смесь уровней 0 и 1 устроена следующим образом. Данные в ряду распределяются точь-в-точь так, как в RAID 0. То есть ряд данных не имеет никакой избыточности. Следующий ряд блоков данных копирует предыдущий со сдвигом на один блок. Таким образом как и в стандартном режиме RAID 1 каждый блок данных имеет зеркальную копию на одном из дисков, поэтому полезный объем массива равен половине суммарного объема входящих в массив жестких дисков. Для работы RAID 1E требуется объединение трех или более дисков.

Мне очень нравится уровень RAID1E. Для мощной графической рабочей станции или даже для домашнего компьютера – оптимальный выбор! Он обладает всеми достоинствами нулевого и первого уровней – отличная скорость и высокая надежность.

Перейдем теперь к уровню **RAID level-5 Enhanced (RAID level-5E)**. Это то же самое что и RAID5, только со встроенным в массив резервным диском *spare drive*. Это встраивание производится следующим образом: на всех дисках массива оставляется свободным 1/N часть пространства, которая при отказе одного из дисков

используется в качестве горячего резерва. За счет этого RAID5E демонстрирует наряду с надежностью лучшую производительность, так как чтение/запись производится параллельно с бОльшего числа накопителей одновременно и spare drive не простаивает, как в RAID5. Очевидно, что входящий в том резервный диск нельзя делить с другими томами (dedicated vs. shared). Том RAID 5E строится минимум на четырех физических дисках. Полезный объем логического тома вычисляется по формуле N-2.

RAID level-5E Enhanced (RAID level-5EE) подобен уровню RAID level-5E, но он имеет более эффективное распределение spare drive и, как следствие, – более быстрое время восстановления. Как и уровень RAID5E, этот уровень RAID распределяет в рядах блоки данных и контрольных сумм. Но он также распределяет и свободные блоки spare drive, а не просто оставляет под эти цели часть объема диска. Это позволяет уменьшить время, необходимое на реконструкцию целостности тома RAID5EE. Входящий в том резервный диск нельзя делить с другими томами – как и в предыдущем случае. Том RAID 5EE строится минимум на четырех физических дисках. Полезный объем логического тома вычисляется по формуле N-2.

Как ни странно, никаких упоминаний об уровне **RAID 6E** на просторах Интернета я не нашел - пока такой уровень никем из производителей не предлагается и даже не анонсируется. А ведь уровень RAID6E (или RAID6EE?) можно предложить по тому же принципу, что и предыдущий. Диск **HotSpare** *обязательно* должен сопровождать любой том RAID, в том числе и RAID 6. Конечно, мы не потеряем информацию при выходе из строя одного или двух дисков, но начать регенерацию целостности массива крайне важно как можно раньше, чтобы скорее вывести систему из «критического» режима. Поскольку необходимость диска Hot Spare для нас не подлежит сомнению, логичным было бы последовать дальше и «размазать» его по тОму так, как это сделано в RAID 5EE, чтобы получить преимущества от использования бОльшего количества дисков (лучшая скорость на чтении-записи и более быстрое восстановление целостности).

Уровни RAID в «числах».

В таблицу я собрал некоторые важные параметры почти всех уровней RAID, чтобы можно было сопоставить их между собой и четче понять их суть.

Уровень	Избы-точ-ность	Исполь-зование емкости дисков	Произво-дитель-ность чтения	Произво-дитель-ность записи	Встроен-ный диск резерва	Мин. кол-во дисков	Макс. кол-во дисков
RAID 0	нет	100%	**Отл**	**Отл**	нет	1	16
RAID 1	+	50%	Хор +	Хор +	нет	2	2
RAID 10	+	50%	Хор +	Хор +	нет	4	16

RAID 1E	+	50%	Хор +	Хор +	нет	3	16
RAID 5	+	67-94%	**Отл**	Хор	нет	3	16
RAID 5E	+	50-88%	**Отл**	Хор	+	4	16
RAID 5EE	+	50-88%	**Отл**	Хор	+	4	16
RAID 6	+	50-88%	**Отл**	Хор	нет	4	16
RAID 00	нет	100%	**Отл**	**Отл**	нет	2	**60**
RAID 1E0	+	50%	Хор +	Хор +	нет	6	**60**
RAID 50	+	67-94%	**Отл**	Хор	нет	6	**60**
RAID 15	+	33-48%	**Отл**	Хор	нет	6	**60**

Все «зеркальные» уровни – RAID 1, 1+0, 10, 1E, 1E0.

Давайте еще раз попробуем досконально разобраться, чем же различаются эти уровни?

RAID 1.

Это – классическое «зеркало». Два (и только два!) жестких диска работают как один, являясь полной копией друг друга. Выход из строя любого из этих двух дисков не приводит к потере ваших данных, так как контроллер продолжает работу с оставшимся диском. RAID1 в цифрах: двукратная избыточность, двукратная надежность, двукратная стоимость. Производительность на запись эквивалентна производительности одного жесткого диска. Производительность чтения выше, так как контроллер может распределять операции чтения между двумя дисками.

RAID 10.

Суть этого уровня в том, что диски массива объединяются парами в «зеркала» (RAID 1), а затем все эти зеркальные пары в свою очередь объединяются в общий массив с чередованием (RAID 0). Именно поэтому его иногда обозначают как **RAID 1+0**. Важный момент – в RAID 10 можно объединить только четное количество дисков (минимум – 4, максимум – 16). Достоинства: от "зеркала" наследуется надежность, от «нуля» – производительность как на чтение, так и на запись.

RAID 1E.

Буква "E" в названии означает "Enhanced", т.е. "улучшенный". Принцип этого улучшения следующий: данные блоками "чередуются" ("striped") на все диски массива, а потом еще раз "чередуются" со сдвигом на один диск. В RAID 1E можно объединять от трех до 16 дисков. Надежность соответствует показателям "десятки", а производительность за счет большего "чередования" становится чуть лучше.

RAID 1E0.

Этот уровень реализуется так: мы создаем "нулевой" массив из массивов RAID1E. Следовательно, общее количество дисков должно быть кратно трем: минимум три и максимум – шестьдесят! Преимущество в скорости при этом мы вряд

ли получим, а сложность реализации может неблагоприятно отразиться на надежности. Главное достоинство – возможность объединить в один массив очень большое (до 60) количество дисков.

Вопросы для контроля:

1. Чем отличаются существующие организации резервирования?
2. Какой способ более экономичен?

Практическое задание №6

Цель: Научиться восстанавливать работоспособность сети.

Ход работы.

Практическое задание №7

Цель: Научиться пользоваться анализатором протоколов Wire Shark.

1 ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

1.1 Захват и анализ сетевого трафика с помощью программы«Wireshark»

Wireshark - программа-анализатор трафика для компьютерных сетей Ethernet. Программа Wireshark позволяет захватывать пакеты протоколов, передаваемые по сети Ethernet и с помощью графического интерфейса представить эти данные пользователю для дальнейшего анализа.

Основное окно Wireshark при его старте имеет следующий вид (рисунок 1).

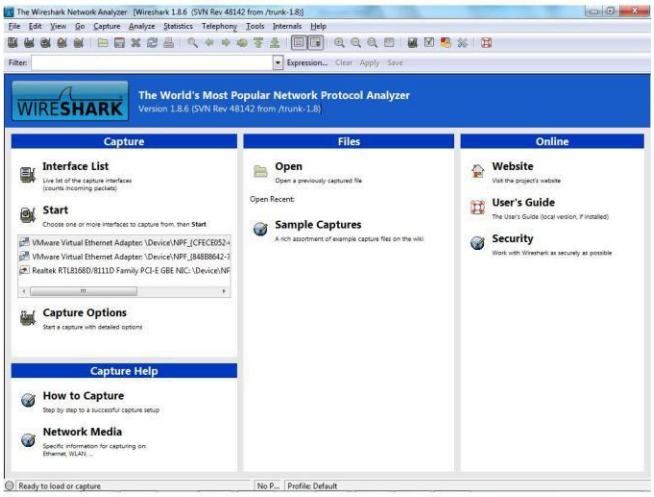


Рисунок 1 – Основное окно Wireshark

Панель инструментов **Wireshark** имеет следующие инструменты (Рисунок 2).

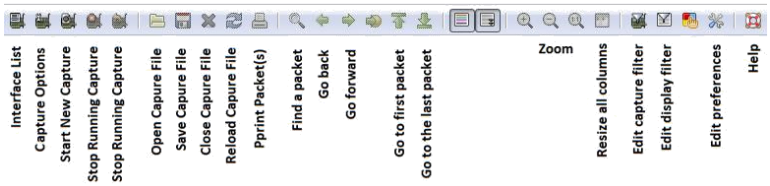


Рисунок 2 – Панель инструментов

С помощью инструментов панели фильтра Wireshark (рисунок 3) можно создавать и сохранять, применять и удалять фильтры, которые представляют возможность фильтрации информации захваченного сетевого трафика.

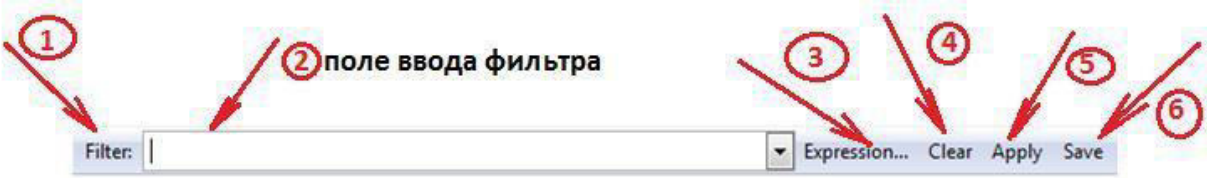


Рисунок 3 – Панель фильтра

Панель фильтра Wireshark имеет следующие поля и инструменты (Рисунок 3).

- Filter (см. указатель 1 на рисунок 3) – предназначен для открытия диалогового окна пользовательских фильтров для создания или редактирования фильтра;

- Поле ввода фильтра (см. указатель 2 на рисунок 3) - предназначено дляредактирования выражения фильтра;
- Expression (см. указатель 3 на рисунок 3) - предназначен для открытия диалоговогоокна – помощника для построения выражения фильтров;
- Clear (см. указатель 4 на рисунок 3) – предназначен для приостановления воздействияфильтра и очистки поля фильтра;
- Apply (см. указатель 5 на рисунок 3) – предназначен для подключения воздействияфильтра;
- Save (см. указатель 6 на рисунок 3) – предназначен для сохранения выражения фильтра для дальнейшего использования.

Окно списка доступных адаптеров (Рисунок 4) можно открыть, нажав на кнопку «Interface List» на панели инструментов (см. Рис. 2) программы Wireshark.

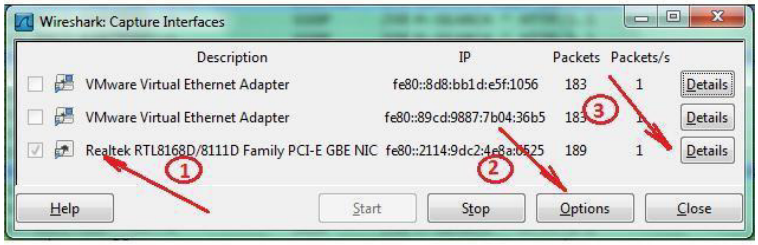


Рисунок 4 – Список доступных адаптеров

- Кнопка «Options» (указатель 2 на рисунок 4) открывает окно настроек захвата трафика (Рисунок 5);

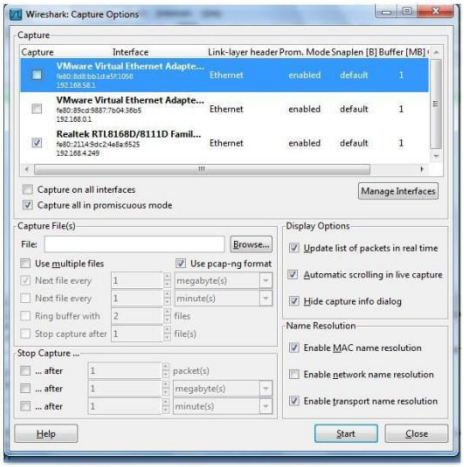


Рисунок 5 – Окно настроек захвата трафика

- Кнопка «Details» (указатель 3 на рисунок 4) открывает окно статических характеристик сетевого адаптера.

Программа Wiresharkпозволяет настроить различные фильтры, вот некоторые из них:

- Фильтр по протоколу - фильтрация на уровне захваченных пакетов/кадров– при этом фильтрация будет выполняться по определённым протоколам;
- Фильтр по полю пакета протокола (Display filter) - фильтрация на уровне значений полей захваченных пакетов/кадров - при этом фильтрация будет виполняться по определённым значениям полей в заголовках протоколов;

Для применения фильтрации по определённому протоколу необходимо ввести имя протокола (например, dhcpv6) в поле ввода фильтра и нажать кнопку «Apply» (Рисунок 6 и 7)

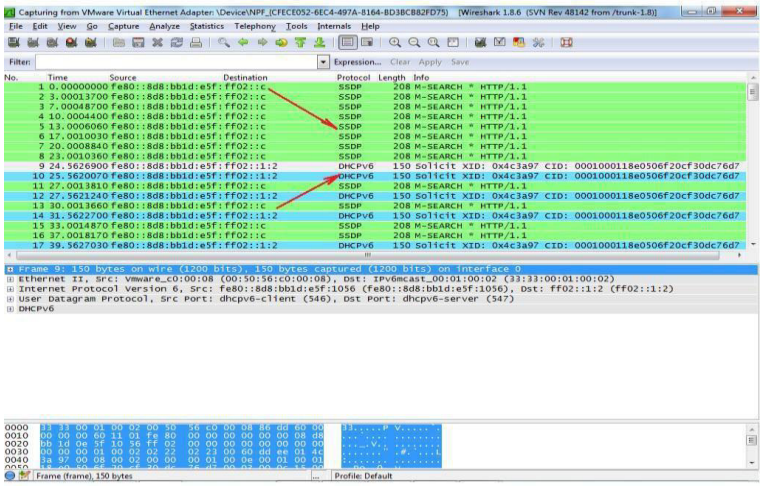


Рисунок 6 – Вид до применения фильтра

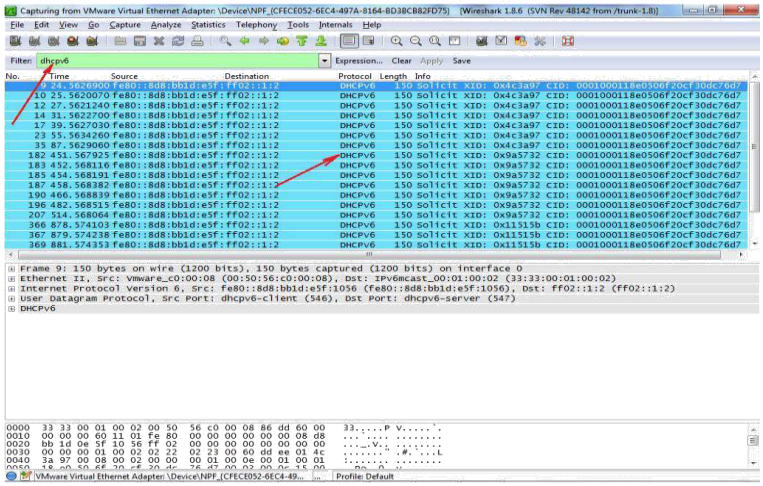


Рисунок 7 – Вид после применения фильтра

Имена полей, которые можно использовать при построении выражений фильтров, доступны через построитель фильтров.

Для построения фильтров надо выполнить следующие шаги:

- Запустить помощник-построитель выражений фильтров, нажав на кнопку «Expression…» (см. указатель 6 на рисунок 8);
- На открывшемся окне в списке «Field name» выбрать имя интересующего нас поля (например, ip.src), которое будет нами использоваться для дальнейшегопостроения фильтра (см. указатель 1 на рисунок 8);
- В списке «Relation» выбрать знак соотношения (см. указатель 2 на рисунок 8)
- В поле «Value» (см. указатель 3 на рисунок 8) ввести интересующее нас значение (например, 192.168.4.249, которое в данном случае взято - см. указатель 5 на рисунок 8);

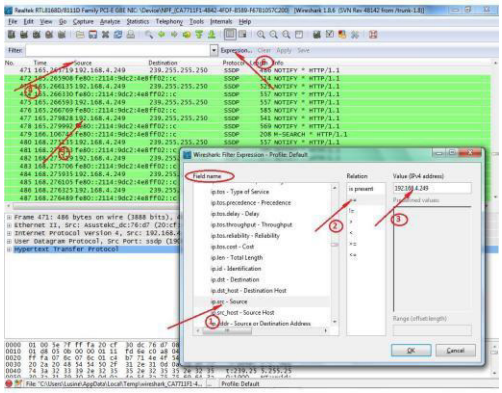


Рисунок 8 – Построение фильтра на уровне полей

- Нажать кнопку «ОК»;
- Поле фильтра будет заполняться вновь построенным выражением фильтра (ip.src== 192.168.4.249) (см. указатель 1 на рис. 7) Нажать на «Apply» (см. указатель 2 на рисунок 9);

Окно будет показывать только соответствующие текущему фильтру данные (см. указатель 3 на рисунок 9)

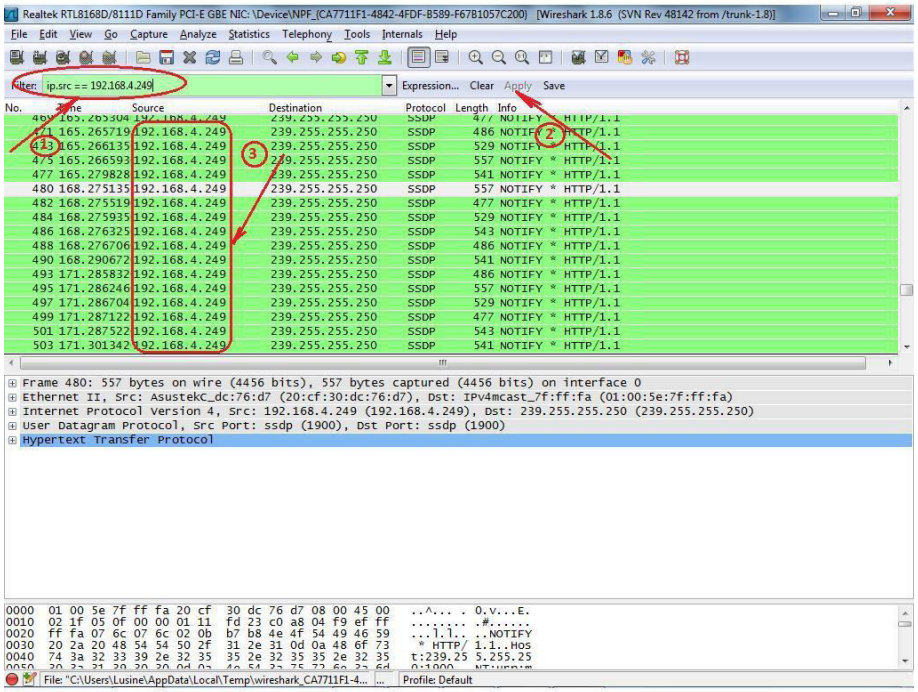


Рисунок 9 – Применение фильтра на уровне значения полей

В фильтре могут комбинироваться два и более элементарных условий (см. указатель 1 на рис. 8), используя логические операторы в следующем формате:

Условие 1 Логический оператор Условие 2

Пример комбинированного фильтра:

- ip.src == 192.168.4.249 andip.dst == 192.168.4.239
- ipand ip.src == 192.168.4.249

В качестве элементарного условия могут использоваться выражения фильтров обоих уровней (см. второй пример выше).

Главное окно Wireshark имеет три панели – дочерние окна (Рисунок 10).

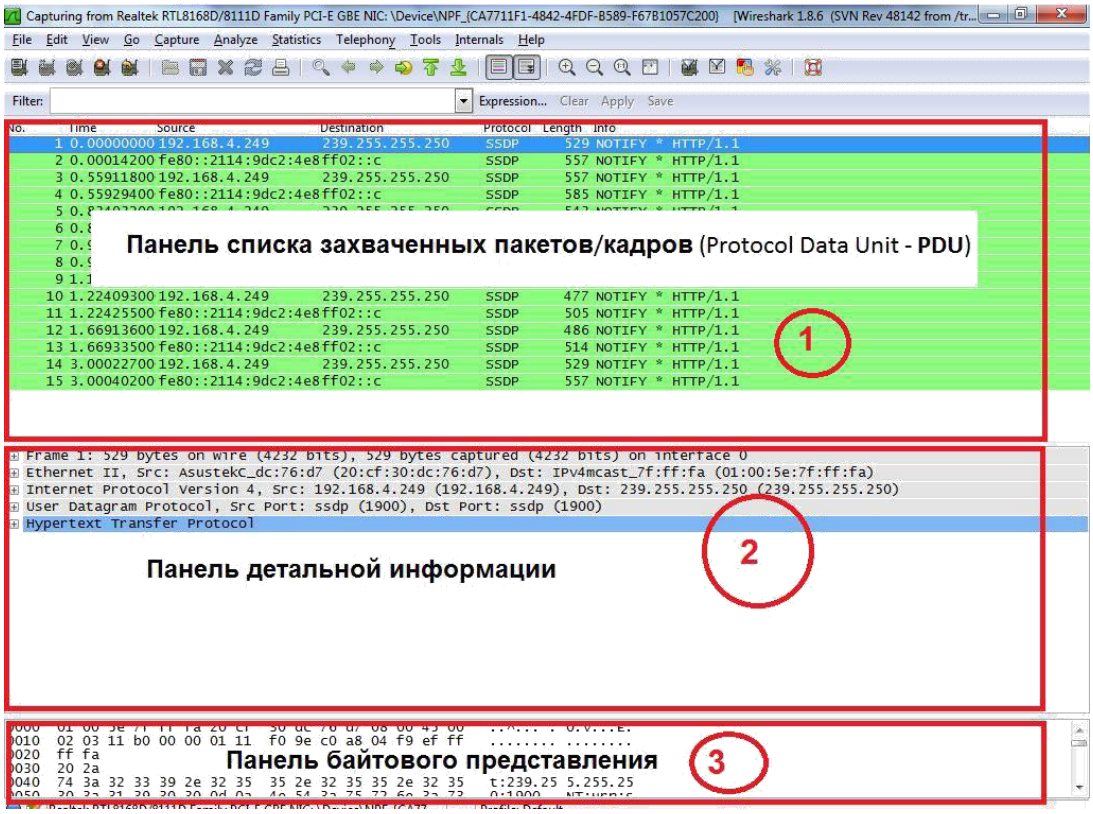
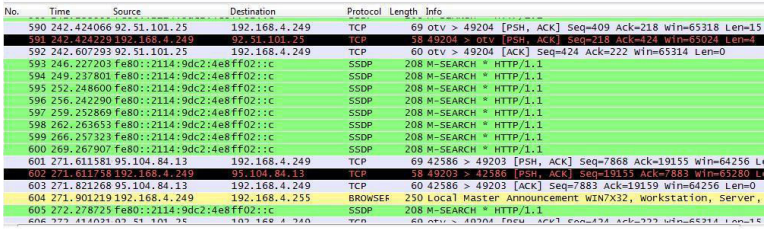

Capturing from Realtek RTL8168D/8111D Family PCI-E GBE NIC: \Device\NPF_{CA7711F1-4842-4FDF-B589-F67B1057C200} [Wireshark 1.8.6 (SVN Rev 48142 from /tr...
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
1 0.00000000 192.168.4.249 239.255.255.250 SSDP 529 NOTIFY * HTTP/1.1
2 0.00014200 fe80::2114:9dc2:4e8 ff02::c SSDP 557 NOTIFY * HTTP/1.1
3 0.55911800 192.168.4.249 239.255.255.250 SSDP 557 NOTIFY * HTTP/1.1
4 0.55929400 fe80::2114:9dc2:4e8 ff02::c SSDP 585 NOTIFY * HTTP/1.1
Панель списка захваченных пакетов/кадров (Protocol Data Unit - PDU)
10 1.22409300 192.168.4.249 239.255.255.250 SSDP 477 NOTIFY * HTTP/1.1
11 1.22425500 fe80::2114:9dc2:4e8 ff02::c SSDP 505 NOTIFY * HTTP/1.1
12 1.66913600 192.168.4.249 239.255.255.250 SSDP 486 NOTIFY * HTTP/1.1
13 1.66933500 fe80::2114:9dc2:4e8 ff02::c SSDP 514 NOTIFY * HTTP/1.1
14 3.00022700 192.168.4.249 239.255.255.250 SSDP 529 NOTIFY * HTTP/1.1
15 3.00040200 fe80::2114:9dc2:4e8 ff02::c SSDP 557 NOTIFY * HTTP/1.1
1
Frame 1: 529 bytes on wire (4232 bits), 529 bytes captured (4232 bits) on interface 0
Ethernet II, Src: AsustekC_dc:76:d7 (20:cf:30:dc:76:d7), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 192.168.4.249 (192.168.4.249), Dst: 239.255.255.250 (239.255.255.250)
User Datagram Protocol, Src Port: ssdp (1900), Dst Port: ssdp (1900)
Hypertext Transfer Protocol
2
Панель детальной информации
0010 02 03 11 b0 00 00 01 11 f0 9e c0 a8 04 f9 ef ff
0020 ff fa
0030 20 2a
0040 74 3a 32 33 39 2e 32 35 35 2e 32 35 35 2e 32 35 t:239.25 5.255.25
Панель байтового представления
3

Рисунок 10 – Панели главного окна

Окно Wireshark имеет следующие три дочерние окна-панели:

- Первое окно -панельсписказахваченныхпакетов/кадров (Protocol Data Unit -PDU)
- Второе окно -панельдетальнойинформации показывает содержимое текущего пакета, выделенного на панели списка захваченных пакетов (на первом окне)
- Третье окно -панельбайтовогопредставления показывает содержимое текущего пакета, выделенного на панели списка захваченных пакетов (на первом окне) в шестнадцатеричном виде

Панель списка захваченных пакетов - PDUсодержит сводную информацию по всемутрафику, захваченному с помощью программы Wireshark. Каждая строка характеризуетотдельно захваченный пакет и описывается следующими полями (Рисунок 11).



No.	Time	Source	Destination	Protocol	Length	Info
590	242.424066	92.51.101.25	192.168.4.249	TCP	69	otv > 49204 [PSH, ACK] Seq=409 Ack=218 Win=65318 Len=15
591	242.424229	192.168.4.249	92.51.101.25	TCP	58	49204 > otv [PSH, ACK] Seq=218 Ack=424 Win=65024 Len=4
592	242.607293	92.51.101.25	192.168.4.249	TCP	60	otv > 49204 [ACK] Seq=424 Ack=222 Win=65314 Len=0
593	246.227203	fe80::2114:9dc2:4e8ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
594	249.237801	fe80::2114:9dc2:4e8ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
595	252.248600	fe80::2114:9dc2:4e8ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
596	256.242290	fe80::2114:9dc2:4e8ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
597	259.252869	fe80::2114:9dc2:4e8ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
598	262.263653	fe80::2114:9dc2:4e8ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
599	266.257323	fe80::2114:9dc2:4e8ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
600	269.267907	fe80::2114:9dc2:4e8ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
601	271.611581	95.104.84.13	192.168.4.249	TCP	69	42586 > 49203 [PSH, ACK] Seq=7868 Ack=19155 Win=64256 L
602	271.611758	192.168.4.249	95.104.84.13	TCP	58	49203 > 42586 [PSH, ACK] Seq=19155 Ack=7883 Win=63280 L
603	271.821268	95.104.84.13	192.168.4.249	TCP	60	42586 > 49203 [ACK] Seq=7883 Ack=19159 Win=64256 Len=0
604	271.901219	192.168.4.249	192.168.4.255	BROWSER	250	Local Master Announcement WIN7X32, Workstation, Server,
605	272.278725	fe80::2114:9dc2:4e8ff02::c		SSDP	208	M-SEARCH * HTTP/1.1

Рисунок 11 – Панель списка захваченных пакетов

- No. – последовательный номер захваченного PDU;
- Time – промежуток времени (в секундах), прошедшее с момента начала захватаPDU;
- Source – сетевой адрес отправителя (IPv4 / IPv6);
- Destination – сетевой адрес получателя (IPv4 / IPv6);
- Protocol – тип протокола;
- Length – длина захваченного пакета;
- Info – некоторая дополнительная информация о захваченном PDU.

Панель детальной информации– в этой панели отображается содержимое пакетавыделенного на панели списка пакетов (см. указатель 1 на рисунок 12) в иерархических структурах (см. указатель 2 на рисунок 12):

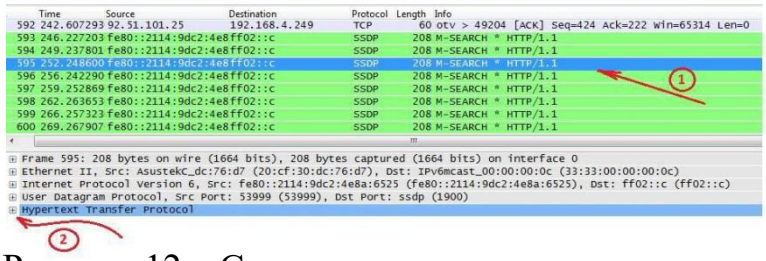


Рисунок 12 – Список захваченных пакетов

- Frame – содержит справочную информацию о захваченном PDU, такую как - время захвата, длинна PDU и т.д.;
- Ethernet II - содержит информацию о заголовке протокола канального (Data Link) уровня;
- Internet Protocol -содержит информацию о заголовке протокола сетевого(Network) уровня;
- User Defined Protocol (UDP) - содержит информацию о заголовке протокола транспортного (Transport) уровня;
- Hypertext -содержит информацию о заголовке протокола прикладного(Application) уровня.

ВЫПОЛНЕНИЕ РАБОТЫ

1. Запустить программу Wireshark;
2. Используя теоретический материал, произвести захват сетевого трафика.
3. На рисунке 13 представлен пример перехваченного трафика. В соответствии с вашим вариантом, вам необходимо исследовать трафик, более подробно рассмотреть указатель 4 и 5 рисунка 13

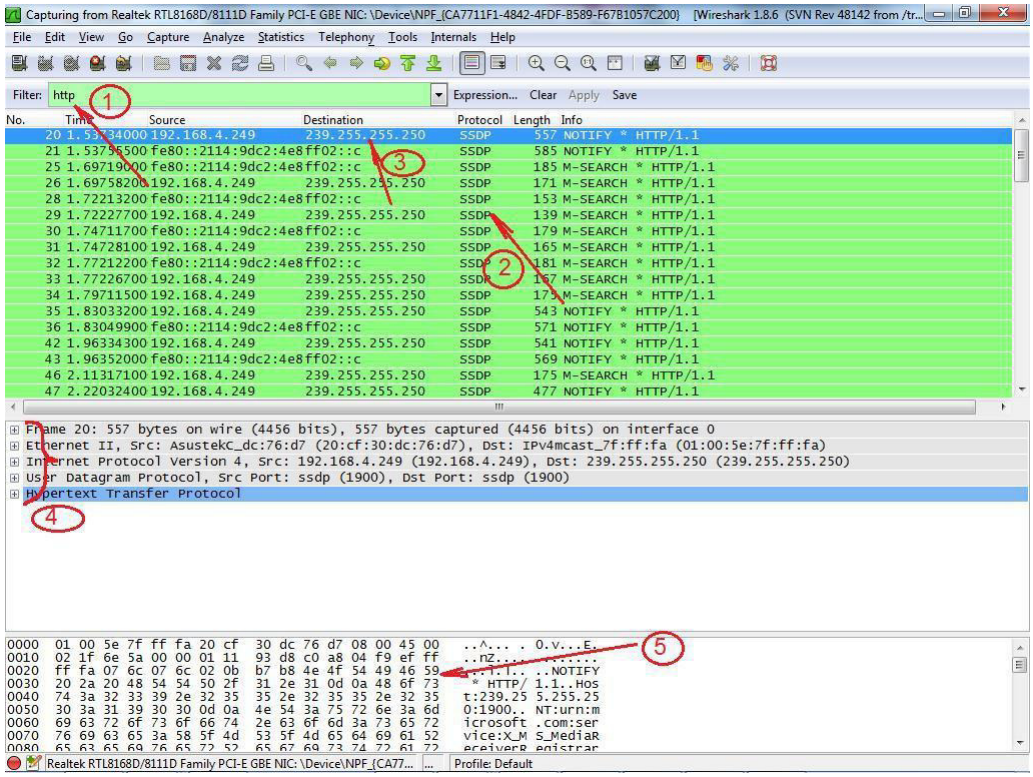


Рисунок 5 – Перехваченный траффик

1 вариант исследовать протокол ARP (1, 6, 11, 16, 21, 26,31)

2 вариант исследовать протокол IP (2, 7, 12, 17, 22, 27, 32)

3 вариант исследовать протокол TCP (3, 8, 13, 18, 23, 28)

4 вариант исследовать протокол UDP (4, 9, 14, 19, 24, 29)

5 вариант исследовать протокол ICMP (5, 10, 15, 20, 25, 30)

В скобках указан номер в списке журнала группы.

Практическое задание №8

Цель: получить навыки по установке и применению программного обеспечения (ПО) для построения карты вычислительной сети на примере ПО AdRem NetCrunch версии 6.5.

ВВЕДЕНИЕ

Для успешного администрирования сети необходимо знать состояние каждого ее элемента с возможностью изменять параметры его функционирования. Обычно сеть состоит из устройств различных производителей и управлять ею было бы нелегкой задачей если бы не программное обеспечение, позволяющее централизованно собирать информацию о всех узлах сети, а так же производить централизованное управление всеми объектами сети. Как правило сбор информации от узлов производится при помочи сканера сетевых портов и при использовании Simple Network Management Protocol (SNMP). SNMP - это протокол включающий набор команд, позволяющий выполнять весь спектр задач управления сетевыми устройствами - от получения информации о местонахождении конкретного устройства, до возможности производить его тестирование.

Основной концепцией протокола является то, что вся необходимая для управления устройством информация хранится на самом устройстве - будь то сервер, модем или маршрутизатор - в так называемой Административной Базе Данных (MIB – Management Information Base). MIB представляет из себя набор переменных, характеризующих состояние объекта управления. Эти переменные могут отражать такие параметры, как количество пакетов, обработанных устройством, состояние его интерфейсов, время функционирования устройства и т.п. Каждый производитель сетевого оборудования, помимо стандартных переменных, включает в MIB какие-либо параметры, специфичные для данного устройства.

Для того, чтобы проконтролировать работу некоторого устройства сети,

необходимо просто получить доступ к его MIB, которая постоянно обновляется самим устройством, и проанализировать значения некоторых переменных.

Важной особенностью протокола SNMP является то, что в нем не содержатся конкретные команды управления устройством. Вместо определения всего возможного спектра таких команд, который считается все-таки простым, определены переменные MIB, переключение которых воспринимается устройством как указание выполнить некоторую команду. Таким образом удается сохранить простоту протокола, но вместе с этим сделать его довольно мощным средством, дающим возможность стандартным образом задавать наборы команд управления сетевыми устройствами. Задача обеспечения выполнения команд состоит, таким образом, в регистрации специальных переменных MIB и реакции устройства на их изменения.

Каждому элементу соответствует численный и символьный идентификатор. В имя переменной включается полный путь до нее от корневого элемента root. Например, время работы устройства с момента перезагрузки хранится в переменной, находящейся в разделе system под номером 3 и называется sysUpTime. Соответственно, имя переменной будет включать весь путь: iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).system(1).sysUpTime(3); или на языке чисел: 1.3.6.1.2.1.1.3. Следует заметить, что при этом узлы дерева разделяются точками. Существует стандартная ветвь MIB, относящаяся к разделу управления mgmt, которую обычно поддерживают все сетевые устройства.

На данный момент существуют 3 версии протокола SNMP: версия v.1, v.2 и v.3. Главное отличие SNMP v.3 от SNMP v.1 и SNMP v.2 в том, что SNMP v.3 предоставляет в значительной степени более высокий уровень безопасности, чем предыдущие версии.

В SNMP v.1 и SNMP v.2 авторизация пользователя выполняется посредством "строки сообщества" - Community String, которая действуют как пароль. Удаленная пользовательская программа SNMP и агент SNMP должны использовать одни и те же Community Strings.

Пакеты SNMP от любой станции, которая не была авторизована,

игнорируются (отбрасываются).

SNMP v.3 используют более сложный процесс авторизации, который разделяется на две части. Первая часть используется для поддержания списка пользователей и их атрибутов, которым разрешено управлять по протоколу SNMP. Вторая часть описывает, что каждый пользователь из данного списка может делать при управлении по SNMP.

Коммутатор позволяет указывать и настраивать группы пользователей в данном списке с одинаковым набором привилегий. Для указанных групп может быть установлена версия SNMP. Таким образом, можно создать группу SNMP, которой разрешено просматривать информацию, предназначенную только для чтения, или получать сообщения traps, используя SNMP v.1, в то время как другой группе назначен более высокий уровень безопасности, предоставляющий привилегии чтения/записи, посредством SNMP v.3.

Используя SNMP v.3 можно позволить или запретить индивидуальным пользователям или группам SNMP-менеджеров выполнять конкретные функции SNMP-управления. Разрешенные или запрещенные функции определяются с помощью идентификатора объекта Object Identifier (OID), ассоциированного с конкретной MIB.

Кроме того, в SNMP v.3 доступен уровень безопасности, в котором SNMP-сообщения могут быть зашифрованы (при использовании уровней авторизации HMAC-SHA-96 или HMAC-MDA-96).

В SNMP есть особый вид сообщений - traps. Traps - это сообщения, которые предупреждают о произошедших событиях при работе сетевого оборудования. События могут быть как важными (перезагрузка устройства), так и менее важными (изменения состояния порта коммутатора). Сетевое оборудование генерирует traps и посылает их станции сетевого управления.

Примером ПО, позволяющим строить подробную карту вычислительной сети с использованием протокола SNMP всех версий и способным принимать сообщения типа trap от сетевых устройств является AdRem NetCrunch.

AdRem NetCrunch определяет и отображает логическую топологию сети (включая сервера, маршрутизаторы, коммутаторы, принтеры, хосты) для обеспечения мониторинга работоспособности устройств, служб и времени

отклика. Программа дает возможность выборочной проверки узлов, отсылки уведомлений (по электронной почте, через ICQ, SMS, SNMP), отслеживания состояний устройств и формирование отчетов. AdRem NetCrunch считывает информацию со счетчиков производительности сетевого оборудования, поддерживающего протокол SNMP и предлагает IP инструменты, такие как измерение времени отклика от устройств (команда ping с графическим представлением результатов), полосу пропускания сетевых каналов, сканер сетевых портов.

ВЫПОЛНЕНИЕ РАБОТЫ

1.Установка. После установки AdRem NetCrunch 6.5 и первого запуска программа предлагает создать карту сети со списком всех устройств. Можно выбрать один из режимов обнаружения устройств в сети (автоматическое обнаружение всех устройств в сети или указать типы устройств, которые NetCrunch будет обнаруживать при сканировании), диапазон IP адресов для сканирования, службы, которые мы хотим обнаружить.

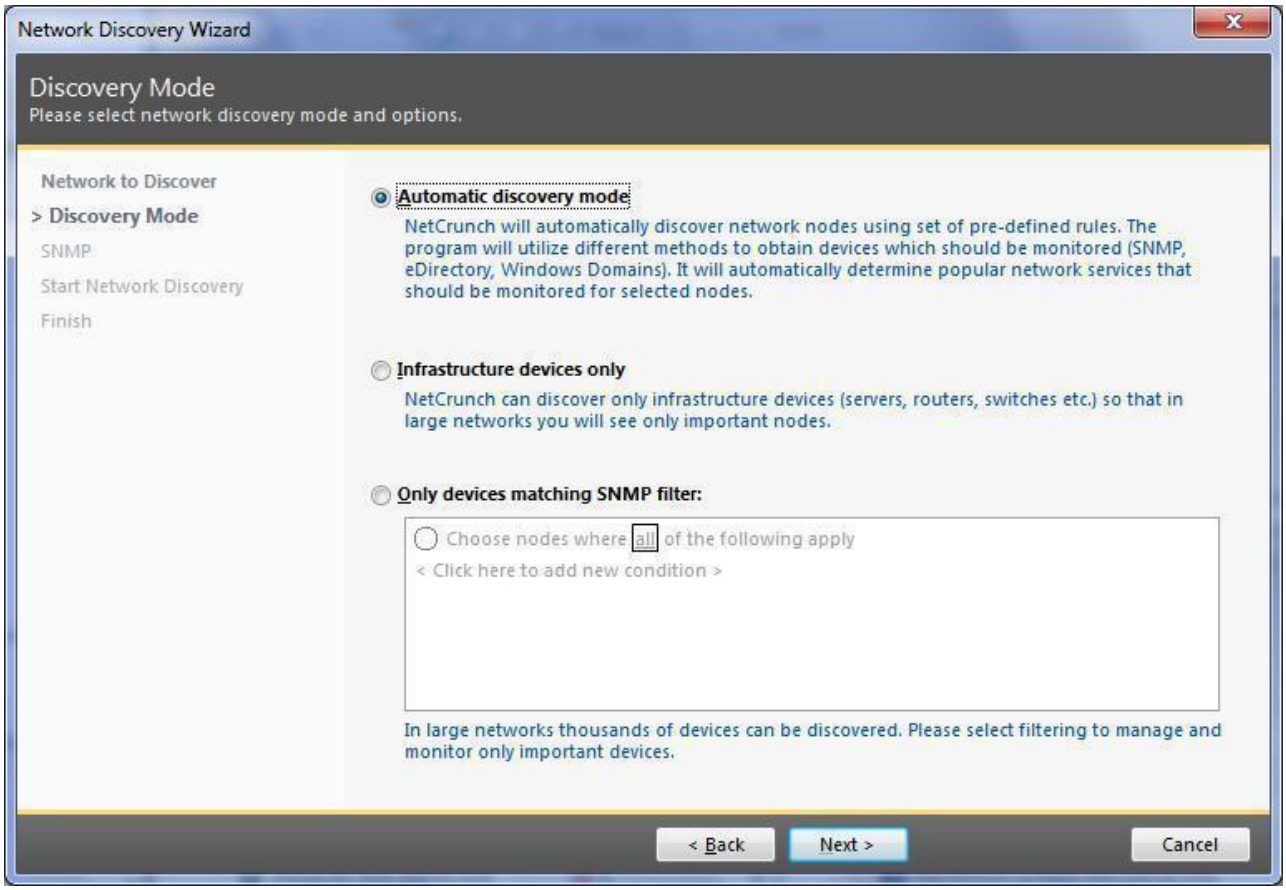


Рисунок 1 – Выбор режима сканирования сети

2. Обнаружение устройств в сети. После сканирования диапазона открывается центральное окно программы, позволяющее увидеть список событий, произошедших в выбранном промежутке времени, таких как основные проблемы и устройства, у которых время отклика при последнем сканировании превысило стандартное значение, что может например быть следствием большой загруженности устройства или его недоступности (неработоспособности).

Рисунок 2 – Центральная консоль управления

3. Список обнаруженных устройств. Выбрав слева на панели управления просканированный диапазон IP-адресов можно увидеть все устройства, обнаруженные при сканировании сети.

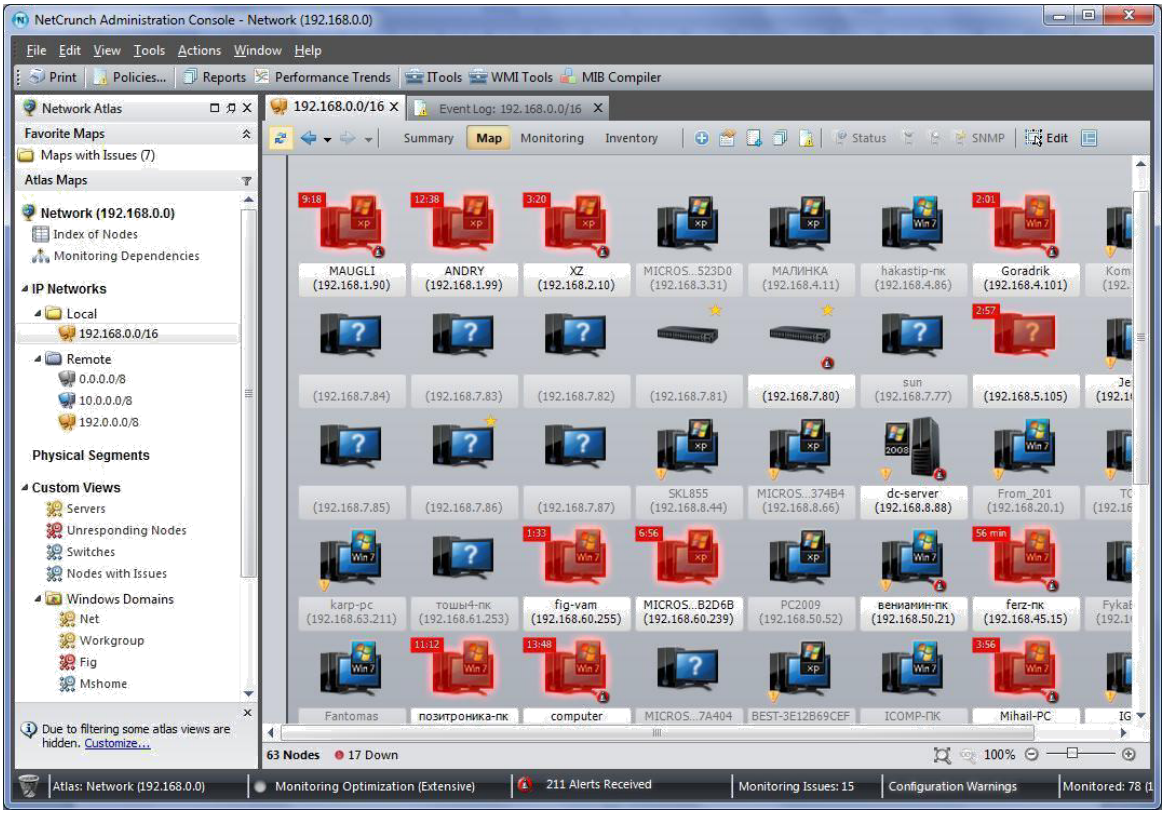


Рисунок 3 – Список устройств в сети

4. Детальное описание устройства в сети. Если выбрать интересующее устройство из списка и перейти в его свойства через контекстное меню, то можно увидеть детальное описание устройства и его состояние. На рисунке 4 видны параметры коммутатора D-link DES-3526, такие как время работы устройства после последней перезагрузки, имя устройства, количество неиспользуемых интерфейсов, время последнего опроса NetCrunch.

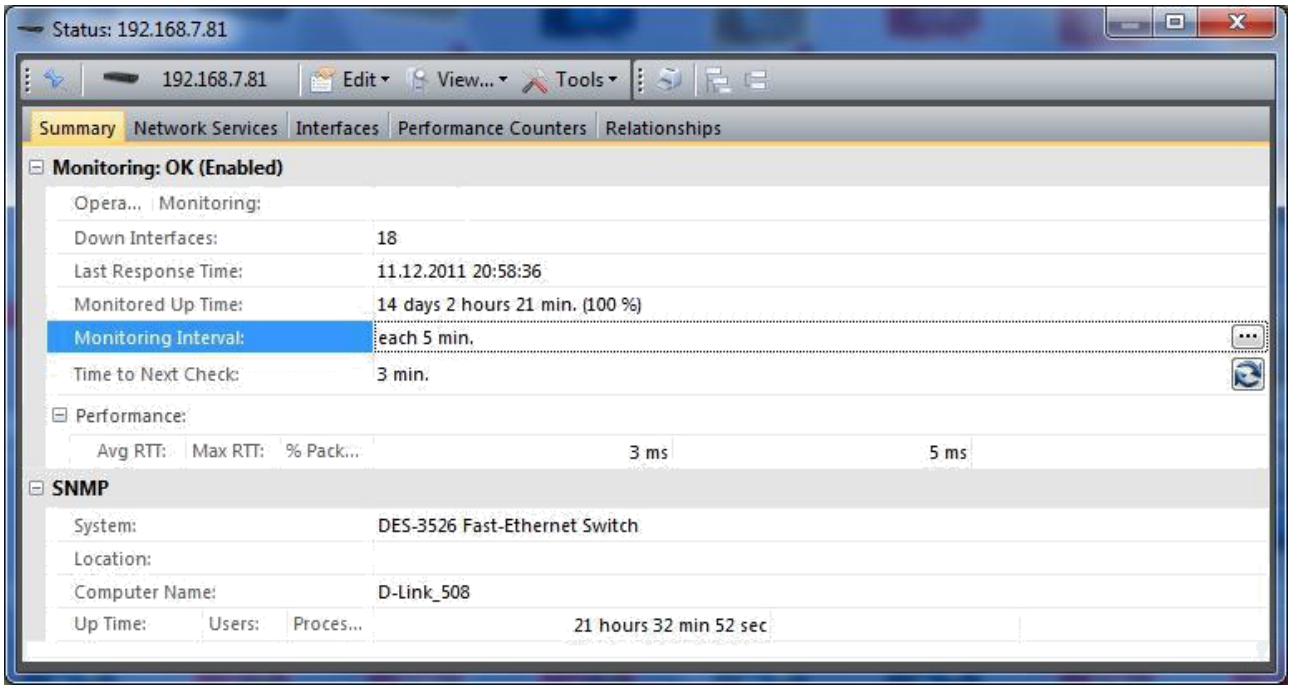


Рисунок 4 – Детальное описание коммутатора сети

На вкладке Network Services можно увидеть, с помощью каких служб осуществляется мониторинг устройства:

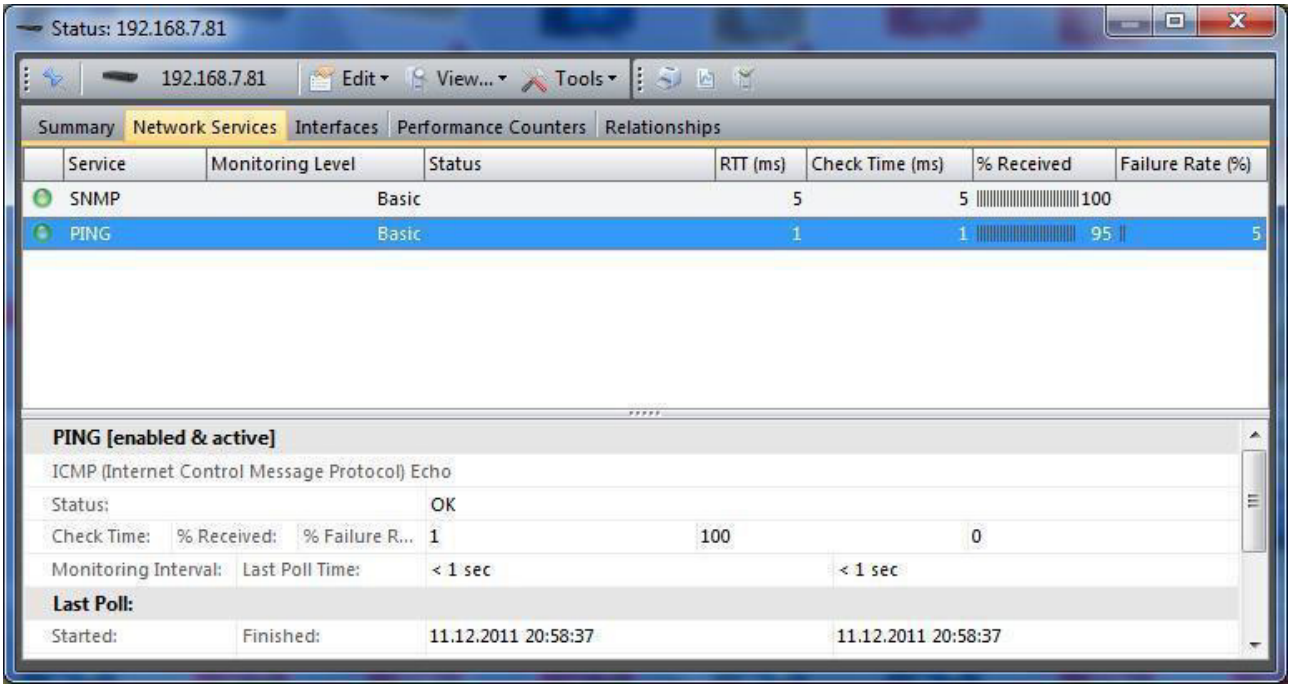


Рисунок 5 – Активные службы на устройстве

Если перейти на вкладку Interfaces, то можем увидеть состояние портов коммутатора и скорость подключения портов:

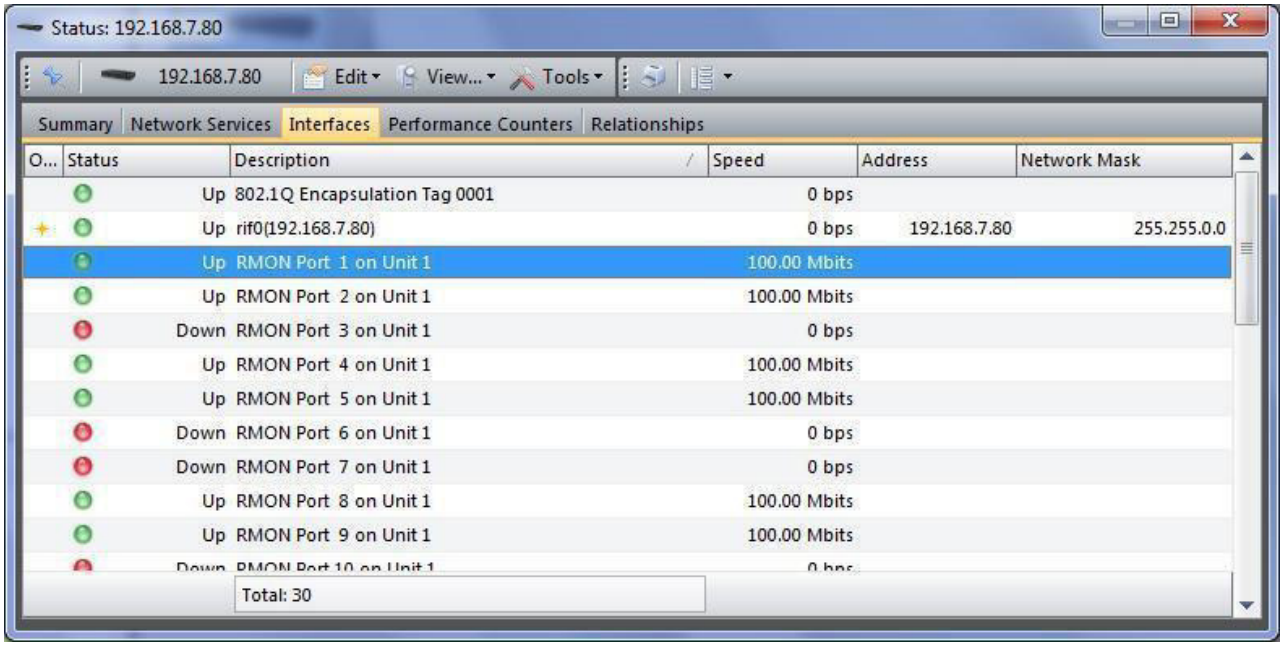


Рисунок 6 – Детальное описание узла сети

5. **Сортировка хостов по типу ОС.** Выбрав слева на панели управления пункт Operating Systems можем увидеть количество хостов активных и недоступных в данныймомент, а так же распределение хостов по типу операционной системы.

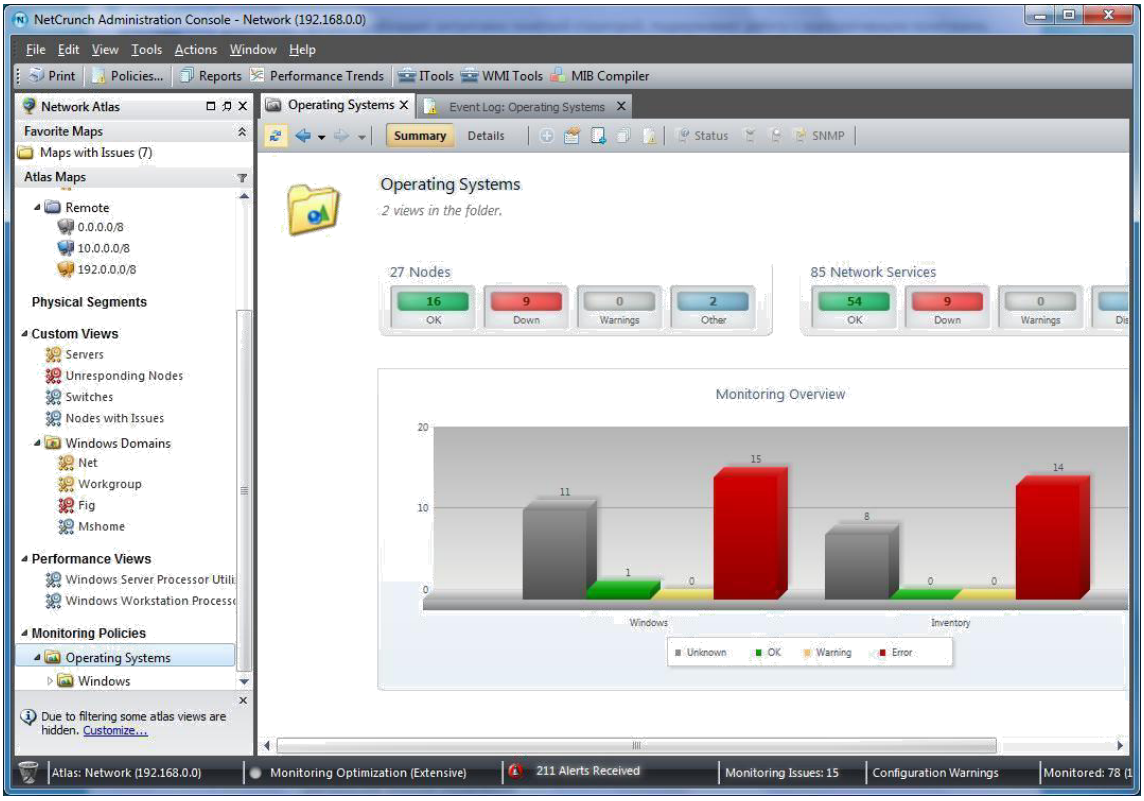


Рисунок 7 – Количество хостов и тип ОС

6. Мониторинг состояния устройств. Перейдем на вкладку Monitoring. Здесь мы можем видеть список всех устройств в сети, доступные сервисы, время последнего опроса.

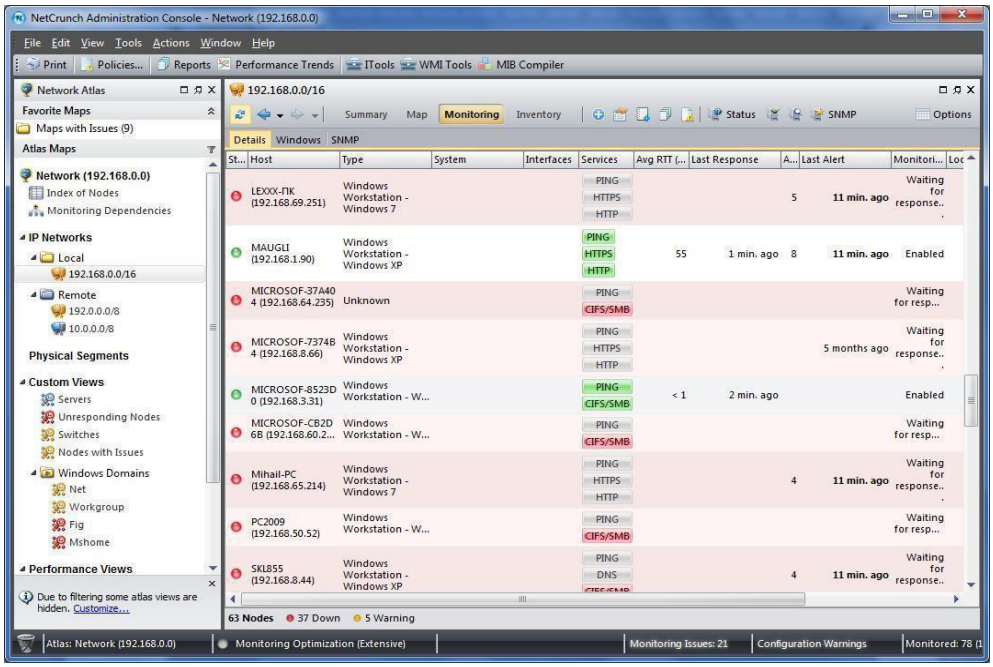


Рисунок 8 – Состояние и доступность устройств в сети

7. Построение карты вычислительной сети. NetCrunch позволяет построить карту сети с отображением подключений хостов к сетевому оборудованию (коммутаторам, маршрутизаторам и другим устройствам) и связей между ними.

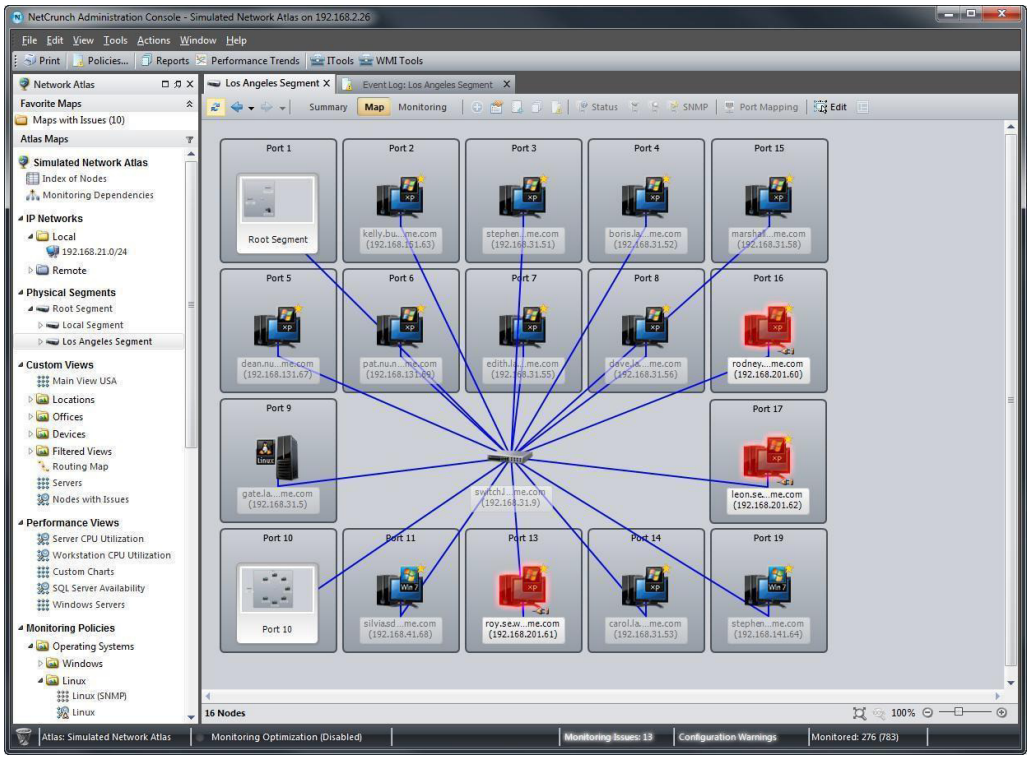


Рисунок 9 – Построение карты вычислительной сети

Практическое задание №9

Цель: Ознакомиться с теоретическими аспектами защиты информации от вредоносных программ: разновидностями вирусов, способами заражения и методами борьбы. Ознакомиться с различными видами программных средств защиты от вирусов.

Ход работы.

Задание 1.

Изучить антивирусный пакет Антивирус Касперского.

Порядок выполнения

1) Сканирование папок на наличие вирусов:

Двойным щелчком на значке антивируса на панели индикации открыть главное окно программы;

Изучить содержимое окна: обратить внимание на дату последнего обновления антивирусной базы и дату последней полной проверки компьютера;

В своей личной папке создать папку Подозрительные файлы и создать там 2 файла: Текстовый файл и Документ Microsoft Word.

Выбрав пункт в главном окне программы пункт Проверка – Быстрая проверка и добавить в окно заданий папку Подозрительные файлы.

Выполнить проверку папки. По завершению сканирования, используя кнопку «Отчеты» - «Сохранить как...», сохранить отчет с результатами проверки в папке Подозрительные файлы.

2) Обновление антивирусной базы:

Нажмите на пункт Обновление и, используя кнопку Обновить, осуществите обновление базы известных вирусов.

По завершению обновления, используя кнопку «Отчеты» - «Сохранить как...»,, сохранить отчет об обновлении в папке Подозрительные файлы.

Задание 2.

Изучить антивирусный пакет Avast!

Порядок выполнения;

1) Найдите иконку антивируса Avast! В системном трее, правой кнопкой мышки вызовите меню и выберите «Открыть интерфейс пользователя Avast!»

2) Перейдите на вкладку «Сканировать компьютер». Вам будет представлены 4 вида сканирования: Экспресс, Полное, Сканирование носителей и возможность выбрать папку для сканирования вручную.

3) Выберите «Сканирование съемных носителей» и нажмите кнопку «Пуск» в окне антивируса – будут автоматически проверены все подключенные к компьютеру съемные носители (диски, флэшки, дискеты).

4) По завершении сканирования выберите четвертый вид сканирования и вручную укажите любую папку на вашем съемном носителе и проверьте её.

5) Во вкладке «Экраны в реальном времени», в подменю «Экран файловой системы» нажав кнопку «Расширенные настройки» вы можете разрешить/запретить антивирусу следующие действия:

– Сканировать программы при выполнении (например, программа excel.exe будет сканироваться при каждом выполнении Microsoft Excel);

– Сканировать сценарии при выполнении (например, файл JS (JavaScript) будет сканироваться при каждом его выполнении);

– Сканировать библиотеки (DLL) при загрузке (при выполнении программы будут сканироваться её вспомогательные файлы – библиотеки DLL и т.д.);

6) Во вкладке «Экраны в реальном времени», в подменю «Веб-экран» нажав кнопку «Расширенные настройки» вы можете разрешить/запретить антивирусу следующие действия:

– Включить веб-сканирование;

– Использовать интеллектуальное сканирование потока;

7) Во вкладке «Обслуживание» в подменю «Обновить» есть возможность ручного запуска обновлений для «Модуля сканирования и определения вирусов» и непосредственно для программы. (По умолчанию модуль обновляется автоматически, а обновление программы запрашивает разрешения пользователя).

8) По завершению сканирования, используя кнопку «Отчеты» -«Сохранить как...», сохранить отчет с результатами проверки

Задание 3.

Изучить антивирусный пакет Dr. Web CureIt

При запуске этого портативного антивируса вам будет предложено запустить его в режиме усиленной защиты – он необходим в случае, если вредоносные программы блокируют работу операционной системы. Нажмите «Отмена».

Далее появится предупреждение, т.к. использование антивируса бесплатно доступно только для лечения домашних компьютеров. Нажмите «Нет».

Нажмите «Пуск» и будет автоматически запущены быстрая проверка компьютера.

В этом режиме проверяются:

- Оперативная память;
- Загрузочные секторы всех дисков;
- Объекты автозапуска;
- Корневой каталог загрузочного диска;
- Корневой каталог диска установки Windows;
- Системный каталог Windows;
- Папка Мои Документы;
- Временный каталог системы;
- Временный каталог пользователя;

По окончании быстрой проверки выбрать в меню пункт «Выборочно» и указать путь к съемному носителю – выполнить его проверку.

По завершению сканирования, используя кнопку «Отчеты» - «Сохранить как...», сохранить отчет с результатам и проверки

Вопросы для контроля:

1) Что называется компьютерным вирусом?
2) Какая программа называется "зараженной"?
3) Каковы признаки заражения вирусом?
4) Какие методы защиты от компьютерных вирусов можно использовать?
5) Перечислите меры защиты информации от компьютерных вирусов.

Практическое задание №10

Цель: Научиться работать с программами для удаленного администрирования TeamViewer, AmmyAdmin.

Ход работы.

Практическое задание №11,12

Цель: получить навыки по установке и использованию программного обеспечения «OCSNG» для инвентаризации аппаратных и программных ресурсов корпоративной сети в соответствии с ГОСТ 27001.

ИТ-ИНВЕНТАРИЗАЦИЯ

Инвентаризация аппаратных и программных ресурсов корпоративной сети или ИТ-инвентаризация – это комплекс работ по составлению перечня оборудования и программного обеспечения, составляющих ИТ-инфраструктуру организации (рабочие станции, серверы, сетевое оборудование, периферийные устройства, ПО и т.д.). Результатом проведения ИТ-инвентаризации будет являться полная информация о текущем состоянии ИТ-инфраструктуры и повышение эффективности использования имеющихся ИТ-ресурсов [1].

ИТ-инвентаризация рекомендуется в следующих случаях:

- для оценки стоимости ИТ-инфраструктуры;
- для независимой оценки актуальности и современности оборудования и программного обеспечения;
- перед началом модернизации и оптимизации ИТ-инфраструктуры;
- для учета и контроля ИТ-ресурсов компании;
- при смене персонала ИТ-отдела (в частности, при изменении материально-ответственного лица компании).

В ходе ИТ-инвентаризации выполняются следующие работы:

- с заказчиком согласовываются объекты, подлежащие инвентаризации;
- выполняется сбор информации об аппаратной части ИТ-инфраструктуры и используемых периферийных устройствах;
- составляется список используемого программного обеспечения с указанием версии и информации о лицензиях;
- выполняется анализ структуры локальной сети и используемого сетевого оборудования;
- составляется схема маршрутизации передаваемой информации в локальной сети;
- составляется список внешних каналов связи с указанием технологий и провайдеров услуг;
- выполняется оценка производительности и стоимости инвентаризированной ИТ-инфраструктуры.

По завершению ИТ-инвентаризации заказчику предоставляется отчѐт о проделанной работе и вся собранная информация, которая в дальнейшем может служить основой для проведения ИТ-аудита.

Существует множество инструментальных средств для проведения ИТ-инвентаризации и ведения учета ИТ-ресурсов как бесплатных, так и за деньги, например, OCS Inventory NG, GLPI, Audit Pro, Total Network Inventory и т.д.

Наиболее удобной считается бесплатная система OCS Inventory NG с открытым кодом, т.е. можно вносить изменения в код системы для настройки.

СИСТЕМА OCSNG

Система OCS Inventory NG (OCSNG, Open Computers and Software Inventory New Generation) предназначена для инвентаризации компьютеров в локальной сети, комплектующих, переферийного оборудования и программного обеспечения [2].

Также с ее помощью можно удаленно разворачивать программы на рабочих местах и получать информацию о сетевой конфигурации. OCS Inventory NG является

клиент-серверным приложением. Для сбора информации об установленном оборудовании с клиентских компьютеров и серверов используется программа-агент.

Все собранные данные, агенты отсылают на сервер управления, в виде XML потока сжатого при помощи Zlib, для передачи используется стандартный протокол HTTP/HTTPS. Сервер OCSNG состоит из 4 компонентов, которые могут быть установлены на одном или нескольких компьютерах:

- база данных – используется для хранения информации, поддерживается MySQL от 4.1;
- служба связи – обеспечивает связь по протоколу HTTP между сервером базы данных и программами-агентами, требуется Apache Web Server 1.3.X/2.X с интегрированным Perl (в Debian/Ubuntu пакет libapache-dbi-perl);
- служба развертывания – предназначен для хранения установочных файлов программ-агентов, подходит любой веб-сервер с поддержкой SSL;
- консоль управления – просмотр собранных данных в браузере, требуется веб-сервер с поддержкой PHP (с активированными ZIP и GD).

Серверная часть OCSNG может быть установлена на компьютер работающий под управлением Windows 2000 Professional/Server, XP Professional Edition и 2003, а также Linux, FreeBSD, OpenBSD, NetBSD, Solaris, IBM AIX и MacOS X.

Агент доступен для клиентских и серверных версий Windows от 95 до Server 2008 R2, а также перечисленных Linux (2.4/2.6, x86, x86_64/AMD64, Sparc64, ARM, PowerPC), MacOS X (10.3 – 10,5), FreeBSD/OpenBSD/NetBSD (x86/Sparc), Solaris 8, 9, 10 (x86/Sparc), IBM AIX (5.1 – 5.3) и HP-UX [3].

Распространяется система OCS Inventory NG по лицензии GPL v2 и является Open Source проектом.

БД результатов инвентаризации OCSNG может использоваться в связке с другой системой управления аппаратными и программными ресурсами сети GLPI (Guestion Libre de Parc Informatique), которая имеет более расширенный функционал.

Система GLPI предназначена для работы с базой данных ИТ и телекоммуникационного оборудования, установленного на предприятии. Также имеется возможность ведения учета расходных материалов и организации службы технической поддержки по расписанию и по заявкам пользователей.

ВЫПОЛНЕНИЕ РАБОТЫ

1. Для развертывания системы OCSNG необходимо установить серверную и клиентские части системы.
2. Для установки серверной части OCSNG есть варианты: развернуть готовый образ Vmware с установленной серверной частью или установить серверную часть вручную, а также для Windows и Unix подобный систем с разрядностями 32 и 64-bit. В нашем случае выбираем образ Vmware Debian 32-х разрядной системы с установленной серверной частью OCSNG.
3. Скачиваем образ Unix-подобной 32-х разрядной ОС и распаковываем.
4. Запускаем Vmware Workstation или Vmware player и подключаем образ ОС Debian (Рисунок 1).

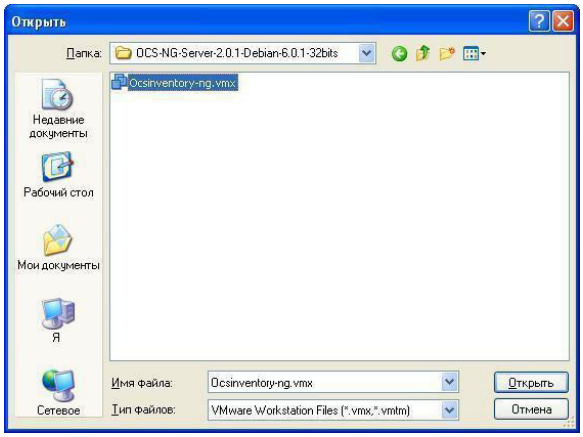


Рисунок 1 - Выбор образа ОС Debian

5. Загружаем ОС Debian. Идет запуск сервисов ОС Debian (Рисунок 2).

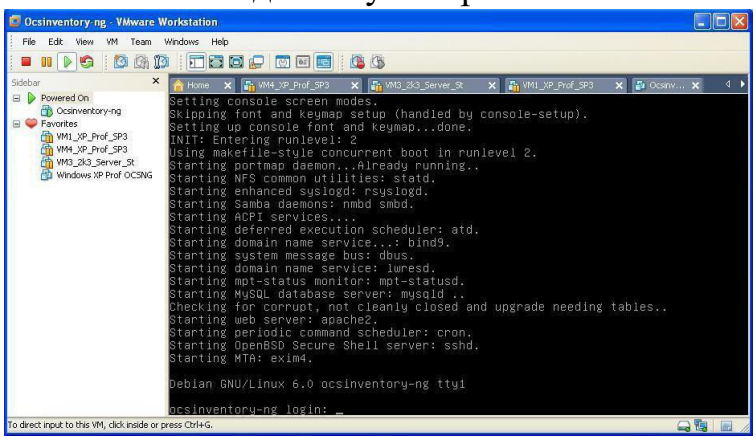


Рисунок 2 - Процесс загрузки ОС Debian

6. При запросе учетной записи вводим имя: **root** и пароль: **ocs** (Рисунок 3)

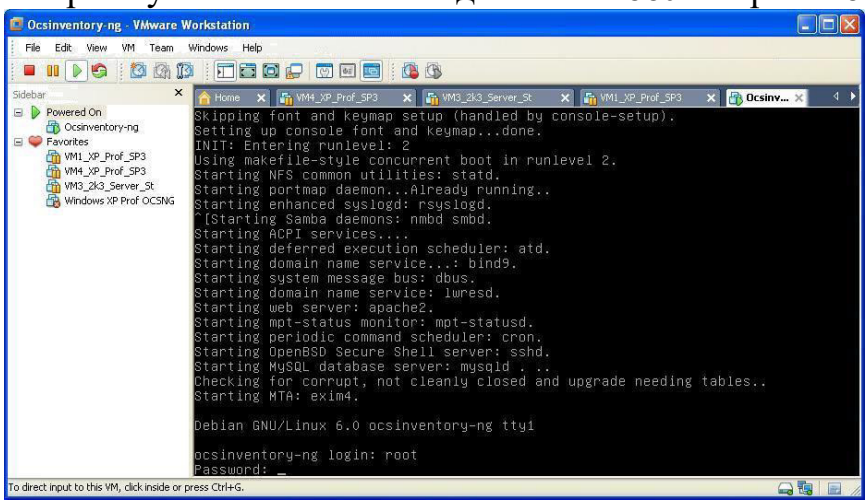


Рисунок 3 - Запрос ввода учетной записи root

7. После входа под учетной записью root проверяем конфигурацию виртуальной машины сервера OCSNG (Рисунок 4).

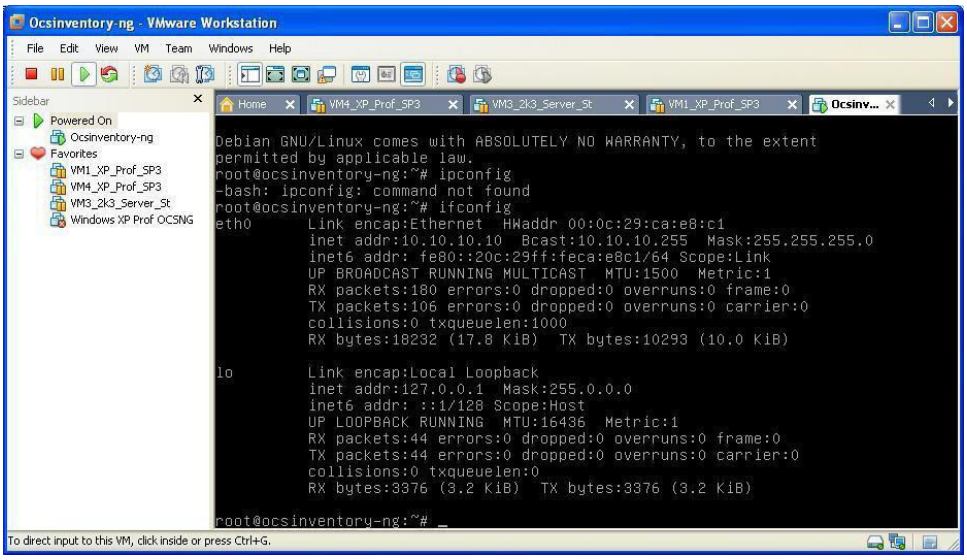


Рисунок 4 - Результат работы команды ifconfig

8. Для сбора инвентаризационных данных с каждого компьютера сети и занесения в БД сервера OCSNG необходимо на каждый пользовательский компьютер установить клиентскую часть - агента OCSNG.

9. Создаем новую виртуальную машину Vmware с операционной системой Windows XP. Скачиваем и устанавливаем VMware Workstation [5]. Настраиваем виртуальную машину: устанавливаем тип соединения сетевой карты клиента в режим Bridged и сетевые настройки клиента из подсети сервера OCSNG (Рисунок 5).

Рисунок 5 - Установка режима Bridged настройка сетевых параметров клиента

10. Проверяем видимость сервера и клиента OCSNG между собой командой Ping (Рисунок 7,8).

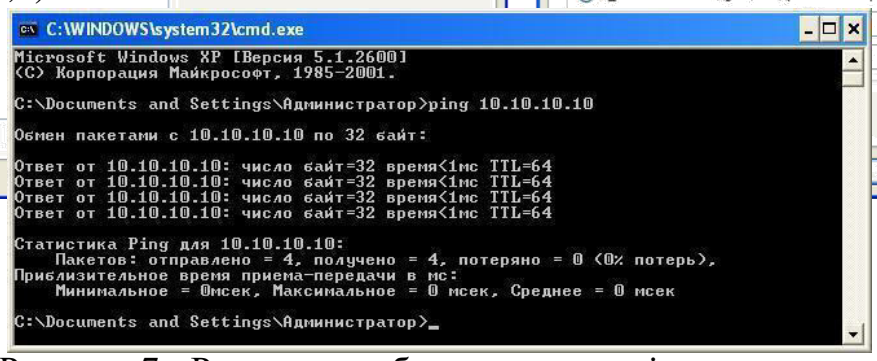


Рисунок 7 - Результат работы команды ping на клиенте

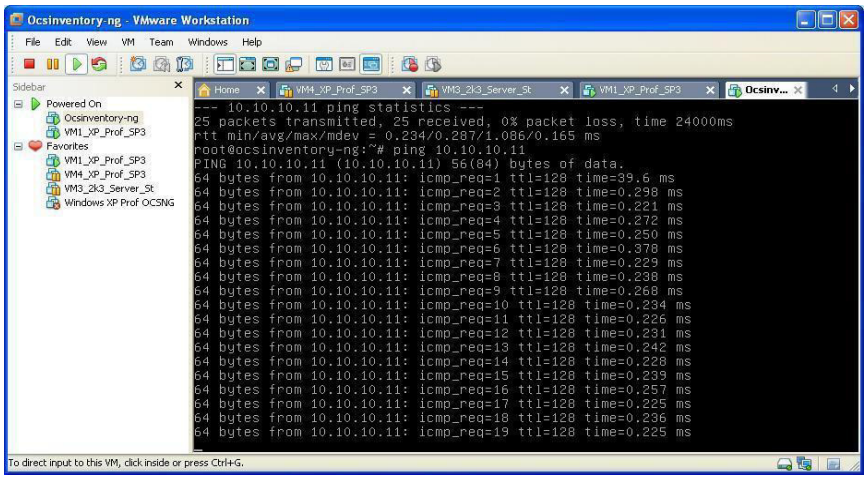
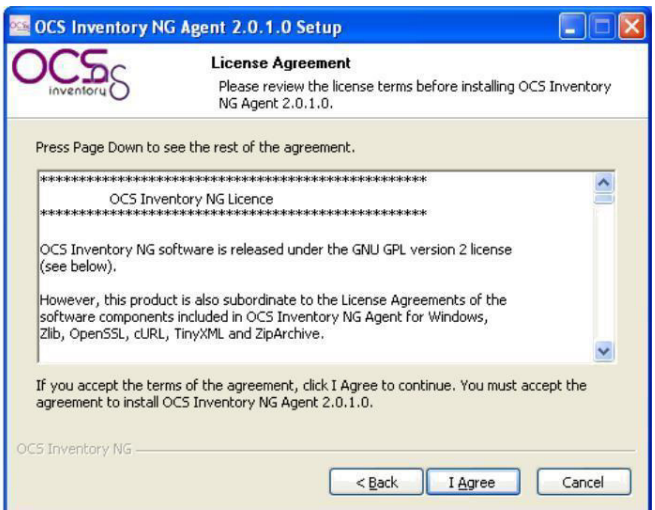


Рисунок 8 - Результат работы команды ping на сервере

11. Скачиваем OCSNG-Windows-Agent-2.0.1.zip и распаковываем.
12. Запускаемустановкуагента OCS-NG-Windows-Agent-Setup.exe (Рисунок 9-13).



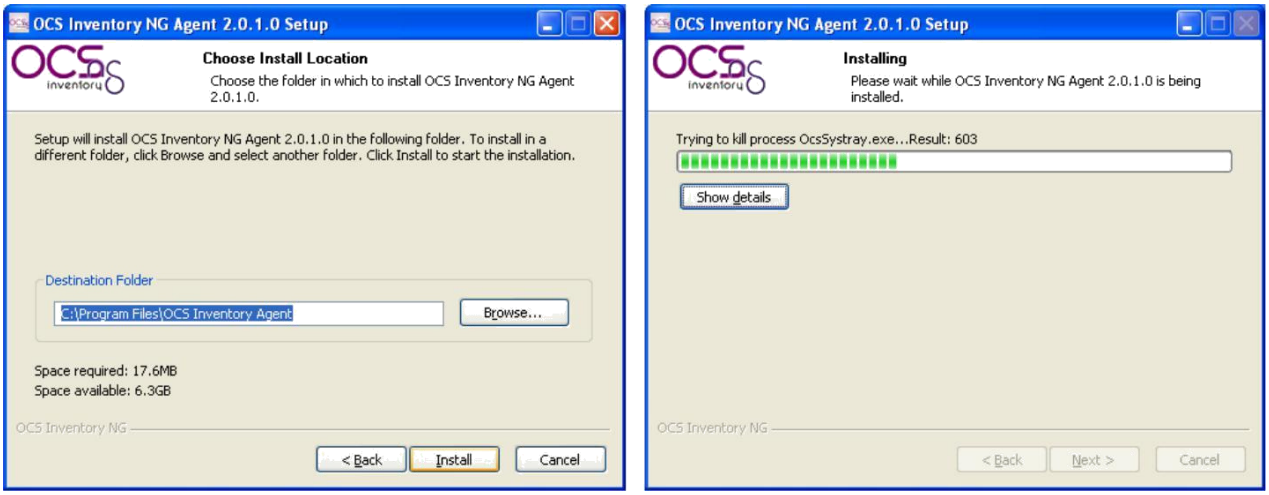


Рисунок 9 - Начальное окно установки и лицензионное соглашение агента

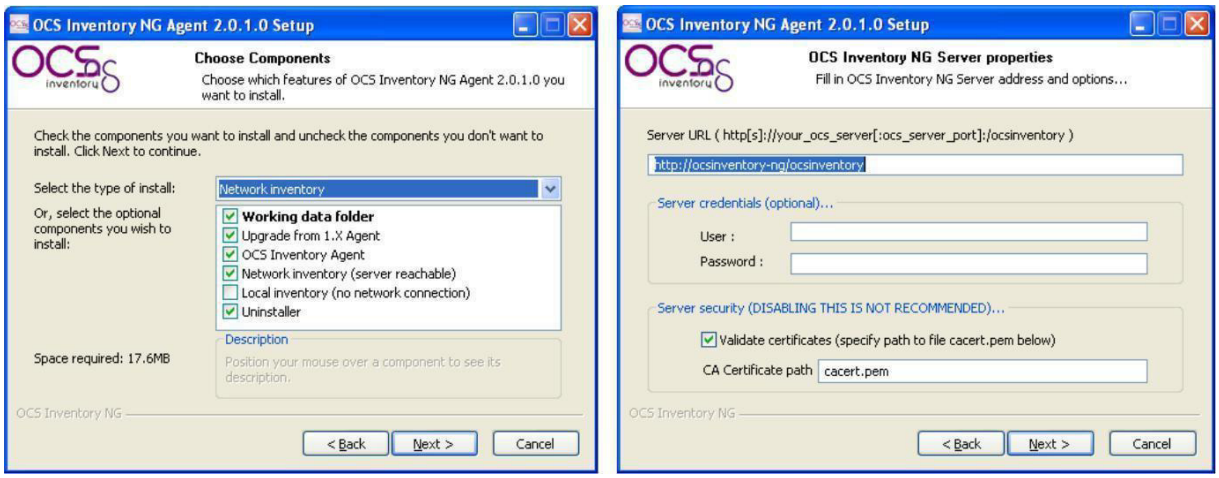


Рисунок 10 - опции клиента и установка настроек подключения к серверу

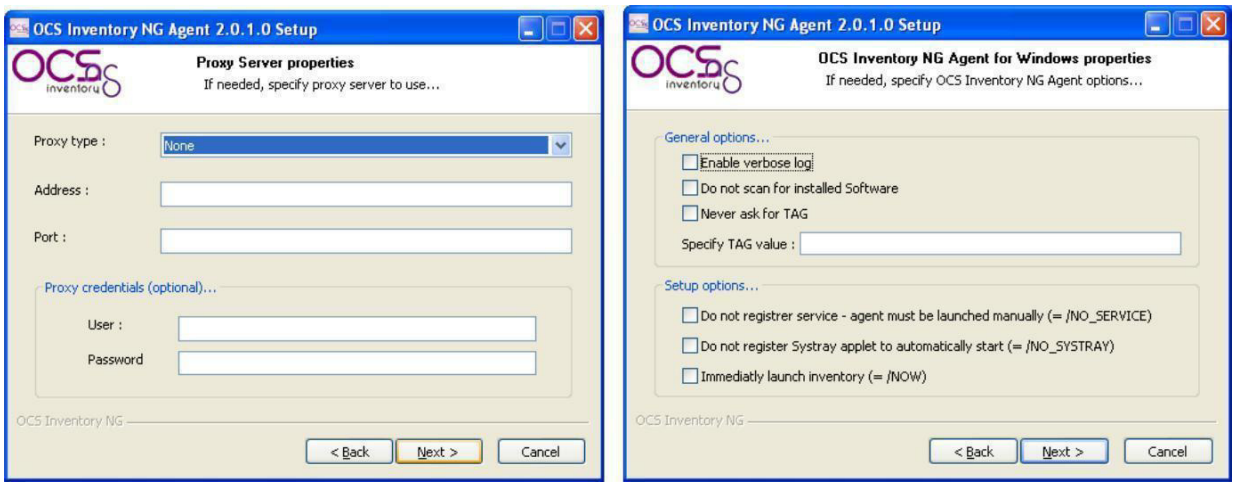


Рисунок 11 - Настройка параметров proxy и выбор настроек агента сервера

Рисунок 12 - Выбор папки установки агента и процесс установки агента

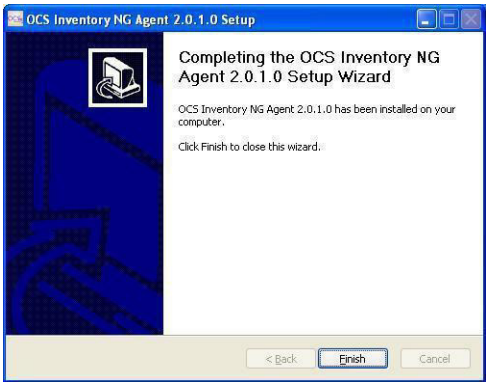


Рисунок 13 - Окончание установки агента

13. После завершения установки агента OCSNG проверяем результат в лог-файле (Рисунок 14).

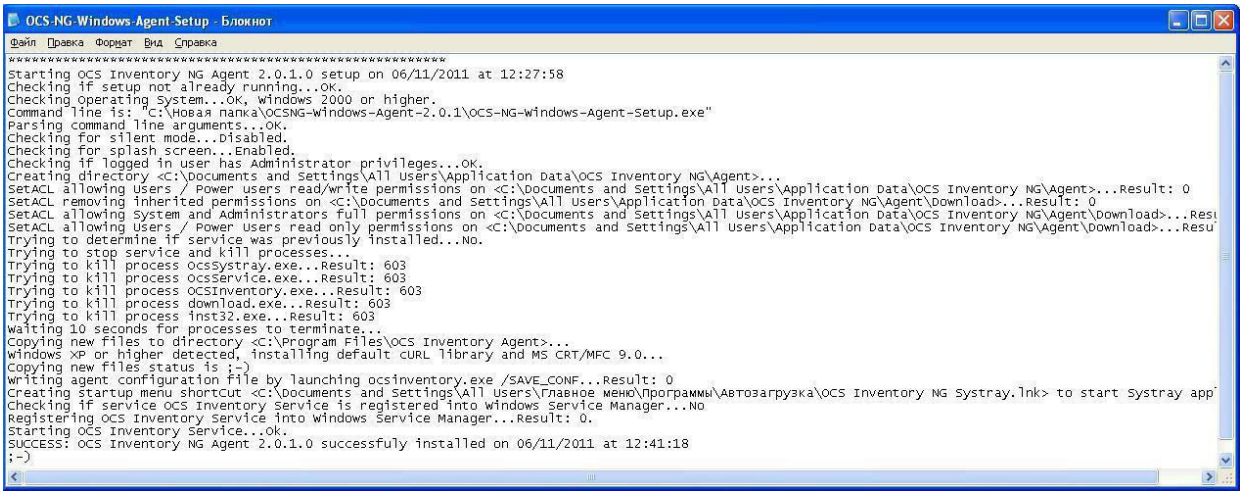


Рисунок 14 - Лог-файл процесса установки агента

Перезагружаем клиентский компьютер, в трее появился значок агента OCSNG.

- Проверяем результат работы агента OCSNG (Рисунок 15).

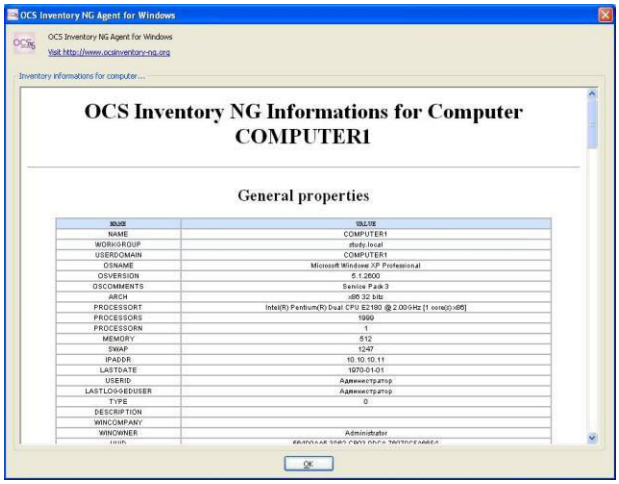


Рисунок 15 - Результат работы агента на клиенте

16. Для подключения к серверу OCSNG загружаем административную консоль. В адресной строке браузера набираем http://ocsinventory-ng/ocsreports/ и подключаемся с учетной записью: имя **admin**, пароль **admin**. Для удобства выбираем русский язык интерфейса (Рисунок 16).

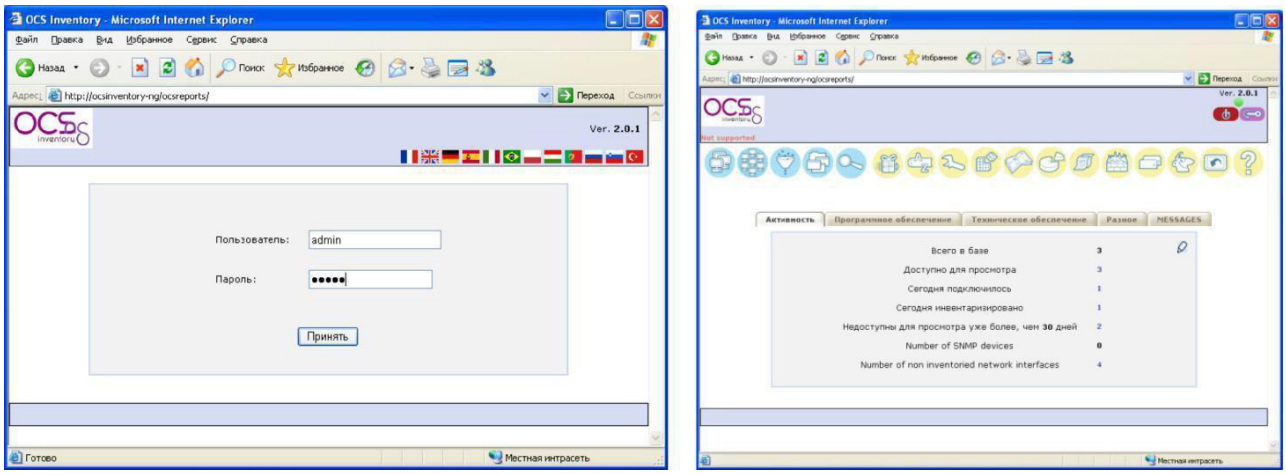


Рисунок 16 - Окно регистрации консоли сервера и статистика работы агентов в сети

16. Просматриваем список проинвентаризированных компьютеров, на которых установлен агент OCSNG (Рисунок 17).

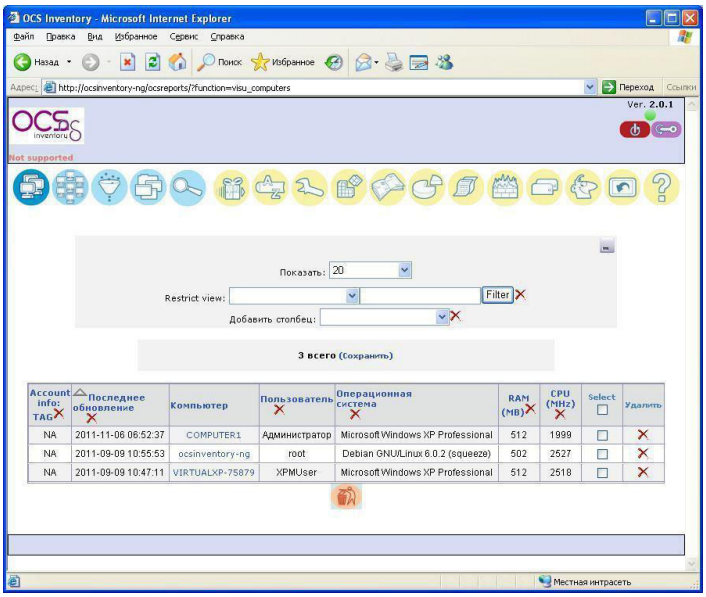


Рисунок 17 - Список проинвентаризированных компьютеров

18.Выбираем из списка компьютер COMPUTER1 (Рисунок 18).

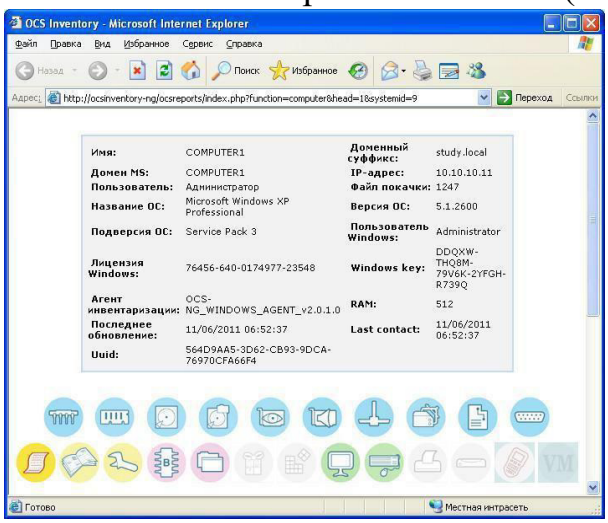


Рисунок 18 - Информация по выбранному компьютеру COMPUTER1

19. Выбирая в нижней части окна иконку одной из группировок результата инвентаризации, можно просмотреть содержание этой группы, например, процессоры. Если выбрать иконку двойной стрелки в нижней части экрана, то отобразится полная информация по выбранному компьютеру (Рисунок 19).

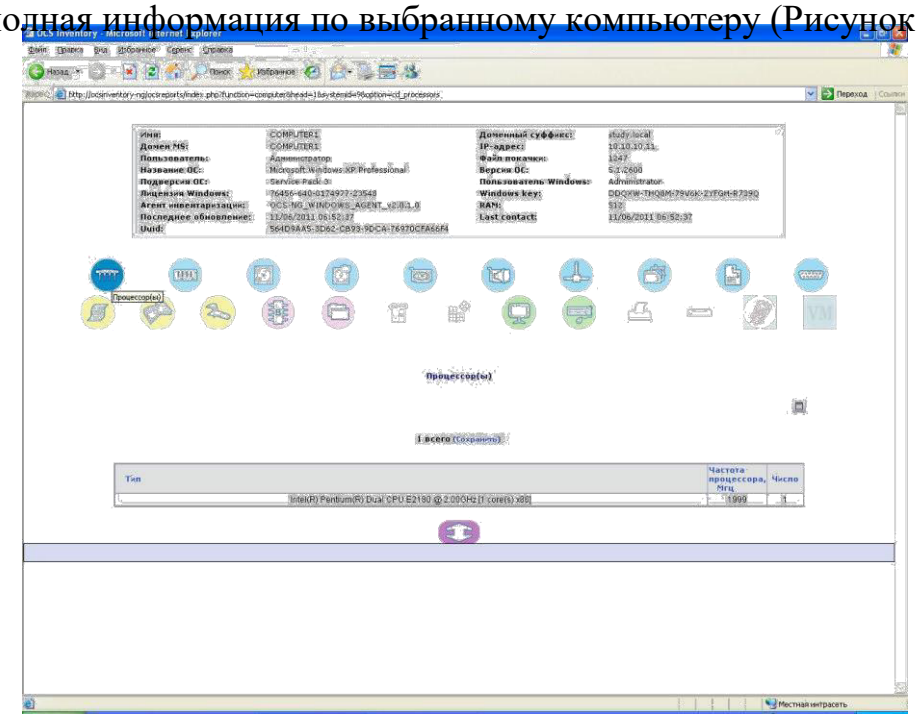


Рисунок 19 - Просмотр раздела «Процессор(ы)»

20. Помимо инвентаризации внутренней аппаратной части компьютера

OCSNG собирает информацию по программному обеспечению, а также по подключенным периферийным устройствам, например, монитор, принтер, источник бесперебойного питания (Рисунок 20).

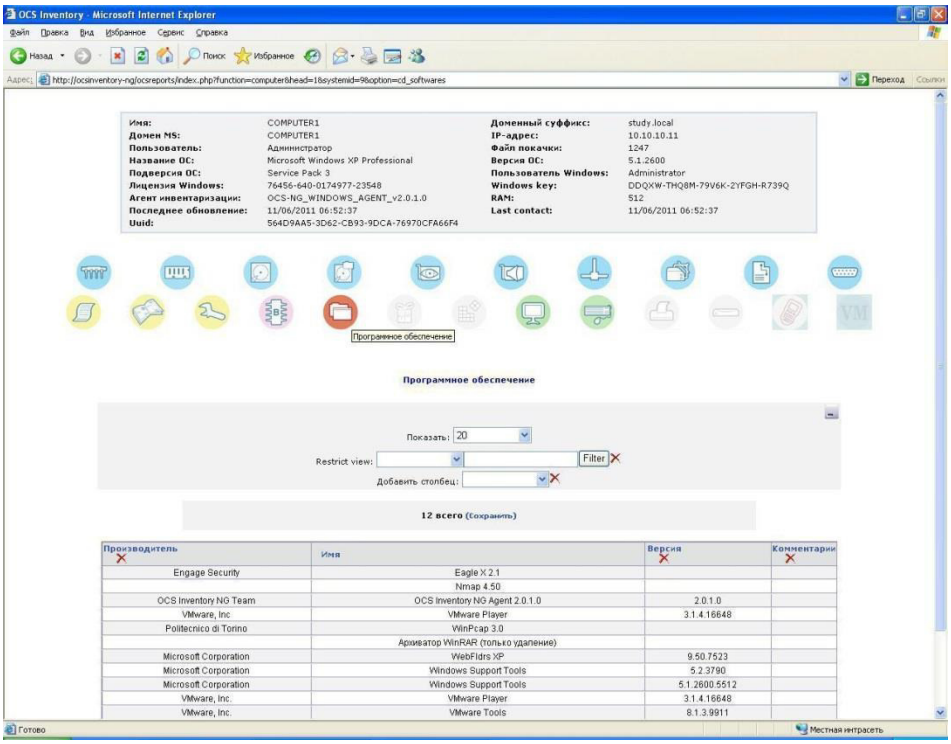


Рисунок 20 - Просмотр раздела «Программное обеспечение»

21.БД результатов инвентаризации OCSNG может использоваться в связке с другой системой управления аппаратными и программными ресурсами сети GLPI (Gestionnaire libre de parc informatique), которая имеет более расширенный функционал (Рисунок 21).

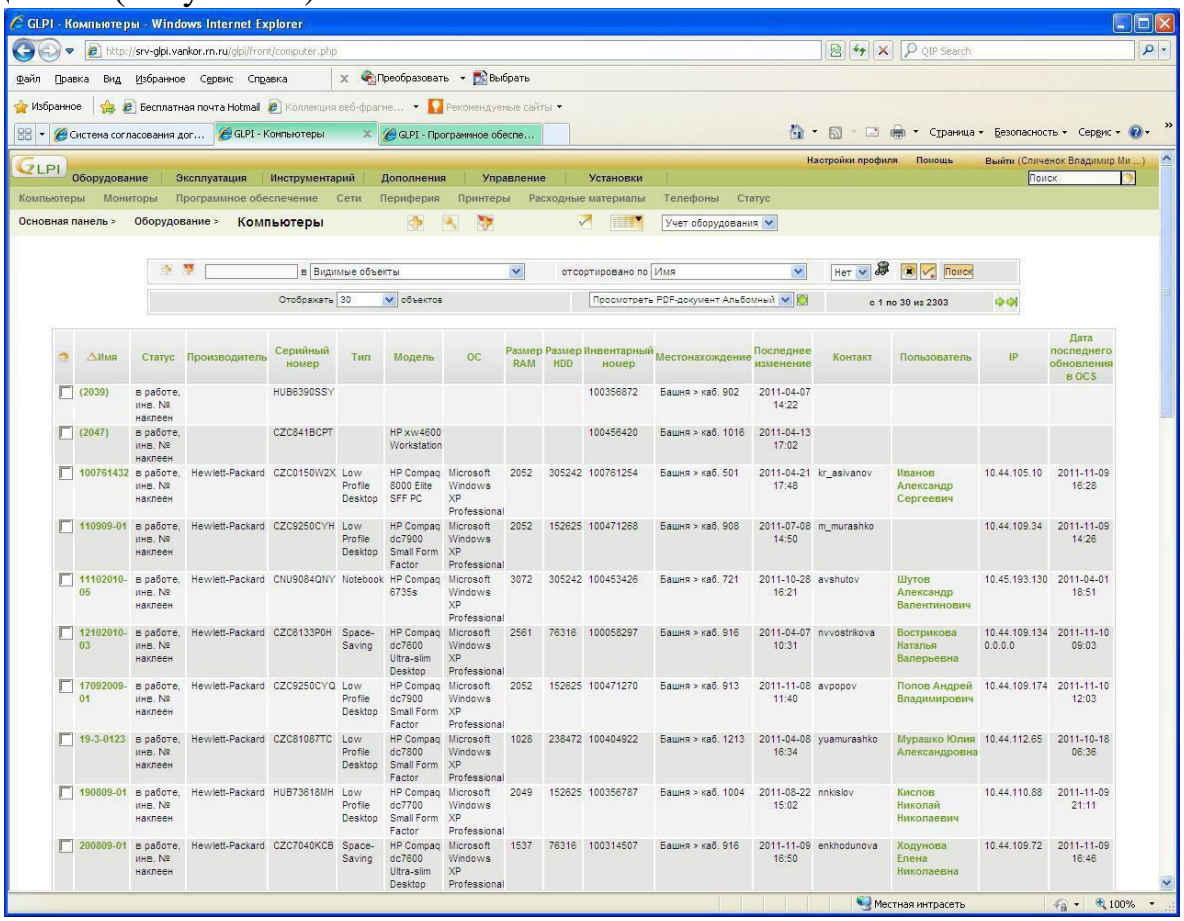


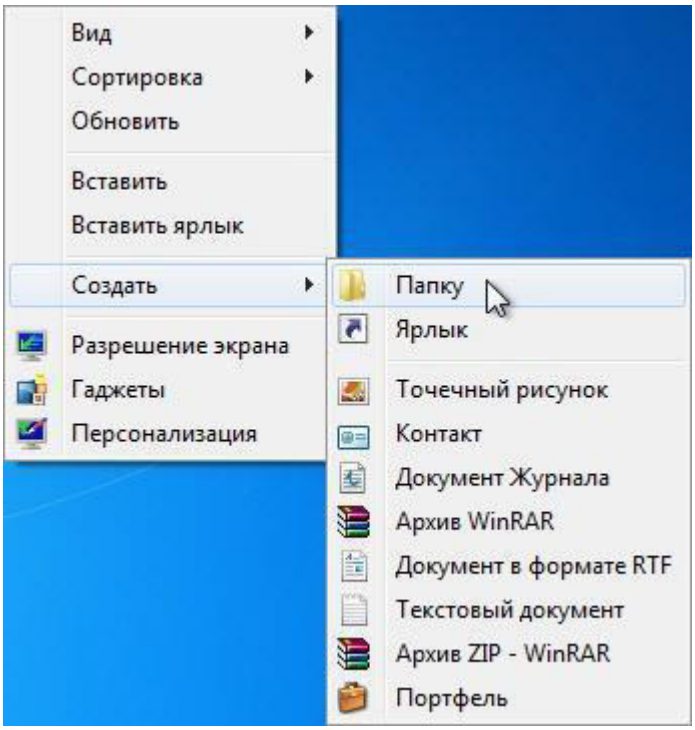
Рисунок 21 - Список проинвентаризированных компьютеров в системе GLPI

Практическое задание №13

Цель: Научиться настраивать межсетевой экран Windows 7.

Действие 1

На компьютере 1 щёлкните правой кнопкой мыши рабочий стол и выберите **Создать > Папку**.



Задайте имя новой папке - TEST.

Щёлкните правой кнопкой мыши на папке TEST и выберите **Предоставить общий доступ >**

Расширенная настройка общего доступа > Расширенная настройка общего доступа.

Откроется окно «Расширенная настройка общего доступа».

Предоставьте общий доступ к этой папке, используя имя по умолчанию TEST.

На компьютере 2 нажмите кнопку **Пуск**, затем выберите **Панель управления > Центр управления сетями и общим доступом > Сеть**.

Дважды щёлкните **компьютер 1**.

Видна ли теперь общая папка TEST?

Примечание. Если ответ отрицательный, обратитесь за помощью к инструктору.

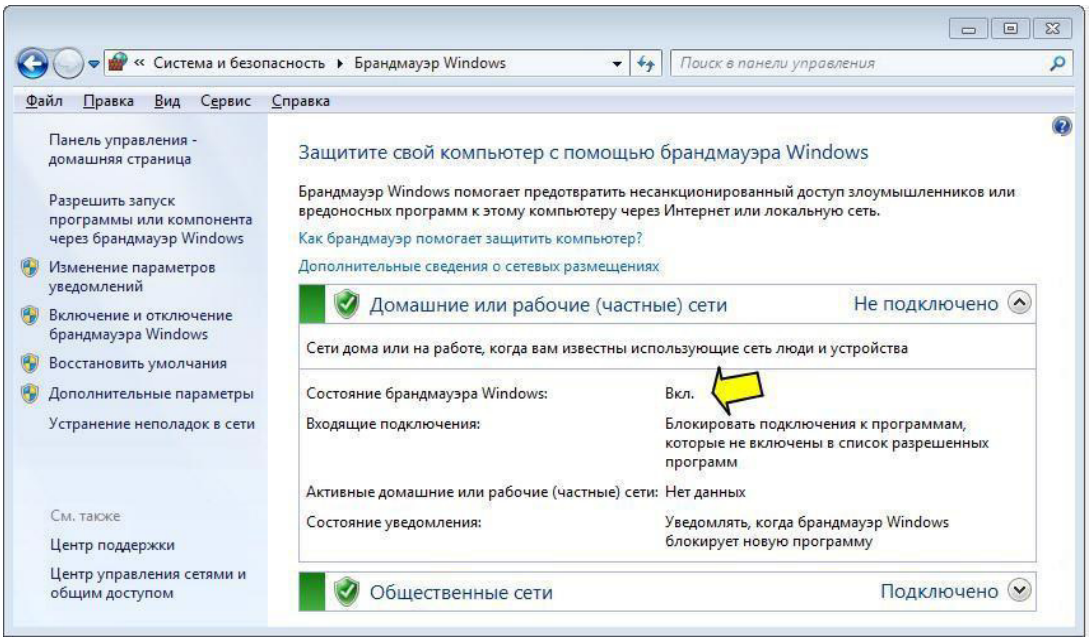
Закройте **Сеть**.

Примечание. При выполнении оставшейся части лабораторной работы используйте компьютер 1, если не указано иначе.

Действие 2

Перейдите к брандмауэру Windows 7.

Выберите **Пуск > Панель управления > Система и безопасность > Брандмауэр Windows**.

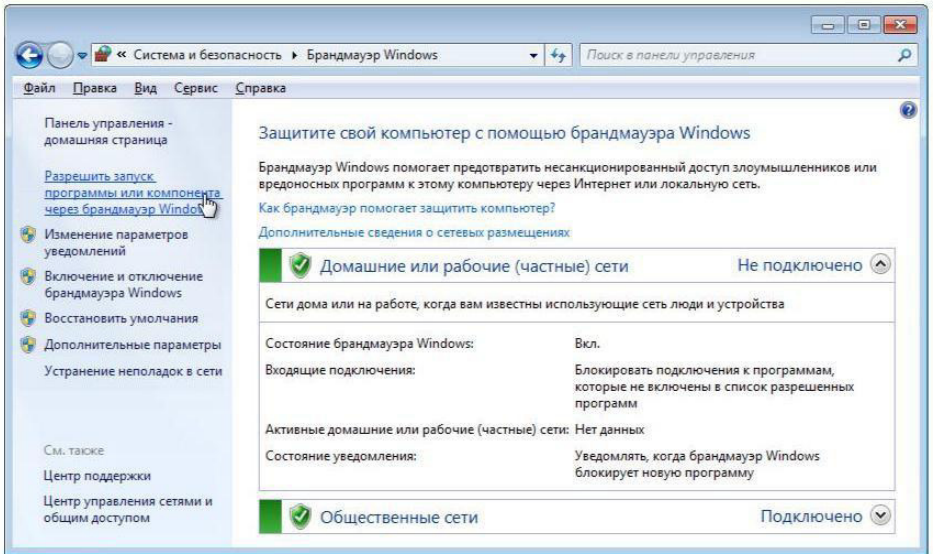


Индикатор брандмауэра показывает состояние брандмауэра. Стандартная настройка – «**Включен**».

В поле ниже укажите преимущества брандмауэра Windows.

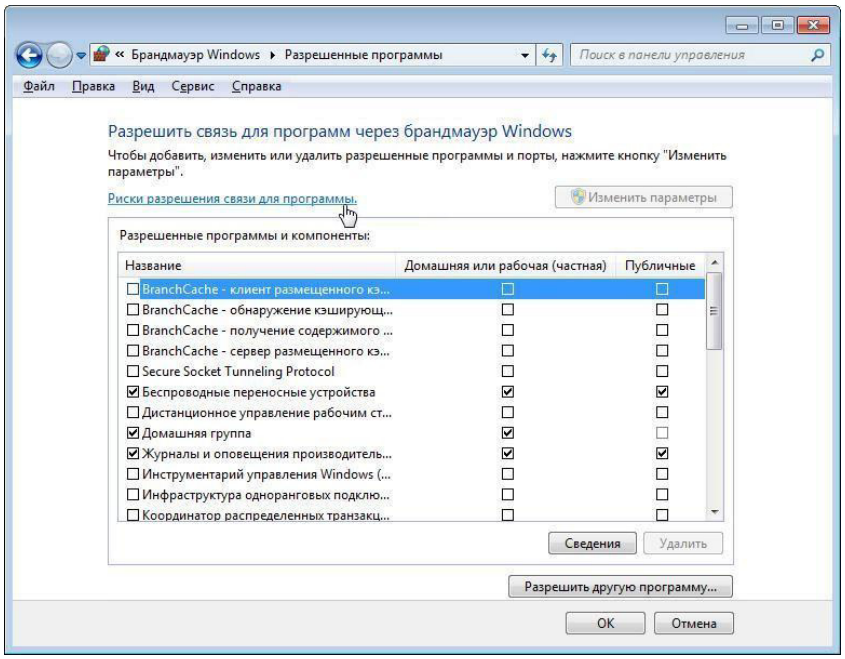
Действие 3

Перейдите по ссылке **Разрешить запуск программы или компонента через брандмауэр Windows**.



Действие 4

Откроется окно «Разрешенные программы».

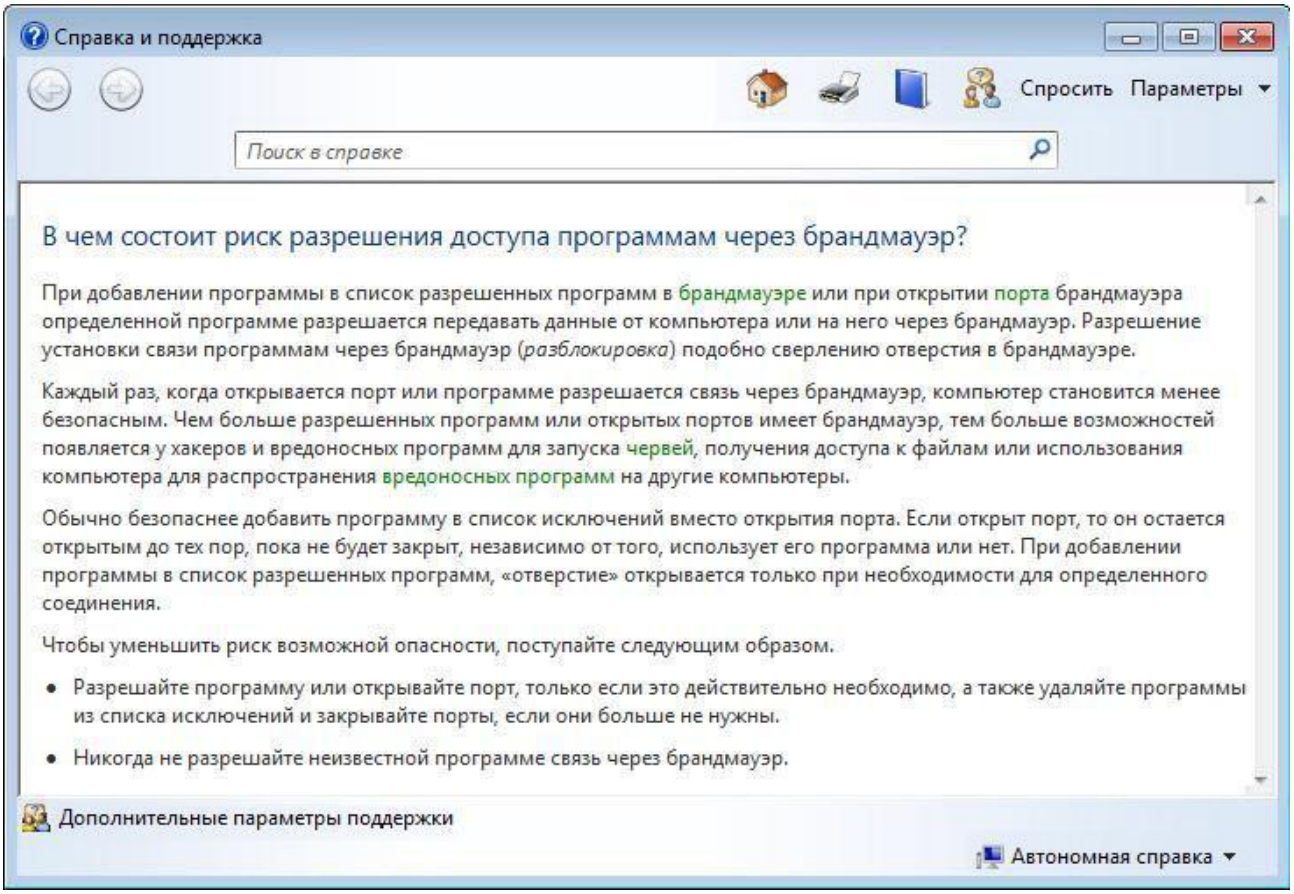


Программы и службы, не блокируемые брандмауэром Windows, будут помечены флажками.

Можно добавлять приложения к этому списку. Это может быть необходимо, если у клиента имеется приложение, требующее связи с внешней сетью, но по какой- то причине брандмауэр Windows не может выполнить настройку автоматически. Для завершения данной процедуры необходимо войти в систему на этом компьютере в качестве администратора.

Перейдите по ссылке **Риски разрешения связи для программы**.

Откроется окно «Справка и поддержка».



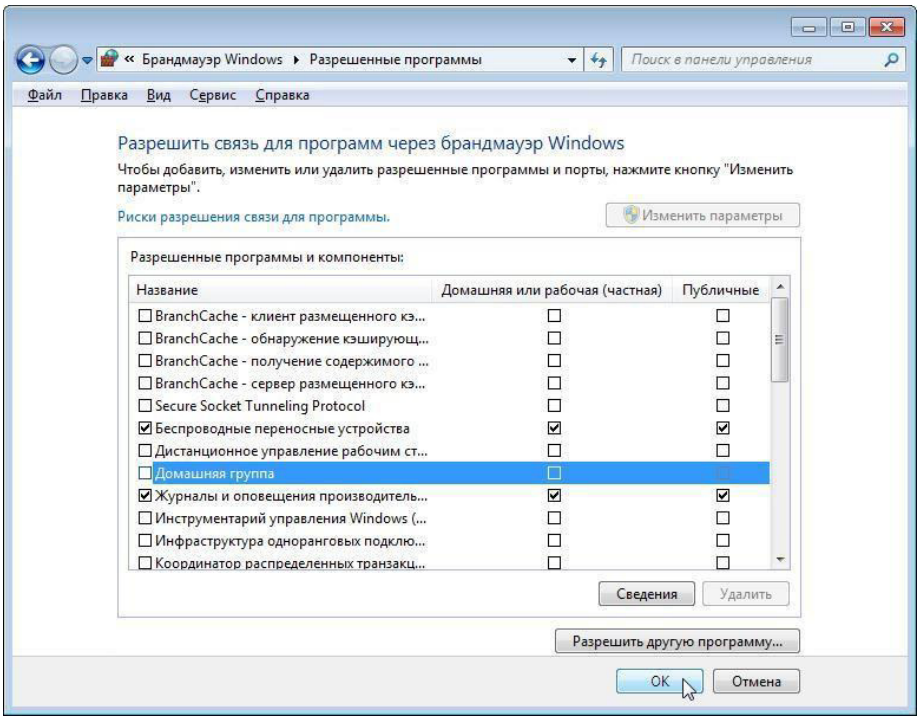
Создание слишком большого числа исключений в файле «Программы и службы» может повлечь негативные последствия. Опишите негативные последствия большого количества исключений.

Закройте окно «Справка и поддержка».

Действие 5

С компьютера 1 выполните следующие действия:

Щёлкните окно «Разрешенные программы», чтобы активировать его.

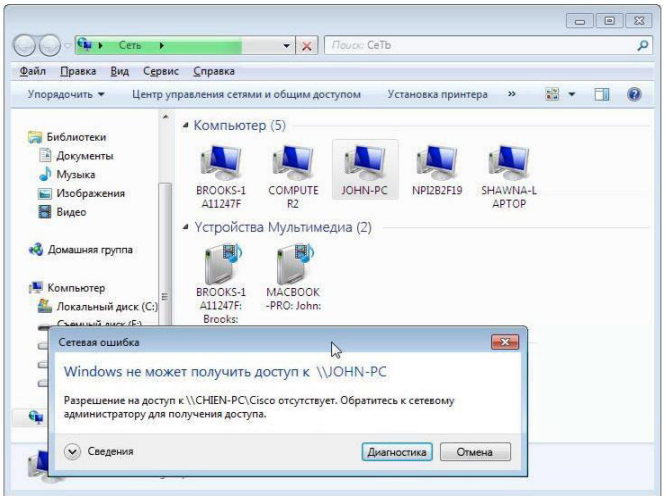


Для отключения исключения снимите флажок **Общий доступ к файлам и принтерам > нажмите кнопку «ОК»**.

С компьютера 2 выполните следующие действия:

Откройте сетевое подключение к компьютеру 1.

Последовательно выберите **Пуск > Панель управления > Центр управления сетями и общим доступом > Сеть**.



Можно ли подключиться к компьютеру 1?

С компьютера 1 выполните следующие действия:

Для включения исключения установите флажок **Общий доступ к файлам и принтерам > нажмите кнопку «ОК»**.

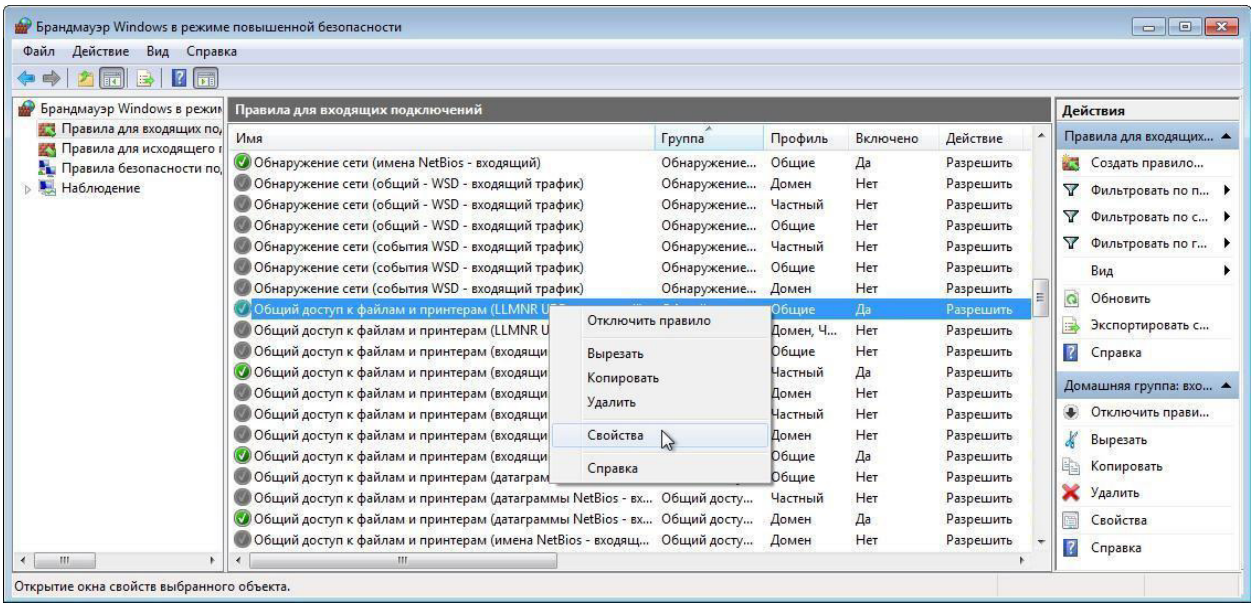
С компьютера 2 выполните следующие действия: Обновите окно **Сеть** и подключитесь к компьютеру 1.

Можно ли подключиться к компьютеру 1?

Завершите сеанс на компьютере 2. Используйте компьютер 1 в оставшейся части лабораторной работы.

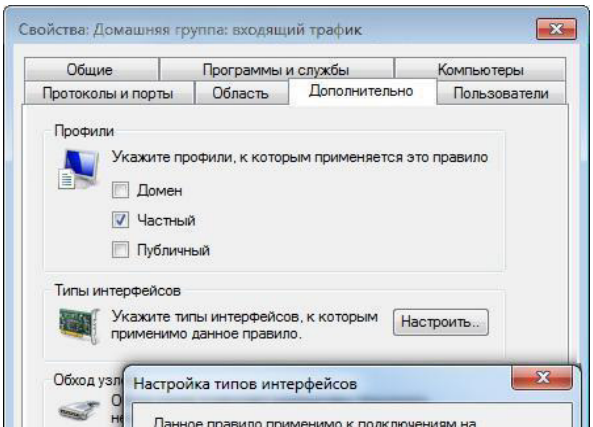
Действие 6

Выберите **Пуск > Панель управления > Система и безопасность > Администрирование > Брандмауэр Windows в режиме повышенной безопасности > Правила для входящих подключений**.



Разверните окно, чтобы можно было увидеть полное имя правил для входящих подключений. Найдите «Общий доступ к файлам и принтерам (эхо-запрос – входящий трафик ICMPv4)».

Щёлкните правило правой кнопкой мыши, выберите **Свойства > вкладка Дополнительно >** нажмите кнопку **Настроить**.

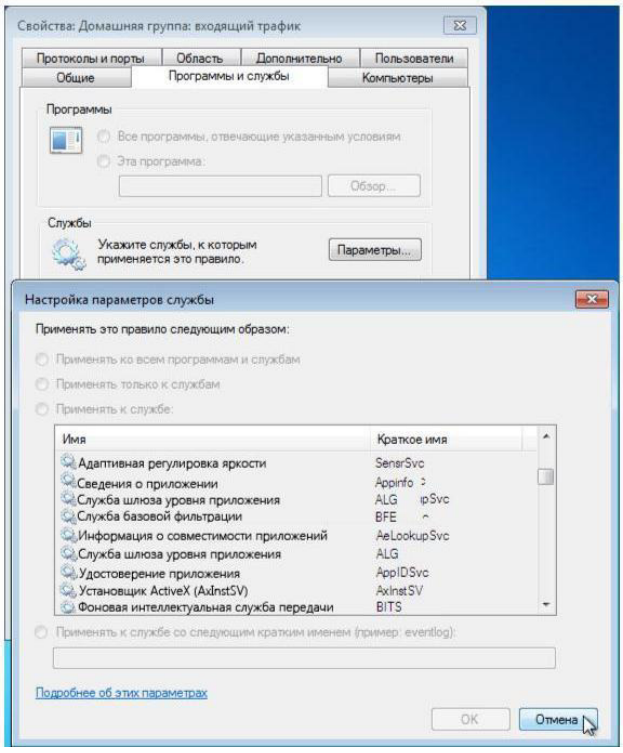


На вкладке «Дополнительно» отображается профиль(-и), используемый компьютером, а в окне «Настройка типов интерфейсов» отображаются различные подключения, настроенные на компьютере.

Нажмите кнопку **ОК**.

Перейдите на вкладку **Программы и службы**.

Откроется окно «Настройка параметров службы».



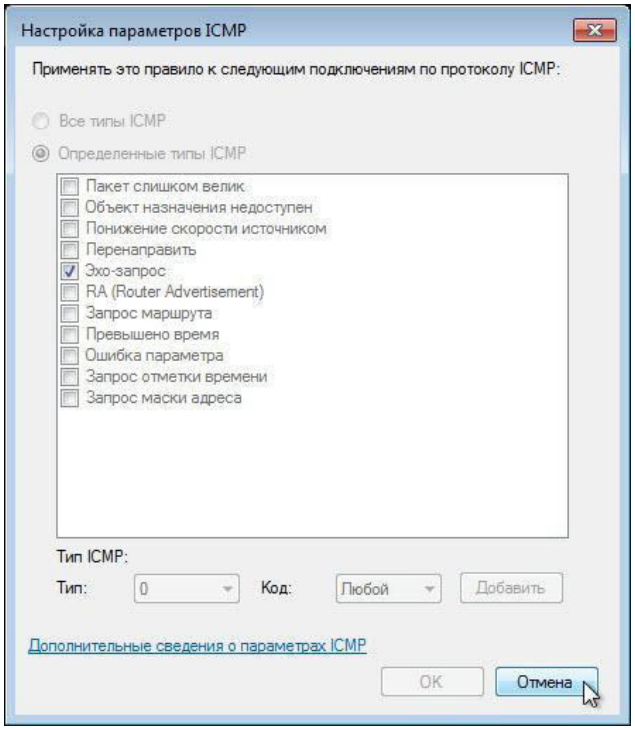
В пространстве ниже перечислите краткие имена четырёх доступных служб.

Нажмите кнопку **Отмена**.

Действие 7

Существует множество приложений, обычно незаметных для пользователя, которым необходимо иметь доступ к компьютеру через брандмауэр Windows. Это команды уровня сети, направляющие трафик в сети и Интернете.

Перейдите на вкладку **Протоколы и порты**. Для настройки ICMP нажмите кнопку **Настроить**. Можно будет увидеть меню, в котором настраиваются исключения ICMP.



В этом примере разрешение входящих эхо-запросов позволяет пользователям сети запрашивать, присутствует ли в ней компьютер. Оно также позволяет видеть, насколько быстро передается информация к компьютеру и от него.

В поле ниже перечислите определенные типы ICMP.

Вопросы для контроля:

1) Что такое межсетевой экран?
2) Каковы функции межсетевого экрана?

Практическое задание №14,15

1. Цель работы: изучить лицензионные и свободно распространяемые программные продукты; научиться осуществлять обновление программного обеспечения с использованием сети Интернет.

2. Оборудование, приборы, аппаратура, материалы: персональный компьютер с выходом в Интернет.

3. Краткие теоретические сведения

Классификация программ по их правовому статусу

Программы по их правовому статусу можно разделить на три большие группы: лицензионные, условно бесплатные и свободно распространяемые.

Лицензионные программы. В соответствии с лицензионным соглашением разработчики программы гарантируют её нормальное функционирование в определенной операционной системе и несут за это ответственность.

Лицензионные программы разработчики обычно продают в коробочных дистрибутивах. В коробочке находятся CD-диски, с которых производится установка программы на компьютеры пользователей, и руководство пользователей по работе с программой.

Довольно часто разработчики предоставляют существенные скидки при покупке лицензий на использовании программы на большом количестве компьютеров или учебных заведениях.

Условно бесплатные программы. Некоторые фирмы разработчики программного обеспечения предлагают пользователям условно бесплатные программы в целях рекламы и продвижения на рынок. Пользователю предоставляется версия программы с определённым сроком действия (после истечения указанного срока действия программы прекращает работать, если за неё не была произведена оплата) или версия программы с ограниченными функциональными возможностями (в случае оплаты пользователю сообщается код, включающий все функции программы).

Свободно распространяемые программы. Многие производители программного обеспечения и компьютерного оборудования заинтересованы в широком бесплатном распространении программного обеспечения. К таким программным средствам можно отнести:

- Новые недоработанные (бета) версии программных продуктов (это позволяет провести их широкое тестирование).

- Программные продукты, являющиеся частью принципиально новых технологий (это позволяет завоевать рынок).
- Дополнения к ранее выпущенным программам, исправляющие найденные ошибки или расширяющие возможности.
- Драйверы к новым или улучшенные драйверы к уже существующим устройствам.

Но какое бы программное обеспечение вы не выбрали, существуют общие требования ко всем группам программного обеспечения:

- Лицензионная чистота (применение программного обеспечения допустимо только в рамках лицензионного соглашения).
- Возможность консультации и других форм сопровождения.
- Соответствие характеристикам, комплектации, классу и типу компьютеров, а также архитектуре применяемой вычислительной техники.
- Надежность и работоспособность в любом из предусмотренных режимов работы, как минимум, в русскоязычной среде.
- Наличие интерфейса, поддерживающего работу с использованием русского языка. Для системного и инструментального программного обеспечения допустимо наличие интерфейса на английском языке.
- Наличие документации, необходимой для практического применения и освоения программного обеспечения, на русском языке.
- Возможность использования шрифтов, поддерживающих работу с кириллицей.
- Наличие спецификации, оговаривающей все требования к аппаратным и программным средствам, необходимым для функционирования данного программного обеспечения.

Преимущества лицензионного и недостатки нелицензионного программного обеспечения

Лицензионное программное обеспечение имеет ряд преимуществ:

- Техническая поддержка производителя программного обеспечения. При эксплуатации приобретенного лицензионного программного обеспечения у пользователей могут возникнуть различные вопросы. Владельцы лицензионных программ имеют право воспользоваться технической поддержкой производителя программного обеспечения, что в большинстве случаев позволяет разрешить возникшие проблемы.

- Обновление программ. Производители программного обеспечения регулярно выпускают пакеты обновлений лицензионных программ (patch, service-pack). Их своевременная установка - одно из основных средств защиты персонального компьютера (особенно это касается антивирусных программ). Легальные пользователи оперативно и бесплатно получают все вышедшие обновления.
- Законность и престиж. Покупая нелицензионное программное обеспечение, вы нарушаете закон, так как приобретаете "ворованные" программы. Вы подвергаете себя и свой бизнес риску юридических санкций со стороны правообладателей. У организаций, использующих нелегальное программное обеспечение, возникают проблемы при проверках лицензионной чистоты программного обеспечения, которые периодически проводят правоохранительные органы. За нарушение авторских прав в ряде случаев предусмотрена не только административная, но и уголовная ответственность. Нарушение законодательства, защищающего авторское право, может негативно отразиться на репутации компании. Нелицензионные копии программного обеспечения могут стать причиной несовместимости программ, которые в обычных условиях хорошо взаимодействуют друг с другом.
- В ногу с техническим прогрессом. Управление программным обеспечением поможет определить потребности компании в программном обеспечении, избежать использования устаревших программ и будет способствовать правильному выбору технологии, которая позволит компании достичь поставленных целей и преуспеть в конкурентной борьбе.
- Профессиональные предпродажные консультации. Преимущества приобретения лицензионного программного обеспечения пользователи ощущают уже при его покупке. Продажу лицензионных продуктов осуществляют сотрудники компаний - авторизованных партнеров ведущих мировых производителей программного обеспечения, квалифицированные специалисты. Покупатель может рассчитывать на профессиональную консультацию по выбору оптимального решения для стоящих перед ним задач.
- Повышение функциональности. Если у вас возникнут пожелания к функциональности продукта, вы имеете

возможность передать их разработчикам; ваши пожелания будут учтены при выпуске новых версий продукта.

Приобретая нелицензионное программное обеспечение вы очень рискуете.

Административная ответственность за нарушение авторских прав. Согласно статьи 7.12 КоАП РФ 1, ввоз, продажа, сдача в прокат или иное незаконное использование экземпляров произведений или фонограмм в целях извлечения дохода в случаях, если экземпляры произведений или фонограмм являются контрафактными: влечет наложение административного штрафа: на юридических лиц - от 300 до 400 МРОТ с конфискацией контрафактных экземпляров, произведений и фонограмм, а также материалов и оборудования, используемых для их воспроизведения, и иных орудий совершения административного правонарушения.

Уголовная ответственность за нарушение авторских прав. Согласно статьи 146 УК РФ (часть 2), незаконное использование объектов авторского права или смежных прав, а равно приобретение, хранение, перевозка контрафактных экземпляров произведений или фонограмм в целях сбыта, совершенные в крупном размере, наказываются штрафом в размере от 200 до 400 МРОТ или в размере заработной платы или иного дохода осужденного за период от двух до четырех месяцев, либо обязательными работами на срок от 180 до 240 часов, либо лишением свободы на срок до двух лет.

При использовании нелицензионного, то есть измененной пиратами версии, программного продукта, могут возникнуть ряд проблем:

- Некорректная работа программы. Взломанная программа– это изменённая программа, после изменений не прошедшая цикл тестирования.
- Нестабильная работа компьютера в целом.
- Проблемы с подключением периферии (неполный набор драйверов устройств).
- Отсутствие файла справки, документации, руководства.
- Невозможность установки обновлений.
- Отсутствие технической поддержки продукта со стороны разработчика.
- Опасность заражения компьютерными вирусами (от частичной потери данных до полной утраты содержимого жёсткого диска) или другими вредоносными программами.

Организация обновления программного обеспечения через Интернет.

Любая операционная система, как и программные продукты, через какое-то время после установки должна обновляться. Обновления выпускаются для:

- устранения в системе безопасности;
- обеспечения совместимости со вновь появившимися на рынке комплектующими компьютеров;
- оптимизации программного кода;
- повышения производительности всей системы.

Если служба «Центр обновления Windows» включена, и некоторые программные компоненты системы, которые связанны с работой службы обновления, нуждаются в обновлении для ее функционирования, то эти обновления должны устанавливаться перед проверкой, загрузкой и установкой любых других обновлений. Эти обязательные обновления исправляют ошибки, а также обеспечивают усовершенствования и поддерживают совместимость с серверами корпорации Майкрософт, поддерживающими работу службы. Если служба обновления отключена, то получать обновления для операционной системы будет невозможно.

Обновления представляют собой дополнения к программному обеспечению, предназначенные для предотвращения или устранения проблем и улучшения работы компьютера. Обновления безопасности для Windows способствуют защите от новых и существующих угроз для конфиденциальности и устойчивой работы компьютера. Оптимальный способ получения обновлений безопасности - включить автоматическое обновление Windows и всегда оставаться в курсе последних проблем, связанных с безопасностью и предоставить операционной системе самостоятельно заботиться о своей безопасности. В этой статье речь пойдет именно о Центре обновления Windows.

Желательно обновлять компьютер как можно чаще. В этом случае использования автоматического обновления, операционная система Windows устанавливает новые обновления, как только они становятся доступными. Если не устанавливать обновления, то компьютер может подвергнуться риску в плане безопасности или же могут возникнуть нежелательные неполадки в работе Windows или программ.

Каждый день появляется все больше и больше новых вредоносных программ, использующих уязвимости Windows и другого программного обеспечения для нанесения ущерба и получения доступа

к компьютеру и данным. Обновления Windows и другого программного обеспечения позволяют устранить уязвимости вскоре после их обнаружения. Если отложить установку обновлений, компьютер может стать уязвимым для таких угроз.

Обновления и программное обеспечение от Microsoft для продуктов Microsoft являются бесплатным предложением от службы поддержки, так что можно не волноваться за то, что с вас будет взиматься дополнительная плата за обеспечение надежности вашей системы. Чтобы узнать, являются ли обновления других программ бесплатными, обращайтесь к соответствующему издателю или изготовителю. При загрузке и установке обновлений различных программ в зависимости от типа подключения к Интернету может взиматься стандартная плата за местные или междугородные телефонные переговоры, а также плата за пользование Интернетом. В связи с тем, что обновления применяются к Windows и установленным на компьютере программам независимо от того, кто ими пользуется, после установки обновлений они будут доступны для всех пользователей компьютера.

Все обновления подразделяются на

- Важные обновления обеспечивают существенные преимущества в безопасности, конфиденциальности и надежности. Их следует устанавливать сразу же, как только они становятся доступны, и можно выполнять установку автоматически с помощью «Центра обновления Windows».
- Рекомендуемые обновления могут устранять менее существенные проблемы или делать использование компьютера более удобным. Хотя эти обновления не предназначены для устранения существенных недостатков в работе компьютера или программного обеспечения Windows, их установка может привести к заметным улучшениям. Их можно устанавливать автоматически.
- К необязательным обновлениям относятся обновления, драйверы или новое программное обеспечение Майкрософт, делающее использование компьютера более удобным. Их можно устанавливать только вручную.
- К остальным обновлениям можно отнести все обновления, которые не входят в состав важных, рекомендуемых или необязательных обновлений.

В зависимости от типа обновления в «Центре обновления Windows» предлагаются следующие возможности:

- Обновления безопасности. Это открыто распространяемые исправления уязвимостей определенных продуктов. Уязвимости различаются по уровню серьезности и указаны в бюллетене по безопасности Майкрософт как критические, важные, средние или низкие.
- Критические обновления. Это открыто распространяемые исправления определенных проблем, которые связаны с критическими ошибками, не относящимися к безопасности.
- Пакеты обновления. Протестированные наборы программных средств, включающие в себя исправления, обновления безопасности, критические и обычные обновления, а также дополнительные исправления проблем, обнаруженных при внутреннем тестировании после выпуска продукта. Пакеты обновления могут содержать небольшое количество изменений оформления или функций, запрошенных пользователями.

Для обновления программного обеспечения через Интернет рекомендуется включить автоматическое обновление

Для автоматического обновления программ необходимо войти в систему с учетной записью «Администратор».

1. Нажмите кнопку Пуск, выберите команду Панель управления и два раза щелкните значок Автоматическое обновление.
2. Выберите вариант Автоматически (рекомендуется).
3. Под вариантом Автоматически загружать и устанавливать на компьютер рекомендуемые обновления выберите день и время, когда операционная система Windows должна устанавливать обновления.

Автоматическое обновление обеспечивает установку первоочередных обновлений, которые включают в себя обновления безопасности и другие важные обновления, помогающие защитить компьютер. Также рекомендуется регулярно посещать веб-узел Windows Update (http://www.microsoft.com/) для получения необязательных обновлений, например рекомендованных обновлений программного обеспечения и оборудования, которые помогут улучшить производительность компьютера.

4. Задание

Задание 1. Найти в Интернет закон РФ «Об информации, информатизации и защите информации» и выделить определения понятий:

- информация;
- информационные технологии;
- информационно-телекоммуникационная сеть;
- доступ к информации;
- конфиденциальность информации;
- электронное сообщение;
- документированная информация.

Задание 2. Изучив источник «Пользовательское соглашение» Яндекс ответьте на следующие вопросы:

1. По какому адресу находится страница с пользовательским соглашением Яндекс?
2. В каких случаях Яндекс имеет право отказать пользователю в использовании своих служб?
3. Каким образом Яндекс следит за операциями пользователей?
4. Что подразумевается под термином «контент» в ПС?
5. Что в ПС сказано о запрете публикации материалов, связанных с:
   a. нарушением авторских прав и дискриминацией людей;
   b. рассылкой спама;
   c. обращением с животными?
6. Какого максимального объема могут быть файлы и архивы, размещаемые пользователями при использовании службы бесплатного хостинга?
7. Ваш почтовый ящик на Почте Яндекса будет удален, если Вы не пользовались им более ___.

Задание 3. Изучив организацию обновления программного обеспечения через Интернет. Настройте автоматическое обновление программного обеспечения еженедельно в 12.00. Опишите порядок установки автоматического обновления программного обеспечения.

5. Содержание отчета.

Отчет должен содержать:

1. Название работы.
2. Цель работы.
3. Задание и его решение.

4. Вывод по работе.

6. Контрольные вопросы:

1. Какие программы называют лицензионными?
2. Какие программы называют условно бесплатными?
3. Какие программы называют свободно распространяемыми?
4. В чем состоит различие между лицензионными, условно бесплатными и бесплатными программами?
5. Как можно зафиксировать свое авторское право на программный продукт?
6. Какие используются способы идентификации личности при предоставлении доступа к информации?
7. Почему компьютерное пиратство наносит ущерб обществу?
8. Какие существуют программные и аппаратные способы защиты информации?
9. Чем отличается простое копирование файлов от инсталляции программ?
10. Назовите стадии инсталляции программы.
11. Что такое инсталлятор?
12. Как запустить установленную программу?
13. Как удалить ненужную программу с компьютера?

Практическое задание №16,17

1. Изменение параметров настройки протокола IP. 1.1 Подключиться к виртуальной машине Windows XP.Перейти в окно конфигурирования сетевых подключений: открыть окно "Сетевые подключения": Пуск/Настройка/Сетевые подключения. Кликнуть правой клавишей мыши по значку "подключение по локальной сети" и выбрать пункт "Свойства". 1.2 В появившемся окне выберите сетевой адаптер, затем "Свойства", затем Протокол Интернета (TCP/IP) и его свойства. * Если доступ к настройке параметров сети запрещен административными настройками ОС, то перейдите к выполнению дополнительного задания, описанного в п.6. 1.3 Запишите значения сетевых параметров, установленных на Вашей машине: − IP– адреса; − Сетевой маски; − Адреса шлюза по умолчанию; − Адреса 1– го и 2– го серверов DNS (если они установлены). Занесите значения этих параметров в отчет. 1.4 Удалите протокол NetBUI, если он установлен на Вашей машине. 1.5 Установите сетевые параметры протокола IP в соответствии с таблицей 2. Таблица 2. Сетевые параметры протокола IP IP– адрес** Сетевая маска Шлюз 192.168.20Y.G+XX 255.255.0.0 Использовать значение,

которое было установлено ранее, либо значение, указанное преподавателем. Где Y, G, XX – десятичные числа; Y – год поступления (одна цифра 0-9). G = номер группы. 00 – для группы УИР-1; 50 – для группы УИР-2; 100 – для группы УИР-3. XX = – порядковый номер студента в группе. Пример. Студент номер 21 (по журналу); группы УИР-2; год поступления 2003. XX=21; G=50; Y=3. Получим сетевой адрес машины: 192.168.203.71 Где 203 = 200+3 71 = 50+21. 1.6 Если в результате изменения параметров настройки протокола IP будет выдано сообщение о необходимости перезагрузки, ни в коем случае не делайте этого, просто откажитесь. 1.7 Открыть консоль системы (соответствующая процедура описана в приложении 2). В командной строке выполнить команду: > ipconfig /all Сохраните результат выполнения этой команды в отчете. 1.8 В командной строке консоли выполните команду: > ping Результаты занесите в файл отчета. 2. Оформление отчета по результатам выполнения практической работы. По результатам выполнения работы необходимо подготовить отчет требования, к которому изложены в Приложении 1. Контрольные вопросы: 1. Имеется сеть с IP = 192.168.55.0 и требуется разбить ее на ряд подсетей. Необходимо, чтобы в каждой подсети можно было использовать по 25 хостов. Какую маску необходимо применить в таком случае, чтобы обеспечить максимально возможное число таких подсетей? A 255.255.255.192; B. 255.255.255.224; C. 255.255.255.240; D 255.255.255.248. 2. У вас имеется маска 255.255.255.252. Какое значение имеет префикс? A. /16; B. /24; C. /30, D. /32 3. Если имеется IP– адрес 172.16.10.5/25, то какой широковещательный адрес должен использовать этот хост? A. 255.255.255.255; B. 172.16.10.127; C. 172.16.10.255; D. 172.16.10.128. 4. Сколько машин позволяет иметь в подсети маска 255.255.255.252? A. 16384; B. 2; C. 4094; D. 6. 5. Каков диапазон допустимых адресов машин для подсети 172.16.10.5/26? A. с 172.16,10.1 по 172.16.10.30; B. с l72.16.10.1 по l72.16.10.31; C. с 172.16.10.1 по 172.16.10.62; D. с 172.16.10.1 по 172.16.10.63. 6. Если вы хотите объединить в подсеть машины с адресами с 192.168.10.64 по 192.168.10.127, то какими будут адрес и маска подсети? A. 192.168.10.64 255.255.255.192; B. 192.168.10.0 255.255.255.192; C. 192.168.10.64 255.255.255.224; D. 192.168.10.0 255.255.255.224. 7. Назовите основное назначение и возможности технологии применения масок переменной длины (VLSM). 8. Назовите основное назначение и возможности технологии бесклассовой междоменной маршрутизации (CIDR). 9. Объясните основные функции, выполняемые шлюзом в коммуникационной схеме протокола IP. 10. Каким образом, машины, работающие в IP сети, определяют, когда пакет необходимо доставить шлюзу, а в каком случае доставка выполняется непосредственно с помощью протоколов канального уровня?

Практическое задание №18

Тема: Уровни управления сетями
Цель:

Ход работы.

Практическое задание №19,20

Защищенность и отказоустойчивость операционной системы

1. Цель работы: выработать практические навыки работы с операционной системой Windows, получить информацию о видах сбоев в работе операционной системы; получить информацию о причинах возникновения сбоев; получить информацию о методах предотвращения сбоев.

2. Оборудование, приборы, аппаратура, материалы: персональный компьютер с операционной системой семейства Windows.

3. Краткие теоретические сведения.

Защита ресурсов

Каждая операционная система должна обеспечивать некоторый уровень защищенности — как ресурсов, так и данных пользователей. Данные пользователей защищаются использованием механизма авторизации и разграничения прав доступа. Безопасность данных пользователей операционных систем регламентируется стандартом безопасности, рассмотренным ранее.

Защиту ресурсов одних процессов от захвата другими процессами организовать не так сложно, как защиту данных пользователей, поскольку, хотя процессы и обладают большей свободой действий, чем большинство пользователей, в то же время процесс не обладает волей и способен выполнять только те действия, на которые запрограммирован. Поэтому вопросы защиты ресурсов от захвата решаются в рамках задачи планирования ресурсов.

Защита данных

Операционные системы включают в себя механизм авторизации доступа. Традиционно пользователь должен иметь учетную запись в операционной системе той машины, на которой работает, чтобы иметь возможность использовать машину для решения своих задач. Если машины объединены в локальную сеть, то учетная запись может храниться не на самой машине, а на сервере сети. В случае когда профили пользователей хранятся на сервере, получить несанкционированный доступ к данным существенно сложнее, чем если бы профили хранились на конкретных машинах, поскольку серверы сети снабжены гораздо более криптостойким механизмом **защиты данных**, нежели рабочие станции. Проблема защиты данных пользователей от несанкционированного доступа также может решаться и самим пользователем. Существует ряд программных продуктов, позволяющих пользователям закрывать доступ к своим данным таким образом, что для чтения их на этой же машине необходимо знать пароль, а для взлома и получения доступа в обход системы защиты — принцип кодирования данных. Эти программные продукты используют такие алгоритмы кодирования данных, что попытка взлома защиты может растянуться на несколько лет.

Отказоустойчивость операционных систем

Отказоустойчивость — способность операционной системы восстанавливать свою работоспособность после сбоев как программного, так и аппаратного характера.

В идеале пользователь вообще не должен наблюдать никаких негативных последствий сбоев в работе операционной системы. Сбои программного характера могут возникать по различным причинам: например, вирусная атака, неосторожное обращение с системными файлами, конфликт драйверов устройств и многое другое. Аппаратные сбои могут возникать по причине несоблюдения условий эксплуатации оборудования, из-за некорректного монтажа плат на системную плату.

Для каждой категории причин возникновения программных сбоев существуют методы их предотвращения. Часть методов включается в руководства по операционным системам в виде обязательных рекомендаций. Например, в руководстве по любой операционной системе перечисляются файлы и папки, удаление которых приведет к серьезным нарушениям в работе операционной системы. Большая же часть методов реализуется в виде специализированных программных комплексов. Например, средства защиты от вирусных и сетевых атак, механизмы блокирования доступа к системным файлам, механизмы сохранения состояния системы.

К сожалению, не существует настолько же надежных методов предотвращения аппаратных сбоев, как в случае с программными сбоями. Если в случае вирусной атаки операционную систему можно восстановить с заранее сохраненного образа системы, то в случае замены какого-либо компонента может потребоваться переустановка операционной системы. А если выйдет из строя носитель данных, то можно потерять важную информацию. Зачастую невозможно даже предугадать возникновение аппаратного сбоя и его последствия, в то время как программные сбои сравнительно легко прогнозируются и предотвращаются. Для того чтобы не возникали аппаратные сбои, необходимо соблюдать условия эксплуатации аппаратных компонентов компьютера. К примеру, попытка разбора жесткого диска приведет к необратимым повреждениям и гарантированной утрате информации.

Любая операционная система содержит программы, предотвращающие большинство стандартных сбоев, в том числе и средства мониторинга состояния аппаратных компонентов, но для предотвращения сбоев, возникающих по причине намеренных действий пользователей, необходимо устанавливать дополнительное программное обеспечение. Например, для отражения сетевых атак необходимо наличие в системе сетевого экрана, а для защиты от вирусных воздействий — комплекс антивирусной защиты.

Основные выводы

1. Операционная система должна обладать механизмами защиты ресурсов и данных пользователей.
2. Операционная система должна обладать механизмами предотвращения программных и, по возможности, аппаратных сбоев.
3. Для того чтобы избежать потери данных и порчи оборудования, необходимо использовать специализированное программное обеспечение и соблюдать условия эксплуатации оборудования.
4. Защита данных может осуществляться как средствами самой операционной системы, так и с помощью специализированного программного обеспечения.

4. Задание

Задание 1. Ответьте на вопросы.

1. При соблюдении каких условий можно считать операционную систему защищенной?
2. При соблюдении каких условий операционная система признается отказоустойчивой?

3. Каким образом пользователь может обеспечить защиту собственных данных от несанкционированного доступа?
4. Какие виды сбоев вы знаете?
5. Какие виды программных сбоев вы знаете?
6. Каковы могут быть последствия программного сбоя?
7. Каковы могут быть последствия аппаратного сбоя?
8. Можно ли утверждать, что для предотвращения возникновения аппаратного сбоя необходимо затратить больше усилий, чем в случае с программными сбоями? Обоснуйте свой ответ.
9. Можно ли утверждать, что несоблюдение условий эксплуатации оборудования может привести к серьезным нарушениям в работе компьютера?
10. Какого рода программные сбои операционная система может предотвратить собственными силами, а какие требуют установки дополнительного программного обеспечения?

Задание 2. Пройдите тест
http://www.e-biblio.ru/xbook/new/xbook330/book/part-023/page.htm#i03611

5. Содержание отчета

Отчет должен содержать:

1. Название работы.
2. Цель работы.
3. Задание и его решение.
4. Вывод по работе.

6. Контрольные вопросы

1. Каким образом можно защитить данные от несанкционированного доступа?
2. Какие причины возникновения программных сбоев вы знаете?
3. Какими методами можно предотвратить программные сбои и их последствия?
4. Почему аппаратные сбои опаснее, чем программные?
5. Какие программы могут входить в поставку операционной системы для обеспечения ее отказоустойчивости?

Практическое задание №21

Оборудование, приборы, аппаратура, материалы: персональный компьютер, видеоматериал, рабочая тетрадь.

3. Краткие теоретические сведения

Самое лучшее средство – это большая диаграмма, приколотая к стене.

Унифицированный язык моделирования UML (Unified Modeling Language) – это преемник того поколения методов объектно-ориентированного анализа и проектирования, которые появились в конце 80-х и начале 90-х годов. Создание UML фактически началось в конце 1994 г., когда Гради Буч и Джеймс Рамбо начали работу по объединению их методов Booch [Буч-1999] и OMT (Object Modeling Technique) под эгидой компании Rational Software. К концу 1995 г. они создали первую спецификацию объединенного метода, названного ими Unified Method, версия 0.8. Тогда же в 1995 г. к ним присоединился создатель метода OOSE (Object-

Oriented Software Engineering) Ивар Якобсон. Таким образом, UML является прямым объединением и унификацией методов Буча, Рамбо и Якобсона, однако дополняет их новыми возможностями.

UML находится в процессе стандартизации, проводимом консорциумом OMG (Object Management Group), в настоящее время он принят в качестве стандартного языка моделирования и получил широкую поддержку. UML принят на вооружение практически всеми крупнейшими компаниями – производителями программного обеспечения (Microsoft, IBM, Hewlett-Packard, Oracle, Sybase и др.). Кроме того, практически все мировые производители CASE-средств, помимо Rational Software (Rational Rose), поддерживают UML в своих продуктах (Paradigm Plus (CA), System Architect (Popkin Software), Microsoft Visual Modeler и др.). Полное описание UML можно найти на сайтах http://www.omg.org и http://www.rational.com. Первое описание UML на русском языке содержится в книге [Фаулер-1999], в дальнейшем изложении терминология языка соответствует данному переводу. Кроме него, имеются также переводы [Боггс-2000], [Буч-2000] и [Ларман-2001].

Средства UML

Создатели UML представляют его как язык для определения, представления, проектирования и документирования программных систем, организационно-экономических систем, технических систем и других систем различной природы. UML содержит стандартный набор диаграмм и нотаций самых разнообразных видов. Стандарт UML версии 1.1, принятый OMG в 1997 г., предлагает следующий набор диаграмм для моделирования:

– диаграммы вариантов использования (use case diagrams) –для моделирования бизнес-процессов организации и требований к создаваемой системе);

– диаграммы классов (class diagrams) – для моделирования статической структуры классов системы и связей между ними;

– диаграммы поведения системы (behavior diagrams):

- диаграммы взаимодействия (interaction diagrams):

  диаграммы последовательности (sequence diagrams) и кооперативные диаграммы (collaboration diagrams) – для моделирования процесса обмена сообщениями между объектами;

  диаграммы состояний (statechart diagrams) –для моделирования поведения объектов системы при переходе из одного состояния в другое;

  диаграммы деятельностей (activity diagrams) – для моделирования поведения системы в рамках различных вариантов использования, или моделирования деятельностей;

– диаграммы реализации (implementation diagrams):

- диаграммы компонентов (component diagrams) – для моделирования иерархии компонентов (подсистем) системы;
- диаграммы размещения (deployment diagrams) – для моделирования физической архитектуры системы.

Диаграммы вариантов использования

Понятие варианта использования (use case) впервые ввел Ивар Якобсон и придал ему такую значимость, что в настоящее время вариант использования превратился в основной элемент разработки и планирования проекта.

Вариант использования представляет собой последовательность действий (транзакций), выполняемых системой в ответ на событие, инициируемое некоторым внешним объектом (действующим лицом).

Вариант использования описывает типичное взаимодействие между пользователем и системой. В простейшем случае вариант использования определяется в процессе обсуждения с пользователем тех функций, которые он хотел бы реализовать.

Действующее лицо (actor) – это роль, которую пользователь играет по отношению к системе. Действующие лица представляют собой роли, а не конкретных людей или наименования работ. Несмотря на то, что на диаграммах вариантов использования они изображаются в виде стилизованных человеческих фигурок, действующее лицо может также быть внешней системой, которой необходима некоторая информация от данной системы. Показывать на диаграмме действующих лиц следует только в том случае, когда им действительно необходимы некоторые варианты использования.

Действующие лица делятся на три основных типа – пользователи системы, другие системы, взаимодействующие с данной, и время. Время становится действующим лицом, если от него зависит запуск каких-либо событий в системе.

Для наглядного представления вариантов использования в качестве основных элементов процесса разработки программного обеспечения (ПО) применяются диаграммы вариантов использования. На рис. 1.1 показан пример такой диаграммы для банкомата (Automated Teller Machine, ATM).

На данной диаграмме человеческие фигурки обозначают действующих лиц, овалы – варианты использования, а линии и стрелки –различные связи между действующими лицами и вариантами использования.

На этой диаграмме показаны два действующих лица: клиент и кредитная система. Существует также шесть основных действий, выполняемых моделируемой системой: перевести деньги, сделать вклад, снять деньги со счета, показать баланс, изменить идентификационный код и осуществить оплату.

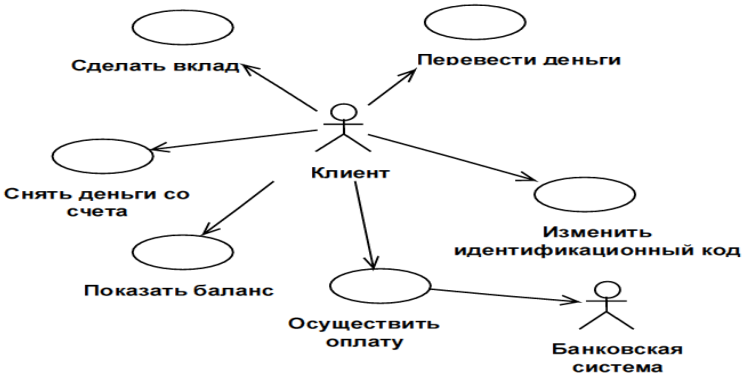


Рис. 1.1. Пример диаграммы вариантов использования

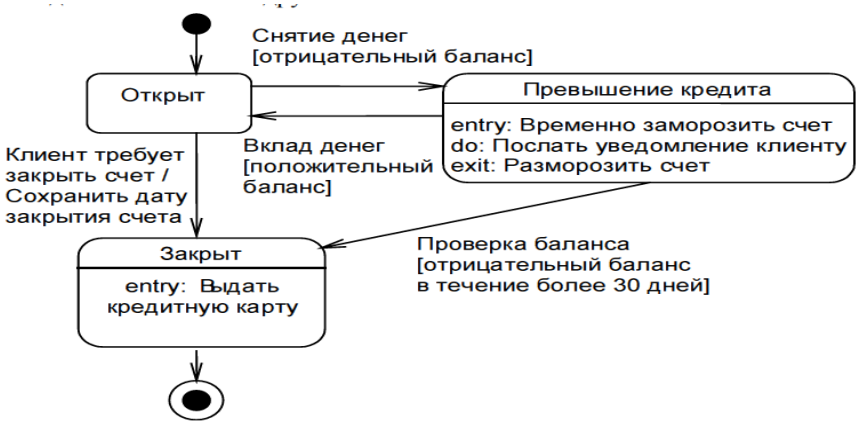
Диаграммы состояний

Диаграммы состояний определяют все возможные состояния, в которых может находиться конкретный объект, а также процесс смены состояний объекта в результате наступления некоторых событий.

Существует много форм диаграмм состояний, незначительно отличающихся друг от друга семантикой. Наиболее распространенная форма, используемая в объектно-ориентированных методах, впервые применялась в методе OMT и впоследствии была адаптирована Гради Бучем.

На рис. 1.16 приводится пример диаграммы состояний для банковского счета. Из данной диаграммы видно, в каких состояниях может существовать счет. Можно также видеть процесс перехода счета из одного состояния в другое. Например, если клиент требует закрыть открытый счет, он переходит в состояние «Закрыт». Требование клиента называется событием (event), именно такие события и вызывают переход из одного состояния в другое.

Рис. 1.16. Диаграмма состояний для класса Account



Если клиент снимает деньги с открытого счета, он может перейти в состояние «Превышение кредита». Это происходит, только если баланс по этому счету меньше ноля, что отражено условием [отрицательный баланс] на нашей диаграмме. Заключенное в квадратных скобках условие (guard condition) определяет, когда может или не может произойти переход из одного состояния в другое.

На диаграмме имеются два специальных состояния – начальное (start) и конечное (stop). Начальное состояние выделено черной точкой, оно соответствует состоянию объекта, когда он только что был создан.

Конечное состояние обозначается черной точкой в белом кружке, оно соответствует состоянию объекта непосредственно перед его уничтожением. На диаграмме состояний может быть одно и только одно начальное состояние. В то же время, может быть столько конечных состояний, сколько вам нужно, или их может не быть вообще. Когда объект находится в каком-то конкретном состоянии, могут выполняться различные процессы. В нашем примере при превышении кредита клиенту посылается соответствующее сообщение. Процессы, происходящие, когда объект находится в определенном состоянии, называются действиями (actions).

С состоянием можно связывать данные пяти типов: деятельность, входное действие, выходное действие, событие и история состояния.

Рассмотрим каждый из них в контексте диаграммы состояний для класса Account системы ATM.

Деятельность

Деятельностью (activity) называется поведение, реализуемое объектом, пока он находится в данном состоянии. Например, когда счет находится в состоянии «Закрыт», происходит возврат кредитной карточки пользователю. Деятельность – это прерываемое поведение. Оно может выполняться до своего завершения, пока объект находится в данном состоянии, или может быть прервано переходом объекта в другое состояние. Деятельность изображают внутри самого состояния, ей должно предшествовать слово do (делать) и двоеточие.

Входное действие

Входным действием (entry action) называется поведение, которое выполняется, когда объект переходит в данное состояние. В примере счета в банке, когда он переходит в состояние «Превышен счет», выполняется действие «Временно заморозить счет», независимо от того, откуда объект перешел в это состояние. Таким образом, данное действие осуществляется не после того, как объект перешел в это состояние, а, скорее, как часть этого перехода. В отличие от деятельности, входное действие рассматривается как непрерываемое. Входное действие также показывают внутри состояния, ему предшествует слово entry (вход) и двоеточие.

Выходное действие

Выходное действие (exit action) подобно входному. Однако, оно осуществляется как составная часть процесса выхода из данного состояния. В нашем примере при выходе объекта Account из состояния «Превышен счет», независимо от того, куда

он переходит, выполняется действие «Разморозить счет». Оно является частью процесса такого перехода. Как и входное, выходное действие является непрерываемым. Выходное действие изображают внутри состояния, ему предшествует слово exit (выход) и двоеточие. Поведение объекта во время деятельности, при входных и выходных действиях может включать отправку события другому объекту. Например, объект account (счет) может посылать событие объекту card reader (устройство чтения карты). В этом случае описанию деятельности, входного действия или выходного действия предшествует знак « ^ ». Соответствующая строка на диаграмме выглядит как Do: ^Цель.Событие(Аргументы) Здесь Цель – это объект, получающий событие, Событие – это посылаемое сообщение, а Аргументы являются параметрами посылаемого сообщения. Деятельность может также выполняться в результате получения объектом некоторого события. Например, объект account может быть в состоянии Открыто. При получении некоторого события выполняется определенная деятельность. Переходом (Transition) называется перемещение из одного состояния в другое. Совокупность переходов диаграммы показывает, как объект может перемещаться между своими состояниями. На диаграмме все переходы изображают в виде стрелки, начинающейся на первоначальном состоянии и заканчивающейся последующим. Переходы могут быть рефлексивными. Объект может перейти в то же состояние, в котором он в настоящий момент находится. Рефлексивные переходы изображают в виде стрелки, начинающейся и завершающейся на одном и том же состоянии. У перехода существует несколько спецификаций. Они включают события, аргументы, ограждающие условия, действия и посылаемые события. Рассмотрим каждое из них в контексте примера АТМ.

События

Событие (event) – это то, что вызывает переход из одного состояния в другое. В нашем примере событие «Клиент требует закрыть» вызывает переход счета из открытого в закрытое состояние. Событие размещают на диаграмме вдоль линии перехода. На диаграмме для отображения события можно использовать как имя операции, так и обычную фразу. В нашем примере события описаны обычными фразами. Если вы хотите использовать операции, то событие «Клиент требует закрыть» можно было бы назвать RequestClosure(). У событий могут быть аргументы. Так, событие «Сделать вклад», вызывающее переход счета из состояния «Превышен счет» в состояние «Открыт», может иметь аргумент Amount (Количество), описывающий сумму депозита. Большинство переходов должны иметь события, так как именно они, прежде всего, заставляют переход осуществиться. Тем не менее, бывают и автоматические переходы, не имеющие событий. При этом объект сам перемещается из одного состояния в другое со скоростью, позволяющей осуществиться входным действиям, деятельности и выходным действиям.

Ограждающие условия

Ограждающие условия (guard conditions) определяют, когда переход может, а когда не может осуществиться. В нашем примере событие «Сделать вклад» переведет счет из состояния «Превышение счета» в состояние «Открыт», но только если баланс будет больше нуля. В противном случае переход не осуществится. Ограждающие условия изображают на диаграмме вдоль линии перехода после имени события, заключая их в квадратные скобки. Ограждающие условия задавать необязательно. Однако если существует несколько автоматических переходов из состояния, необходимо определить для них взаимно исключающие ограждающие условия. Это поможет читателю диаграммы понять, какой путь перехода будет автоматически выбран.

Действие

Действием (action), как уже говорилось, является непрерываемое поведение, осуществляющееся как часть перехода. Входные и выходные действия показывают внутри состояний, поскольку они определяют, что происходит, когда объект входит или выходит из него. Большую часть действий, однако, изображают вдоль линии перехода, так как они не должны осуществляться при входе или выходе из состояния. Например, при переходе счета из открытого в закрытое состояние выполняется действие «Сохранить дату закрытия счета». Это непрерываемое поведение осуществляется только во время перехода из состояния «Открыт» в состояние «Закрыт». Действие рисуют вдоль линии перехода после имени события, ему предшествует косая черта. Событие или действие могут быть поведением внутри объекта, а могут представлять собой сообщение, посылаемое другому объекту. Если событие или действие посылается другому объекту, перед ним на диаграмме помещают знак « ^ ». Диаграммы состояний не надо создавать для каждого класса, они применяются только в сложных случаях. Если объект класса может существовать в нескольких состояниях и в каждом из них ведет себя по-разному, для него может потребоваться такая диаграмма.

4. Задания

Задание 1. Ответьте на вопросы, приведенные ниже.

1. Дайте понятие UML
2. Какие виды диаграмм моделирования данных вы знаете
3. Дайте понятие и характеристику диаграммы вариантов использования и классов.
4. Дайте понятие и характеристику диаграммы поведения системы
5. Дайте понятие и характеристику диаграммы реализации

Задание 2. Заполните таблицу, используя страницы из учебника по UML.

Дайте понятие диаграммы состояния	
Начальное и конечное состояние	
Типы, связываемы с состоянием (описать)	

Задание 3. Изобразите диаграммы

Изобразите диаграмму вариантов использования	Изобразите диаграмму состояния для класса Account

5. Содержание отчета

Отчет должен содержать:

1. Название работы.
2. Цель работы.
3. Задание и его решение.
4. Вывод по работе.

6. Контрольные вопросы

1. Унифицированный язык моделирования UML
2. Средства UML
3. Когда и кем был создан язык моделирования UML

Практическое задание №22,23

Цель работы: изучить работу диспетчера задач, изучить размещения файлов в файловой системе FAT, исследование методов организации файловых систем

2. Оборудование, приборы, аппаратура, материалы: персональный компьютер с операционной системой семейства Windows.

3. Краткие теоретические сведения.

WindowsAPI (Application Programming Interface) - это системный интерфейс программирования в семействе операционных систем Microsoft Windows. API состоит из большого количества динамических библиотек и содержит множество функций, которые прикладные программы могут использовать для взаимодействия с операционной системой. Каждая операционная система реализует различную подмножество Windows API.

API выполняет роль связующего звена между приложениями и операционной системой. Windows API содержит несколько тысяч функций, сгруппированы в следующие основные категории: базовые сервисы, сервисы компонентов, сервисы пользовательского интерфейса, сервисы графики и мультимедиа, сервисы коммуникаций, сетевые и Web-сервисы.

Функции, службы и процедуры

API содержит совокупность функций, которые доступны программистам при разработке программ - их называют функциями Windows API. К ним относятся документированные подпрограммы, такие, как CreateProcess, CreateFile, GetMessage и другие.

Функции ядра - это подпрограммы внутри операционной системы Windows, которые можно вызвать только в режиме ядра.

К службам относятся процессы, которые запускаются диспетчером управления служб. Они, как правило, работают в фоновом режиме независимо от других приложений и предназначенны для обслуживания определенных потребностей пользователя или системы. Например, служба Task Scheduler-планировщик, который позволяет управлять запуском других программ.

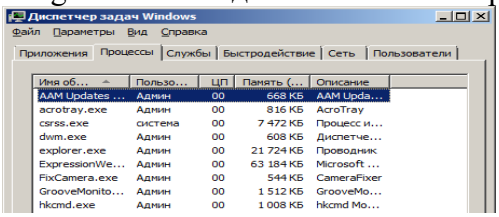
Windows содержит большой набор функций (подпрограмм), объединенных в отдельные бинарные файлы, которые программы могут динамически загружать во время своего выполнения. Такие библиотеки функций называют динамическими библиотеками (DLL).

Различные программные механизмы, которые операционная система предоставляет программистам для выполнения определенных действий, называют также сервисами, поскольку они предназначены для обслуживания различных потребностей пользователя системы. К таким сервисам относятся и функции API. Отдельное подмножество составляют неуправляемые системные сервисы (или исполнительные системные сервисы). Они охватывают недокументированные низкоуровневые сервисы операционной системы, которые можно вызвать в пользовательском режиме.

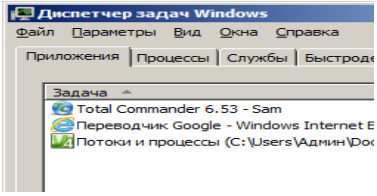
Процессы, потоки и задания

Когда в среде Windows запускается прикладная программа, система создает специальный объект - процесс, - который предназначен для поддержания ее исполнения. Может показаться, что программа и процесс - понятие похожие, они фундаментально отличаются. Программа - это статический набор команд, а процесс - контейнер для ресурсов, которые используются при выполнении экземпляра программы.

Известная утилита для анализа активности процессов-системный Task Manager (диспетчер задач). В ядре Windows нет такого понятия, как задачи, поэтому Task Manager на самом деле является инструментом для управления процессами.

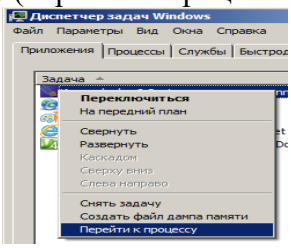


Диспетчер задач Windows отображает список активных процессов. Его можно запустить различными способами: 1) нажав комбинацию клавиш Ctrl + Shift + Esc, 2) щелкнув на панели задач правой кнопкой мыши и выбрав команду Task Manager (диспетчер задач), 3) нажав клавиши Ctrl + Alt + Del. Для просмотра списка процессов после запуска диспетчера задач следует открыть вкладку Processes (процессы). В этом окне процессы идентифицируются по имени образа, экземплярами которого они являются. В отличие от других объектов в Windows процессам нельзя присваивать глобальные имена. Для просмотра подробных сведений выберите из меню View (вид) команду Select Columns (выбрать столбцы) и выберите любую дополнительную информацию нужно отобразить.



Если вкладка Processes окна диспетчера задач показывает список процессов, то содержание вкладки Applications (приложения) отображает список видимых окон верхнего уровня всех объектов "рабочий стол" интерактивного объекта WindowStation. (По умолчанию существуют два объекта "рабочий стол", но можно создать дополнительные рабочие столы через Windows - функцию CreateDesktop). Столбик Status (состояние) дает представление о том, находится ли поток - владелец окна в состоянии ожидания сообщения. Состояние "Running" ("выполняется") означает, что поток ожидает ввода, а Not Responding ("не отвечает ") - не ожидает (т.е. занят, или ждет завершения операции ввода-вывода, или освобождение какого-то синхронизирующего объекта).

Вкладка Applications позволяет идентифицировать процесс, которому принадлежит поток, обладающий каким-то окном задачи. Для этого следует щелкнуть правой кнопкой мыши на названии задачи и выбрать команду Go To Process (перейти к процессам).

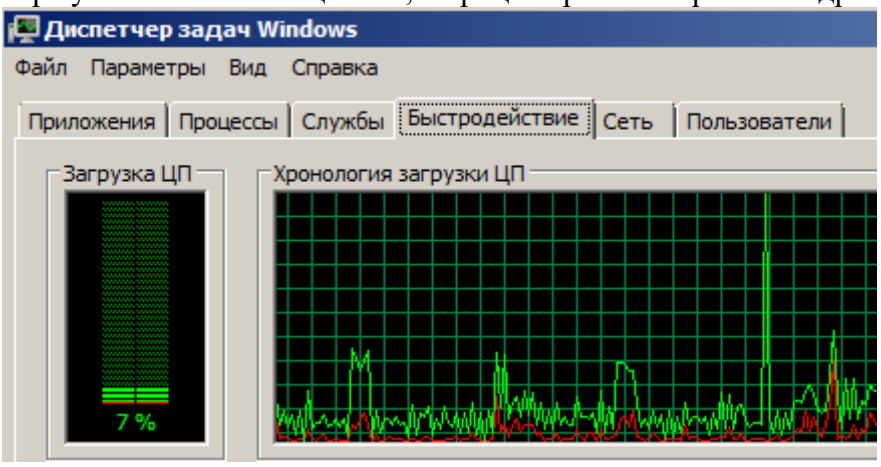


Для предотвращения доступа приложений к критически важным данным операционной системы и устранения риска их модификации Windows использует два режима доступа к процессору (даже если он поддерживает более двух режимов): пользовательский режим (user mode) и режим ядра (kernel mode). Код программ работает в пользовательском режиме, тогда как код операционной системы (например, системные сервисы и драйверы устройств) - в режиме ядра. В режиме ядра предоставляется доступ ко всей системной памяти и разрешается выполнять любые машинные команды процессора. Предоставляя операционной

системе высший уровень привилегий, чем прикладным программам, процессор позволяет разработчикам операционных систем реализовать архитектуру, которая не дает возможности отдельным программам нарушать стабильность работы всей системы.

Прикладные программы могут переключаться с пользовательского режима в режим ядра, обращаясь к системному сервису. Переключение с пользовательского режима в режим ядра осуществляется специальной командой процессора. Операционная система перехватывает эту команду, обнаруживает запрос системного сервиса, проверяет аргументы, которые поток передал системной функции, и выполняет внутреннюю подпрограмму. Перед возвращением управления пользовательскому потоку процессор переключается обратно в пользовательский режим. Благодаря этому операционная система защищает себя и свои данные от возможной модификации приложениями.

Поэтому ситуация, когда пользовательский поток часть времени работает в пользовательском режиме, а часть - в режиме ядра, обычная. Поскольку подсистема, отвечающая за поддержку графики и окон, функционирует в режиме ядра, то программы, интенсивно работающих с графикой, большую часть времени действуют в режиме ядра, а не в пользовательском режиме. Самый простой способ проверить это - запустить программу типа Adobe Photoshop или Microsoft Pinball и, выполняя в ней какие-то действия, наблюдать за показателями работы в пользовательском режиме и в режиме ядра с помощью Task Manager (диспетчер задач). В его окне на вкладке Performance (производительность), включив в меню View (вид) опцию Kernel Times (вывод времени ядра), можно увидеть, сколько времени процессор проводит в режиме ядра. На графике процент загрузка процессора указано зеленым цветом, а процент работы в режиме ядра - красным.



4. Задания

Задание 1. Заполните пропуски

WindowsAPI (Application Programming Interface) - _____
_____
_____
_____
_____
_____

API состоит из большого количества динамических библиотек и содержит множество функций, которые прикладные программы могут использовать для взаимодействия с операционной системой. Каждая операционная система реализует различную подмножество Windows API.

API выполняет роль связующего звена между приложениями и операционной системой. Windows API содержит несколько тысяч функций, сгруппированы в следующие основные категории: _____
_____
_____
_____
_____
_____
_____
_____
_____

API содержит совокупность функций, которые доступны программистам при разработке программ - их называют _____ К ним относятся _____
_____

Функции ядра - _____
_____
_____
_____
_____
_____

К службам относятся процессы, которые запускаются диспетчером управления служб. Они, как правило, работают в фоновом режиме независимо от других приложений и предназначенны для обслуживания определенных потребностей пользователя или системы. Например, служба Task Scheduler-планировщик, который позволяет управлять запуском других программ.

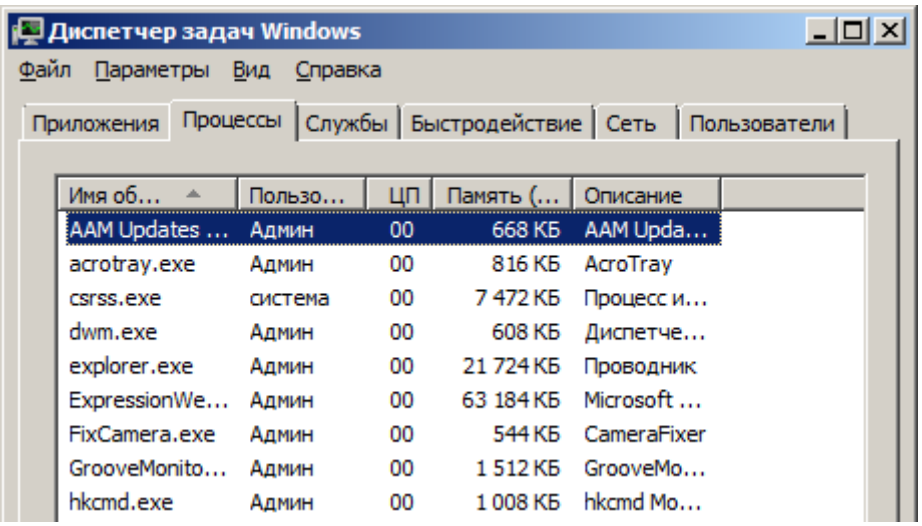
Windows содержит большой набор функций (подпрограмм), объединенных в отдельные бинарные файлы, которые программы могут динамически загружать во время своего выполнения. Такие библиотеки функций называют _____
_____
_____

Различные программные механизмы, которые операционная система предоставляет программистам для выполнения определенных действий, называют также сервисами, поскольку они предназначены для обслуживания различных потребностей пользователя системы. К таким сервисам относятся _____ Отдельное подмножество составляют неуправляемые системные сервисы (или исполнительные системные сервисы). Они охватывают недокументированные низкоуровневые сервисы операционной системы, которые можно вызвать в пользовательском режиме.

Когда в среде Windows запускается прикладная программа, система создает специальный объект - _____, - который _____
_____. Может показаться, что программа и процесс - понятие похожие, они фундаментально отличаются. Программа - _____, а процесс - _____
_____
_____
_____

Известная утилита для анализа активности процессов-системный Task Manager (_____). В ядре Windows нет

такого понятия, как задачи, поэтому Task Manager



Диспетчер задач Windows отображает список активных процессов. Его можно запустить различными способами:

В этом окне процессы идентифицируются по имени образа, экземплярами которого они являются. В отличие от других объектов в Windows процессам нельзя присваивать глобальные имена.

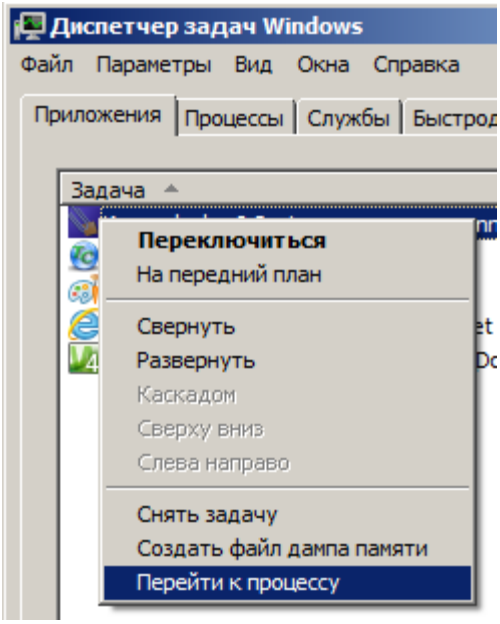
Если вкладка Processes окна диспетчера задач показывает список процессов, то содержание вкладки Applications (приложения) отображает список видимых окон верхнего уровня всех объектов "рабочий стол" интерактивного объекта WindowStation. Столбик Status (состояние)

. Состояние "Running" ("выполняется")

, а Not Responding ("не отвечает ") -

_____
_____.

Вкладка Applications позволяет
_____
_____
_____
_____
_____
_____
_____
_____
_____



Для предотвращения доступа приложений к критически важным данным операционной системы и устранения риска их модификации Windows использует два режима доступа к процессору (даже если он поддерживает более двух режимов): _____. Код программ работает в _____, тогда как код операционной системы (например, системные сервисы и драйверы устройств) - в _____. В режиме ядра предоставляется доступ ко всей системной памяти и разрешается выполнять любые машинные команды процессора.

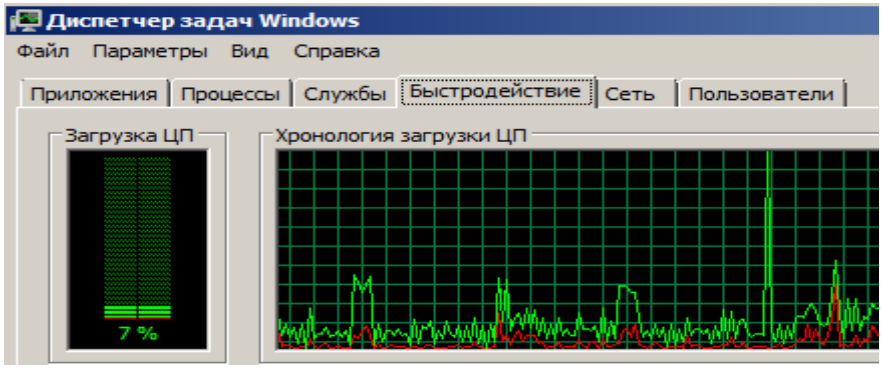
Прикладные программы
_____
_____
_____
_____. Переключение с пользовательского режима в режим ядра осуществляется _____
_____.

Операционная система
_____
_____
_____
_____
_____.

Перед возвращением управления пользовательскому потоку процессор переключается обратно в пользовательский режим. Благодаря этому операционная система

_____
_____
_____.

Поэтому ситуация, когда пользовательский поток часть времени работает в пользовательском режиме, а часть - в режиме ядра, обычная. Поскольку подсистема, отвечающая за поддержку графики и окон, функционирует в режиме ядра, то программы, интенсивно работающих с графикой, большую часть времени действуют в режиме ядра, а не в пользовательском режиме. Самый простой способ проверить это -
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____



Задание 2. Диспетчере задач.

Задание 2.1. Просмотр состояния процессов через диспетчер задач.

Просмотр и анализ взаимосвязей процессов и потоков.

Запустите диспетчер задач. Переключитесь на закладку Процессы. В меню Вид выберите пункт Выбрать столбцы… и укажите столбцы согласно рисунка 1. ***Сделайте скриншот вашей работы и сохраните его под именем «Рисунок 1. Выбор столбцов диспетчера задач»***

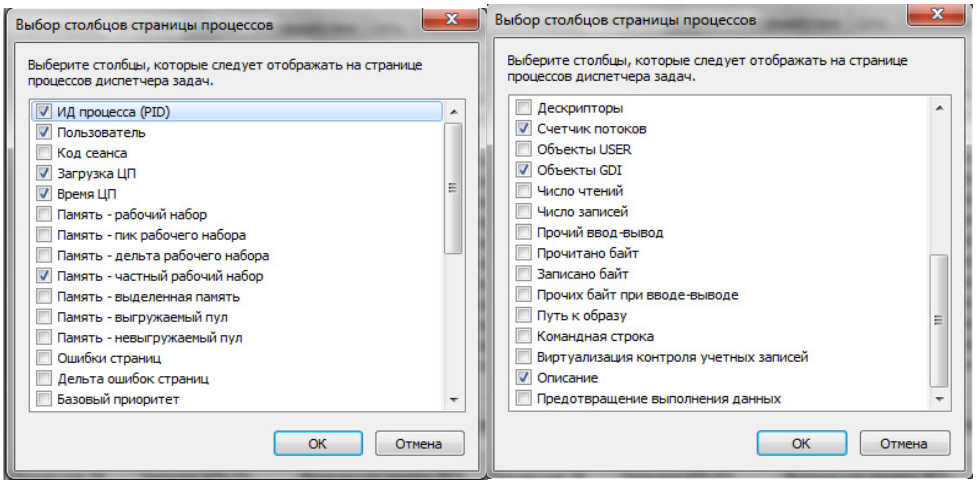


Рисунок 1. Выбор столбцов диспетчера задач

Потом определите сколько процессов запущено системой. Для этого я передите на закладку Быстродействие и в меню Вид выберите пункт Загрузка ЦП. (см. рис.2) Например: из рисунка мы видим что системой запущено 53 процесса, загрузка ЦП колеблется от 3-5%, файл подкачки загружен на 931 МБ. ***Сделайте скриншот вашей работы и сохраните его под именем «Рисунок 2. Диспетчер задач. Вкладка "Быстродействие"»***

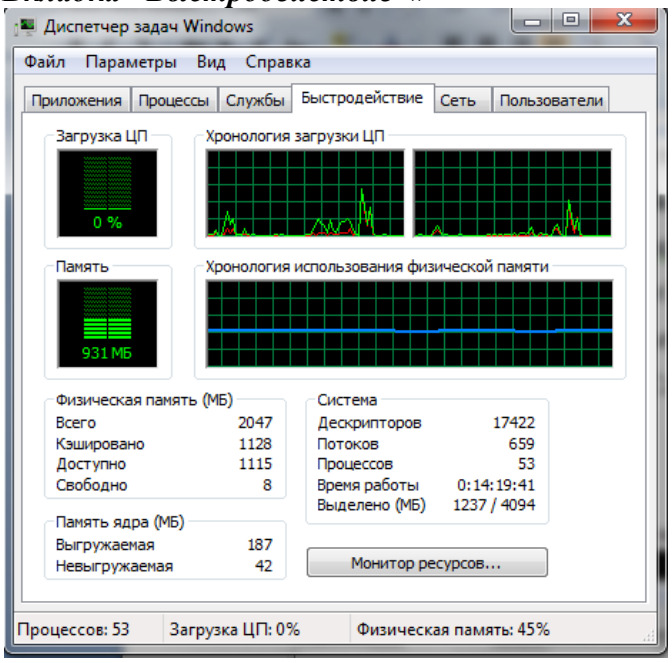


Рисунок 2. Диспетчер задач. Вкладка "Быстродействие"

Теперь запускаем приложение Paint и смотрим на изменения ЦП. Например в примере: загрузка ЦП колеблется в пределах 1-4%, файл подкачки загрузился на 942 МБ. Если сравнить объёмы используемого файла подкачки и доступной физической памяти, то можно сделать вывод что в сумме они дают общий объем физической памяти. (см. рис.3).

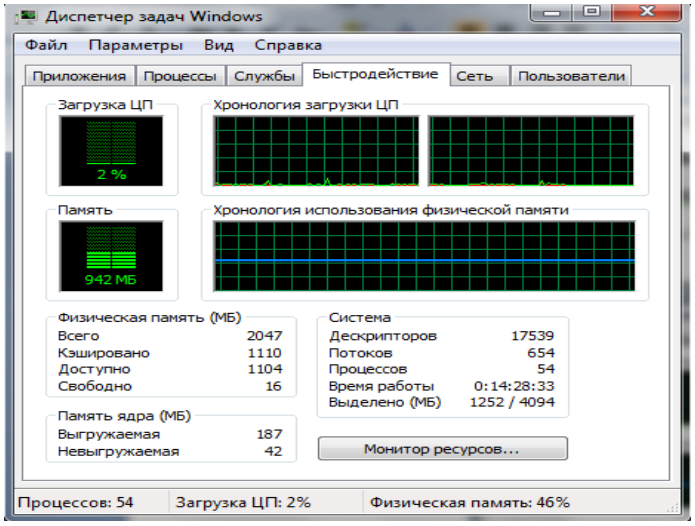


Рисунок 3. Результат после запуска приложения Paint

Сделайте скриншот вашей работы и сохраните его под именем «Рисунок 3. Результат после запуска приложения Paint». Напишите в каких пределах колеблется загрузка ЦП, как изменился файл подкачки.

Просмотр времени работы системы в пользовательском режиме и режиме ядра.

Переключитесь на закладку Быстродействие и в меню Вид выберите пункт Вывод времени ядра (см. Рисунок 4). Быстро прокручиваем страницы любого текстового документа. На индикаторе Загрузка ЦП процент работы процессора в пользовательском режиме отражается зеленым цветом, в режиме ядра красным. Из рисунка четко видны изменения работы процессора при прокрутке страниц.

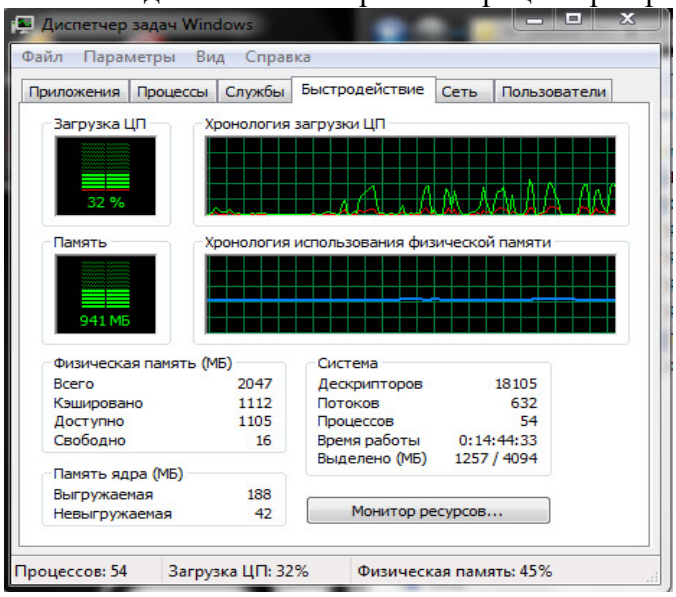


Рисунок 4. Состояние системы при прокрутке страниц

Сделайте скриншот вашей работы и сохраните его под именем «Рисунок 4. Состояние системы при прокрутке страниц»

Задание 2.2. Просмотр сведений о поддержке многопроцессорных систем.

Согласно следующему заданию откройте диспетчер устройств (Пуск – Панель управления – Диспетчер устройств). В списке устройств раскройте узел Компьютер. В окне свойств (Правой кнопкой свойства) перейдите на закладку Драйвер и с помощью кнопки Сведения просмотрите сведения о файлах драйверов (см. Рисунок 5).

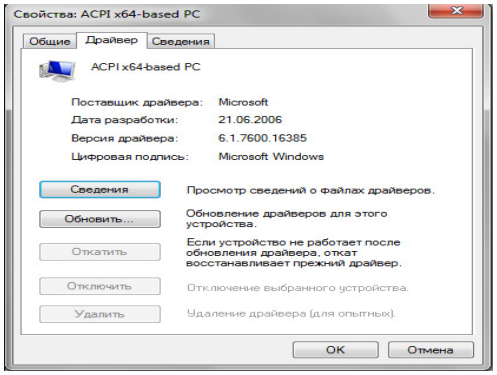


Рисунок 5. Сведения о файлах поддержки многопроцессорных систем

Сделайте скриншот вашей работы и сохраните его под именем «Рисунок 5. Сведения о файлах поддержки многопроцессорных систем»

Задание 2.3. Изучение отношения процессов родитель-потомок

1. Запустите командную строку (Пуск – Все программы – Стандартные – Командная строка)

2. Потом наберите start cmd для запуска второго окна командной строки.

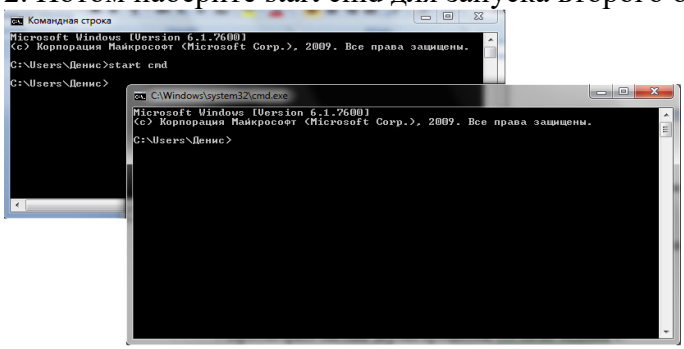


Рисунок 6. Запуск окон командной строки

Сделайте скриншот вашей работы и сохраните его под именем «Рисунок 6. Запуск окон командной строки»

3. Далее я откройте диспетчер задач.

4. Переключился на второе окно командной строки.

5. Ввел mspaint для запуска Microsoft Paint.

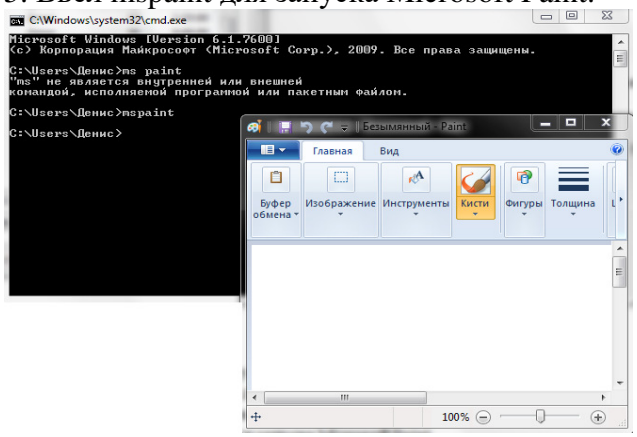


Рисунок 7. Запуск приложения Paint

Сделайте скриншот вашей работы и сохраните его под именем «Рисунок 7. Запуск приложения Paint»

6. Потом выберите второе окно командной строки.

7. Ввел команду exit, тем самым завершив работу второго окна.

Сделайте скриншот вашей работы и сохраните его под именем «Рисунок 8. Завершение работы второго окна»

8. Потом переключитесь в диспетчер задач. Откройте его вкладку Приложения. Щелкнул правой кнопкой мыши задачу Командная строка (cmd.exe) и выбрал Перейти к процессу.

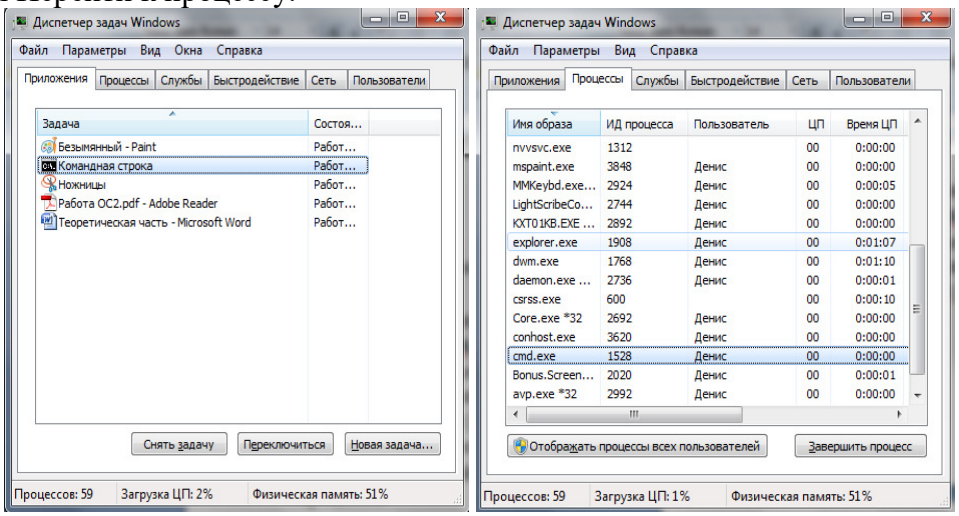


Рисунок 9. Диспетчер задач. Переход к процессу cmd.exe

Сделайте скриншот вашей работы и сохраните его под именем «Рисунок 9. Диспетчер задач. Переход к процессу cmd.exe»

11. Щелкните процесс Cmd.exe, выделенный цветом.

12. Щелкнув правой кнопкой мыши, выберите команду Завершить дерево процессов.

13. В окне Предупреждение диспетчера задач щелкните кнопку Завершить дерево процессов.

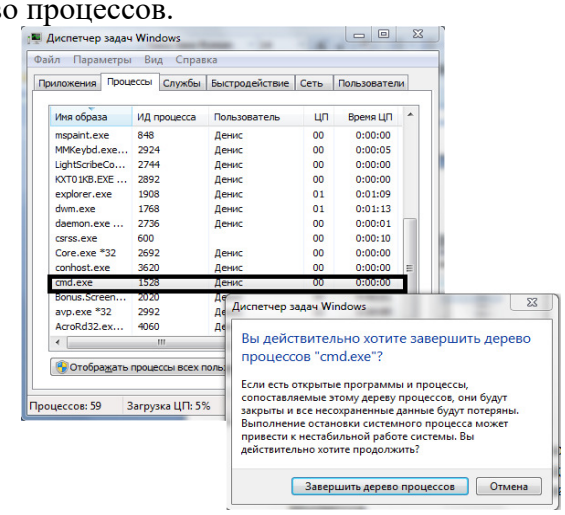


Рисунок 10. Диспетчер задач. Переход к процессу cmd.exe

Первое окно командной строки исчезнет, но окно Paint по прежнему работает.

Сделайте скриншот вашей работы и сохраните его под именем «Рисунок 10. Диспетчер задач. Переход к процессу cmd.exe»

Задание 2.4. Увеличение быстродействия Windows

1. Откройте Диспетчер Задач нажатием (Ctrl+Alt+Del)

Перейдите на вкладку Процессы, щелкните прав на строке Explorer.exe и в контекстном меню выберите команду Завершить Процесс. Опишите в отчете, что вы видите на экране и почему.

2. **Закройте окно Диспетчера Задач завершив процесс taskmgr.exe**. Внесите в отчет сведения: работает ли компьютер, загружена ли ОС, реагирует ли система на манипуляции мышью, на нажатие клавиш? Почему?

3. Нажмите (Ctrl+Alt+Del) и снова откройте Диспетчер Задач

4. Перейдя на вкладку Приложения, нажмите кнопку Новая задача

5. В окне Создать Новую Задачу наберите Explorer и нажмите OK.

5. Содержание отчета

Отчет должен содержать:

1. Название работы.
2. Цель работы.
3. Задание и его решение.
4. Вывод по работе.

6. Контрольные вопросы

1. Что такое WindowsAPI
2. Что такое процессы
3. Что такое потоки
4. Что такое задачи
5. Что такое диспетчер задач

Практическое задание №24

Тема: Основные сведения о сетевом мониторе

Цель: Использование сетевого монитора позволяет собирать сведения, обеспечивающие бесперебойную работу, начиная от определения шаблона до предотвращения и устранения неполадок. Сетевой монитор предоставляет сведения о трафике сетевого адаптера того компьютера, на котором он установлен. Сбор и анализ этих сведений позволяет предотвращать, диагностировать и устранять сетевые неполадки различных типов.

Можно настроить сетевой монитор для предоставления конкретных наиболее важных сведений. Например, можно так установить триггеры, что сетевой монитор будет начинать и завершать сбор сведений при соблюдении определенного условия или набора условий. Также можно установить фильтры для контроля за типом собираемых и отображаемых сетевым монитором сведений. Для облегчения анализа сведений можно изменить способ отображения данных на экране, а также сохранить или распечатать данные, чтобы просмотреть их позднее.

С помощью компонента Сетевой монитор, включенного в операционные системы Microsoft Windows Server 2003, можно собирать данные, отправленные или полученные с компьютера, на котором установлен сетевой монитор. Для сбора данных, посылаемых или

получаемых с удаленного компьютера, необходимо использовать компонент Сетевой монитор, входящий в Microsoft Systems Management Server (SMS), с помощью которого можно собирать данные, посылаемые или получаемые с любого компьютера, на котором установлен драйвер сетевого монитора. Дополнительные сведения о сервере Systems Management Server см. на веб-узле корпорации Майкрософт(http://www.microsoft.com/smsmgmt).

Сведения, предоставляемые сетевым монитором, получены из сетевого трафика и разделены на кадры. Эти кадры содержат такие сведения как адрес компьютера, пославшего кадр, адрес компьютера, которому кадр был послан, и протоколы, существующие в кадре.

Принцип работы сетевого монитора.

Данные, пересылаемые по сети, делятся на кадры. В каждом таком кадре содержатся следующие сведения:

- Адрес источника. Адрес сетевого адаптера, с которого поступил кадр.
- Адрес назначения. Адрес сетевого адаптера, которому предназначался кадр. Этот адрес может также определять группу сетевых адаптеров.
- Данные заголовка. Данные для каждого протокола, используемого при передаче кадра.
- Данные. Передаваемые данные (или часть данных).

Каждый компьютер сегмента сети получает кадры, отправленные данному сегменту. Сетевой адаптер каждого компьютера сохраняет и обрабатывает только адресованные данному адаптеру кадры. Остальные кадры отбрасываются и больше не обрабатываются. Сетевой адаптер также сохраняет широковещательные (и, потенциально, многоадресные) кадры.

После установки программы сетевого монитора можно записать в файл все кадры, отправленные сетевому адаптеру данного компьютера, или сохраненные им. Записанные кадры можно просмотреть или сохранить для дальнейшего анализа. Программа позволяет задать фильтр записи, разрешающий запись только определенных кадров. В этом случае

запись кадров будет производиться на таких условиях, как адрес источника, адрес назначения или протокол. Сетевой монитор также дает возможность пользователям разработать триггер записи для запуска определенных действий при обнаружении им в сети конкретного набора условий. Такими действиями могут быть запуск записи, конец записи или запуск программы.

По умолчанию размер буфера записи равен 1 МБ. Размер данных можно уменьшить, уменьшив размер буфера записи.

Запись данных.

Процесс копирования пакетов сетевым монитором называется записью. Можно записывать как весь сетевой трафик локального сетевого адаптера, так и отдельные наборы пакетов с помощью фильтров записи. Можно также задать набор условий для триггеров событий. После создания триггеров сетевой монитор может отвечать на события в сети. Например, операционная система может запустить исполняемый файл, если сетевой монитор обнаруживает в сети выполнение определенного набора условий. После записи данных их можно просмотреть. Сетевой монитор преобразует исходные данные в соответствии с логической структурой пакета.

При записи кадров сетевым монитором сведения о кадрах отображаются в окне записи данных, разделенном на четыре панели.

Панель	Значение
График	Графическое представление кадров, отправленных на локальный компьютер или с локального компьютера.
Статистика сеанса	Сведения о каждом отдельном сеансе.
Статистика станции	Сведения о кадрах, отправленных на локальный компьютер или с локального компьютера, на котором запущен сетевой монитор.
Общая статистика	Обобщенные сведения о кадрах, отправленных на локальный компьютер или с локального компьютера после начала процесса записи.

Сетевой монитор копирует передаваемые по сети пакеты с требуемыми характеристиками в буфер записи с помощью спецификации NDIS.

Фильтры записи.

Фильтр записи работает как запрос базы данных, который используется

для указания типов пакетов, передаваемых по сети, которые планируется записывать для последующего анализа. Например, для сбора данных, относящихся к определенному подмножеству компьютеров или протоколов, следует подготовить базу данных адресов, использовать эту базу для создания фильтра записи, а затем сохранить этот фильтр в файле. В дальнейшем при необходимости этот файл можно загружать для работы с фильтром. Использование фильтра позволяет сэкономить время и память буфера записи.

Создание фильтров записи

Чтобы создать фильтр записи, следует выбрать критерии фильтрации в диалоговом окне Фильтр записи. В этом диалоговом окне отображается дерево критериев, которое является графическим представлением логики фильтра. При каждом добавлении или исключении компонентов спецификации записи эти изменения отражаются в дереве критериев.

Фильтрация на основе протоколов

Для записи пакетов, передаваемых по сети с использованием конкретного протокола, необходимо указать этот протокол в строке SAP/ETYPE= дерева критериев. Например, для работы только с пакетами протокола IP сначала следует запретить все протоколы, а после этого разрешить IP ETYPE 0x800 и IP SAP 0x6. По умолчанию все поддерживаемые сетевым монитором протоколы разрешены. Протокол можно указать только с помощью ETYPE или SAP.

Фильтрация на основе адресов

Задайте одну или несколько пар адресов в фильтре записи для сбора данных, посылаемых или получаемых с конкретного компьютера сети. Допускается одновременное наблюдение за четырьмя адресными парами.

Адресная пара состоит из:

- адресов двух компьютеров, за трафиком между которыми ведется наблюдение;
- стрелок, указывающих интересующее направление передачи данных;
- ключевого слова INCLUDE или EXCLUDE, которое определяет, будет ли сетевой монитор захватывать или игнорировать соответствующие пакеты данных.

Независимо от того, в каком порядке располагаются адресные пары в диалоговом окне Фильтр записи, инструкции **EXCLUDE** обрабатываются первыми. Поэтому, если пакет удовлетворяет критериям, указанным в инструкции **EXCLUDE**, он будет игнорирован независимо от того, присутствует ли в спецификации фильтра инструкции **INCLUDE и EXCLUDE**. Сетевой монитор не проверяет, удовлетворяет ли этот пакет условиям инструкций **INCLUDE**.

Например, чтобы записать весь трафик компьютера **Comp1** за исключением трафика между компьютерами **Comp1 и Comp2**, следует указать следующие адресные пары в разделе пар адресов дерева критериев:

Addresses

include Comp1 <----> Any

exclude Comp1 <----> Comp2

Если в списке отсутствуют инструкции INCLUDE, то неявно будет использоваться пара локальный_компьютер <----> любой_компьютер.

Фильтрация на основе соответствия шаблону

Указывая шаблон для соответствия в фильтре записи, имеется возможность:

- ограничить запись подмножеством кадров, которые содержат указанный шаблон (его можно задавать в текстовом или шестнадцатеричном виде);
- определить, на каком расстоянии (смещение) от начала или конца кадра должен начаться поиск.

При задании фильтра соответствия шаблону необходимо указать место в кадре, откуда должен начаться поиск соответствия шаблону. Эти настройки определяют расстояние в байтах от начала кадра или от конца заголовка топологии до места совпадения шаблона. Если пакеты

не имеют постоянной длины (например пакеты протокола MAC в сетях Ethernet или Token Ring), следует указывать смещение от конца заголовка пакета соответствующей топологии.

Триггеры записи.

После создания триггеров записи сетевой монитор может отвечать на события в сети. По умолчанию условия включения триггера не установлены.

Типы триггеров

С помощью сетевого монитора можно определить степень заполнения буфера записи и наличие определенного шаблона данных в записанном кадре. Можно создавать триггеры записи на основе одного из этих условий или на основе обоих условий.

Если триггер задан на основе определенного шаблона данных в записанном кадре, то сетевой монитор выполнит определенное действие при обнаружении кадра с нужным шаблоном. Шаблон может быть задан шестнадцатеричной строкой или строкой ASCII. Можно задать триггер на основе определенного шаблона данных в записанном кадре и определенного процента заполнения буфера записи. Также можно задать начало поиска для сетевого монитора: с начала каждого кадра, после заголовка каждого кадра или через несколько байт после любого из этих положений. По умолчанию сетевой монитор выполняет поиск по шаблону для всего кадра.

Действия триггера

Можно выбрать одно из следующих действий триггера, которое будет исполняться при выполнении условий триггера.

- Компьютер издает звуковой сигнал.
- Сетевой монитор прекращает запись кадров.
- Выполняется выбранная команда.

Чтобы задать команду, которая запускает программу, введите имя и путь к файлу программы, или нажмите кнопку Обзор и найдите файл программы. Для использования команды MS-DOS, такой как copy, введите CMD /K и затем введите команду.

Установка сетевого монитора.

Чтобы установить сетевой монитор выполните следующее:

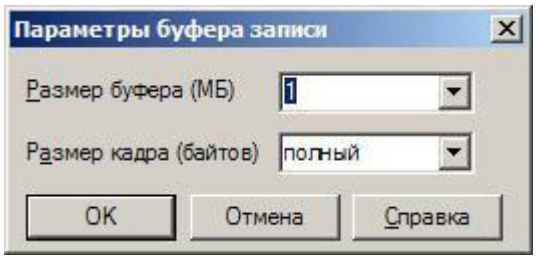
- Откройте Мастер компонентов Windows.
- В мастере компонентов Windows выберите **Средства управления и наблюдения (Management and Monitoring Tools)**, а затем нажмите кнопку **Состав**.
- Установите флажок **Средства сетевого монитора (Network Monitor)** и нажмите кнопку **OK.**

В случае запроса дополнительных файлов вставьте установочный компакт-диск операционной системы или укажите путь к расположению этих файлов в сети.

Эта процедура автоматически устанавливает драйвер сетевого монитора.

Настройка сетевого монитора.

Вы можете изменить параметры буфера записи, для этого, в меню **Запись** выберите команду **Параметры буфера**.

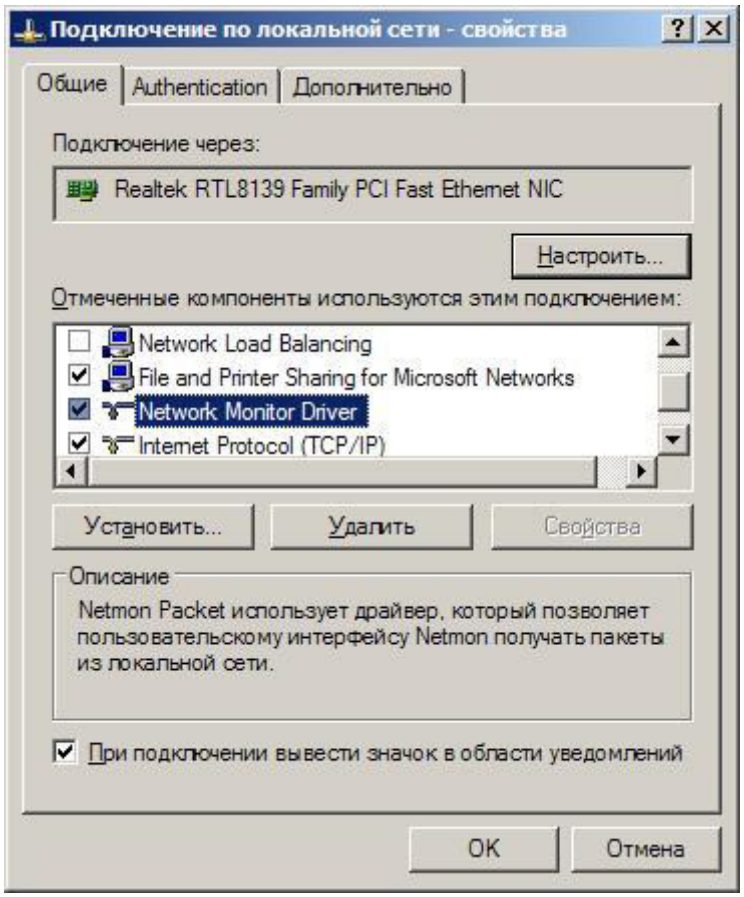


Задание максимального размера буфера записи. При необходимости можно задать максимальный размер записанных кадров и нажать кнопку **OK**.

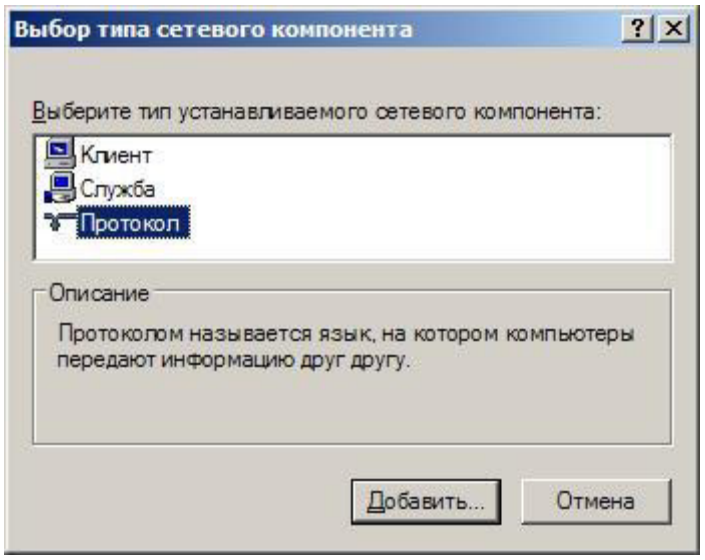
Если размер буфера превышает объем доступной памяти компьютера, то кадры могут теряться.

Вы также можете установить драйвер сетевого монитора. Для этого откройте компонент Сетевые подключения, выделите значок Подключение по локальной сети, а затем выберите

команду **Свойства** из меню Файл.



В диалоговом окне Свойства подключения по локальной сети нажмите кнопку **Установить.**



В диалоговом окне Выбор типа сетевого компонента выберите строку Протокол и нажмите кнопку **Добавить**.

В диалоговом окне Выбор сетевого протокола выберите Драйвер сетевого монитора и нажмите кнопку **Добавить**.

В случае запроса дополнительных файлов вставьте установочный компакт-диск операционной системы или укажите путь к расположению этих файлов в сети.

Если Драйвер сетевого монитора уже установлен, то он не появится в диалоговом окне Выбор сетевого протокола.

Практическое задание №26,27

Устранение неполадок с помощью Ping и PathPing

Ping служит для проверки связи на уровне IP, а PathPing позволяет обнаружить потерю пакетов на маршруте со многими переходами. Команда Ping направляет эхо-запрос узла или IP-адреса по протоколу ICMP. Используйте Ping для проверки возможности узла передавать IP-пакеты другому узлу-адресату. Также эта команда применяется для устранения неполадок оборудования и несовместимости конфигурации.

Устранение неполадок сетевой связи с помощью команды Ping рекомендуется выполнять в такой последовательности.

Примечание Информация, получаемая в пп. 1 и 2, также предоставляется командой Ipconfig /all и Netdiag. (*Диагностика сети* автоматически выполняет только п. 2. Если эта утилита сообщает о неудаче самопроверки, можно выполнить п. 1 вручную.)

1. Проверьте с помощью Ping *адрес замыкания на себя* (loopback address), чтобы убедиться в наличии и корректности настройки TCP/IP на локальном компьютере. Для этого в командной строке выполните команду:

ping 127.0.0.1.

Отсутствие реакции говорит о неполадках стека IP: порче драйверов TCP, неработоспособности сетевого адаптера или конфликта IP с другой службой.

2. Проверьте правильную настройку своего адреса (нет ли адресов – дубликатов в сети) командой:

ping <*свой IP-адрес*>

3. Проверьте работу внутри сетевого сегмента:

ping <*соседний IP-адрес в локальной сети*>

4. Проверьте доступность IP-адреса основного шлюза:

Это позволяет убедиться в доступности основного шлюза и способности локального компьютера связываться с другими узлами сети.

ping <*IP-адрес основного шлюза* >

5. Проверьте доступность удаленного узла, расположенного за основным шлюзом:

ping <*IP-адрес удаленного узла*>

Это проверка связи с узлами других сетевых сегментов

Примечание Для более быстрого выполнения последней проверки можно воспользоваться командой Tracert утилиты PathPing. Tracert находит сбойные места сети, но не предоставляет статистики об эффективности маршрутизатора.

Ping использует разрешение имен узлов для определения IP-адреса на основании имени компьютера, поэтому если при указании адреса проверка утилитой Ping проходит успешно, а при указании имени — нет, то проблема в механизме разрешения имен, а не сетевых подключениях.

Если проверка с помощью Ping вообще не дает результатов, надо удостовериться:

- правильно ли определен IP-адрес и маска подсети локального компьютера;
- определен ли основной шлюз и есть ли связь между узлом и основным шлюзом. При устранении неполадок обязательно определять не более одного основного шлюза.

Примечание Если на пути к удаленной системе, проверяемой эхо-запросом Ping, находится отрезок, характеризующийся большими задержками, например линия спутниковой связи, на получение эхо-ответов может понадобиться больше времени. Для увеличения тайм-аута служит параметр —w, например команда

ping -w 2000 172.16.48.10

ожидает ответа 2 секунды (по умолчанию — 1 сек, или 1000 мс).

Устранение неполадок с помощью Tracert

Tracert отслеживает маршрут пакета на расстоянии до 30 переходов между маршрутизаторами. Tracert направляет эхо-запрос по протоколу ICMP на IP-адрес и увеличивает поле TTL в IP-заголовке, начиная с единицы, и анализирует возвращенные ошибки протокола ICMP. Tracert выводит упорядоченный список маршрутизаторов на пути пакета, которые возвратили сообщения об ошибках. В следующем примере Tracert применяется для проверки пути от локального компьютера к удаленному с адресом www.contoso.com.

C:\>tracert www.contoso.com

Tracing route to www.contoso.com [10.10 2.252.1]

over a maximum of 30 hops:

1. 300 ms 281 ms 280 ms roto.contoso.co m [10.181.164.100]
2. 300 ms 301 ms 310 ms sl-stk-1-S12- T1.contoso.com [10.228.192.65]
3. 300 ms 311 ms 320 ms sl-stk-5-FO/ 0.contoso.com [10.228.40.5]
4. 380 ms 311 ms 340 ms icm-fix-w-H2/0- T3.contoso.com [10.228.10.22]
5. 310 ms 301 ms 320 ms arc-nas- gw.arc.contoso.com [10.203.230.3]
6. 300 ms 321 ms 320 ms n254-ed- cisco7010.contoso.com [10.102.64.254]
7. 360 ms 361 ms 371 ms www.contoso.com [10.102.252.1]

Надо четко понимать разницу между Tracert и PathPing. Tracert применяется для быстрого определения разрыва на пути к удаленному узлу, а PathPing полезнее в ситуациях, когда наблюдается эпизодическая потеря пакетов или длительные задержки. PathPing позволяет точно установить, где потерялся пакет.

Устранение неполадок с помощью утилиты ARP

Иногда сетевой трафик не проходит из-за того, что в ответ на ARP-запрос

прокси маршрутизатора возвращает неправильный адрес. Если удается получить ответы на эхо-запросы Ping по адресу замыкания на себя и собственному IP-адресу компьютера, но Ping-запрос другого компьютера локальной подсети терпит неудачу, то далее следует проверить корректность информации в кэше ARP.

Команда ARP позволяет изучить содержимое кэша ARP Если два узла одной подсети не в состоянии обменяться эхо-запросами, попытайтесь выполнить на обоих компьютерах команду ARP с параметром -a, это позволит выяснить корректность определения MAC-адресов компьютера-адресата. Для определения MAC-адреса можно воспользоваться командой Ipconfig /all или Getmac. Затем надо выполнить команду ARP с параметром -d, чтобы удалить все неправильные записи; новые записи создаются с помощью параметра -s.

Если эхо-запрос Ping компьютера локальной подсети по IP-адресу безуспешен, а команда ARP -a говорит об отсутствии ошибок в MAC-адресах, надо проверить исправность физических устройств — сетевых карт, концентраторов и кабелей.

Настройка TCP/IP-адресов

Упражнение 1. Проверка существующего IP-адреса

1. Войдите в систему

Login администратор

Password

Domen IT7 (SDC)

Из командной строки исполните **ipconfig /all**. Эта команда служит для просмотра конфигурации протокола IP и выводит на экран информацию о сетевых подключениях.

Упражнение 2. Ручная настройка адреса

В этом упражнении надо назначить статический IP-адрес компьютеру. Статический IP-адрес необходим компьютерам, на которых устанавливаются важные сетевые сервисы, например DNS или DHCP

1. В окне **Сетевые подключения** щелкните правой кнопкой **Подключение по локальной сети (Local Area Connection)** и выберите **Свойства** (операции выполняются под учетной записью *Администратор).*
2. В списке **Отмеченные компоненты используются этим подключением (This connection uses the following items)** диалогового окна **Подключение по локальной сети — свойства (Local Area Connection Properties)** выберите **Протокол Интернета (TCP/IP) [Internet Protocol (TCP/IP)]** и щелкните **Свойства.**
3. На вкладке **Общие** окна свойств TCP/IP установите переключатель **Использовать следующий IP-адрес (Use the following IP address).**
4. **В** поле **IP-адрес (IP Address)** введите 192.168.0.1.
5. Поместите курсор в поле **Маска подсети (Subnet Mask). В** нем появится значение маски подсети — 255.255.255.0. Щелкните ОК.
6. Закройте окно **Подключение по локальной сети — свойства.**
7. Проверьте назначение адреса с помощью **ipconfig**.

3. Настройка альтернативного статического адреса

В этом упражнении вы измените конфигурацию компьютера так, чтобы при отсутствии DHCP-сервера ему присваивался заданный адрес.

1. В окне **Сетевые подключения** щелкните правой кнопкой **Подключение по локальной сети** и выберите **Свойства.**

В списке **Компоненты, используемые этим подключением (This connection uses the following items)** отображаются компоненты подключения к локальной сети: **Клиент для сетей Microsoft (Client for microsoft networks), Служба доступа к файлам и принтерам сетей Microsoft (File and printer sharing for Microsoft networks)** и **Прото кол Интернета (TCP/ IP) [Internet Protocol (TCP/ IP)].**

2. Выберите **Протокол Интернета (TCP/ IP)** и щелкните **Свойства.**

Убедитесь, что на вкладке **Общие** установлены

переключатели **Получить IP-адрес автоматически (Obtain an IP address automatically)** и **Получить адрес DNS-сервера автоматически (Obtain DNS server address automatically).**

3. Перейдите на вкладку **Альтернативная конфигурация.** На ней установлен переключатель **Автоматический частный IP-адрес (Automatic Private IP Address).**
4. Установите переключатель **Настраиваемый пользователем (User Configured).**
5. В поле **IP-адрес** введите 192.168.0.2.
6. Поместите курсор в поле **Маска подсети. В** нем появится значение маски подсети по умолчанию — 255.255.255.0. Оставьте его без изменений и щелкните **ОК.** Заданный альтернативный IP-адрес 192.168.0.2 будет использоваться, пока недоступен DHCP-сервер.
7. Закройте окно **Подключение по локальной сети — свойства.**
8. Проверьте назначение адреса с помощью **ipconfig**.

Диагностика сети

Упражнение 1. Устранение неполадок с помощью Ping

1. Проверьте с помощью Ping *адрес замыкания на себя* (loopback address), чтобы убедиться в наличии и корректности настройки TCP/IP на локальном компьютере. Для этого в командной строке выполните команду:

ping 127.0.0.1.

Отсутствие реакции говорит о неполадках стека IP: порче драйверов TCP, неработоспособности сетевого адаптера или конфликта IP с другой службой.

2. Проверьте правильную настройку своего адреса (нет ли адресов – дубликатов в сети) командой:

ping <*свой IP-адрес*>

3. Проверьте работу внутри сетевого сегмента:

ping <*соседний IP-адрес в локальной сети*>

4. Проверьте доступность IP-адреса основного шлюза:

Это позволяет убедиться в доступности основного шлюза и способности локального компьютера связываться с другими узлами сети.

ping <*IP-адрес основного шлюза* >

Упражнение 2. Использование утилиты диагностики сети

Вы воспользуетесь утилитами *Диагностика сети* (Network Diagnostics) и сохраните результаты их работы в файлах.

Выберите **Пуск (Start)/ Cnpавка и поддержка (Help and Support).** Откроется окно **Центр справки и поддержки (Help and Support Center).**

1. **В** панели **Задачи поддержки (Support Tasks)** выберите **Служебные программы (Tools).**
2. **В** панели **Средства (Tools)** разверните узел **Средства центра справки и поддержки (Help and Support Center Tools)** и выберите **Диагностика сети (Network Diagnostics).**
3. Щелкните кнопку **Собрать информацию (Scan Your System).** Несколько секунд потреуется на проверки, а затем появятся данные, разбитые на три раздела: **Службы Интернета (Internet Service), Информация о компьютере (Computer Information)** и **Модемы и сетевые адаптеры (Modems and Network Adapters).**
4. Разверните узлы всех категорий, щелчком соответствующих значков «плюс» — появится полная информация о только что выполненных проверках. Познакомьтесь с представленным сведениями.
5. Вернитесь в окно **Диагностика сети** и щелкните кнопку **Настроить параметры сбора информации (Set Scanning Options).** Под заголовком **Параметры (Options)** появятся списки **Действия (Actions)** и **Категории (Categories).**

8. В списке **Действия** установите флажок **Подробно (Verbose).**
9. **В** списке **Категории** сбросьте следующие флажки: **Почтовая**

служба (Mail Service), Служба новостей (News Service), Прокси-сервер (Internet Proxy Server), Информация о компьютере (Computer Information), Операционная система (Operating System) и Версия Windows (Windows Version). Должны остаться только **Модемы (Modems), Сетевые Клиенты (Network Clients) и Сетевые адаптеры (Adapters).**

10. Щелкните кнопку **Собрать информацию.** По завершении проверок появится только информация категории **Модемы и сетевые адаптеры.**
11. Щелкните кнопку **Сохранить в файл (Save to file),** чтобы сохранить результаты в файл. Откроется информационное окно с сообщением о том, что файл сохранен на рабочем столе и в еще одной папке (она указана). Щелчком **ОК** закройте окно.
12. Щелкните ссылку **Показать сохраненные файлы (Show Saved Files)** рядом с кнопкой **Сохранить в файл.** Откроется одна из папок, в которой сохранен новый файл.
13. На панели **Быстрый запуск (Quick Launch)** щелкните **Показать рабочий стол (Show Desktop).** На рабочем столе находится другая копия HTML-файла, созданного утилитой **Диагностика сети.**
14. Закройте ненужные окна.

Практическое задание №28,29

Описание команды NETSTAT

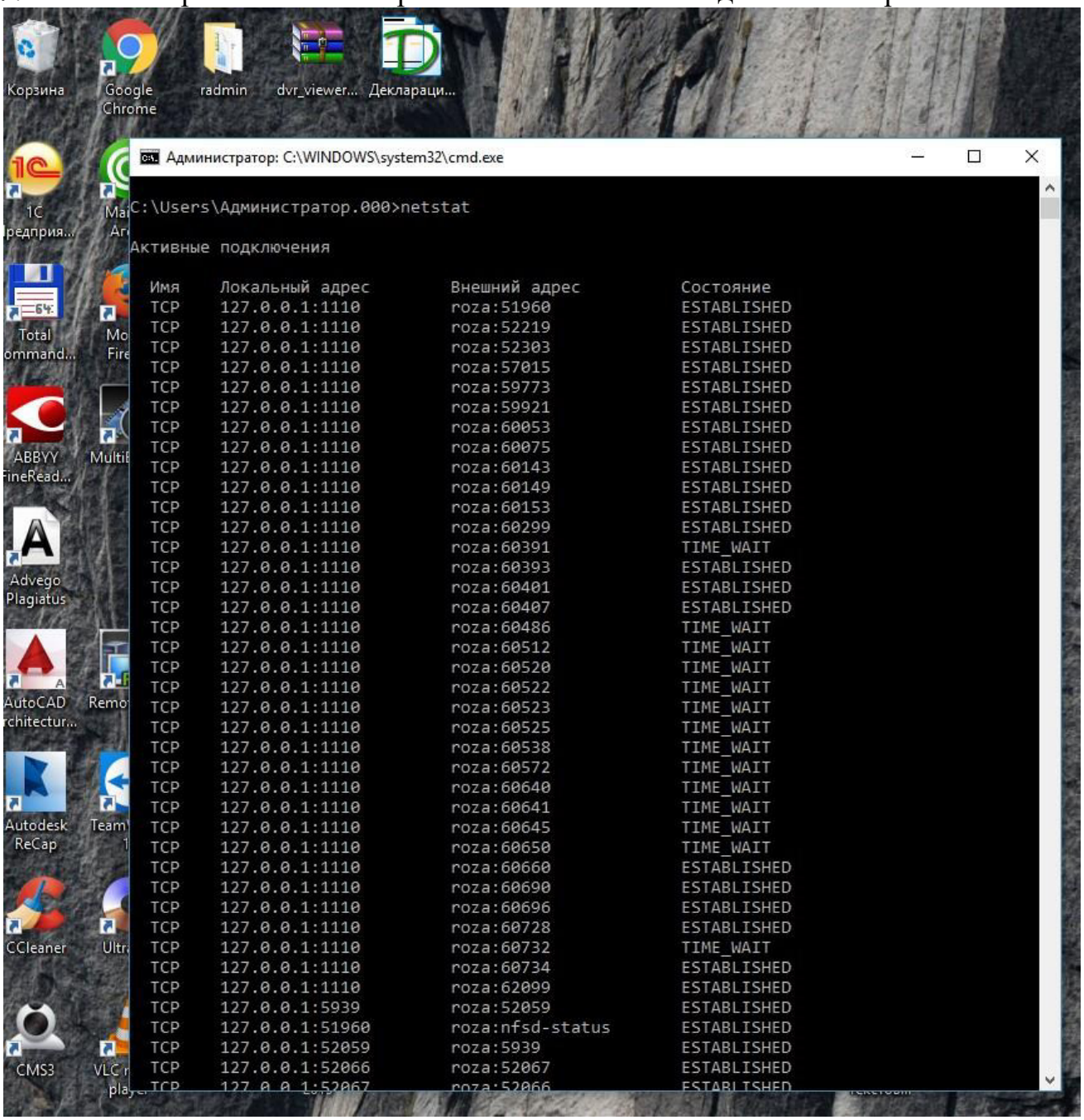
Netstat - это утилита командной строки Windows выводящая на дисплей состояние TCP-соединений. Команда netstat отображает статистику активных подключений TCP, портов, прослушиваемых компьютером, статистики Ethernet, таблицы маршрутизации IP, статистики IPv4 (для протоколов IP, ICMP, TCP и UDP) и IPv6 (для протоколов IPv6, ICMPv6, TCP через IPv6 и UDP через IPv6). Запущенная без параметров, команда netstat отображает подключения TCP.

Синтаксис и параметры команды NETSTAT

netstat [-a] [-e] [-n] [-o] [-p протокол] [-r] [-s] [интервал], где

- *-a* - вывод всех активных подключений TCP и прослушиваемых компьютером портов TCP и UDP.
- *-e* - вывод статистики Ethernet, например количества отправленных и принятых байтов и пакетов. Этот параметр может комбинироваться с ключом -s.
- *-n* - вывод активных подключений TCP с отображением адресов и номеров портов в числовом формате без попыток определения имен.
- *-o* - вывод активных подключений TCP и включение кода процесса (PID) для каждого подключения. Код процесса позволяет найти приложение на вкладке Процессы диспетчера задач Windows. Этот параметр может комбинироваться с ключами -a, -n и -p.
- *-p протокол* - вывод подключений для протокола, указанного параметром протокол. В этом случае параметр протокол может принимать значения tcp, udp, tcpv6 или udpv6. Если данный параметр используется с ключом -s для вывода статистики по протоколу, параметр протокол может иметь значение tcp, udp, icmp, ip, tcpv6, udpv6, icmpv6 или ipv6.
- *-s* - вывод статистики по протоколу. По умолчанию выводится статистика для протоколов TCP, UDP, ICMP и IP. Если установлен протокол IPv6 для Windows XP, отображается статистика для протоколов TCP через IPv6, UDP через IPv6, ICMPv6 и IPv6. Параметр -p может использоваться для указания набора протоколов.
- *-r* - вывод содержимого таблицы маршрутизации IP. Эта команда эквивалентна команде route print.
- *интервал* - обновление выбранных данных с интервалом, определенным параметром интервал (в секундах). Нажатие клавиш CTRL+C останавливает обновление. Если этот параметр пропущен, netstat выводит выбранные данные только один раз.

- */?* - отображение справки в командной строке.



Примеры команды NETSTAT

Пример работы команды Netstat на Windows 10 показан на рисунке выше, утилита работает на всех версиях операционных систем Windows.

- Для отображения справки по команде введите в командной строке **netstat /?**;
- Для вывода статистики Ethernet и статистики по всем протоколам введите следующую команду: **netstat -e -s**;
- Для вывода статистики только по протоколам TCP и UDP введите следующую команду: **netstat -s -p tcp udp**;

- Для вывода активных подключений TCP и кодов процессов каждые 5 секунд введите следующую команду: **netstat -o 5**.