|  |  |
| --- | --- |
| Департамент образования Ярославской области  Государственное профессиональное образовательное автономное учреждение  Ярославской области  «ЯРОСЛАВСКИЙ ПРОМЫШЛЕННО-ЭКОНОМИЧЕСКИЙ КОЛЛЕДЖ  им. Н.П. ПАСТУХОВА» | |
| **Отчет По учебной практике**  **по междисциплинарному курсу МДК.07.02**  **Сертификация информационных систем** | |
| ОУП МДК.07.02.09.02.07.18ИП1,2.13 | |
|  | |
|  | |
|  | |
|  | |
|  | Студент  \_\_\_\_\_\_\_\_\_\_\_\_\_ А.Э. Кязимова  «\_\_\_\_» Февраль 2022 г. |
|  | Преподаватель  \_\_\_\_\_\_\_\_\_\_\_\_\_ К. А. Простова  «\_\_\_\_» Февраль 2022 г. |
| 2022 | |

Содержание

[Лабораторная работа №1 3](#_Toc96538718)

[Лабораторная работа №2 17](#_Toc96538719)

[Лабораторная работа №3 26](#_Toc96538720)

[Лабораторная работа №4 31](#_Toc96538721)

[Лабораторная работа №5 35](#_Toc96538722)

[Лабораторная работа №6-7 38](#_Toc96538723)

# **Лабораторная работа №1**

**Настройка политики безопасности**

**Цель работы:** освоение средств администратора, предназначенных для:

* регистрации пользователей и групп в системе, определения их привилегий;
* определения параметров политики безопасности, относящихся к аутентификации;
* авторизации пользователей при интерактивном входе;
* определения параметров политики безопасности;
* определения параметров политики аудита;
* просмотра и очистки журнала аудита;
* разграничения доступа субъектов к папкам и файлам;
* обеспечения конфиденциальности папок и файлов с помощью, шифрующей файловой
* системы;
* определения параметров политики ограниченного использования программ.

**Выполнение работы**

Для дальнейшей работы создадим пользователя.

Откроем панель управления (Рис. 1)

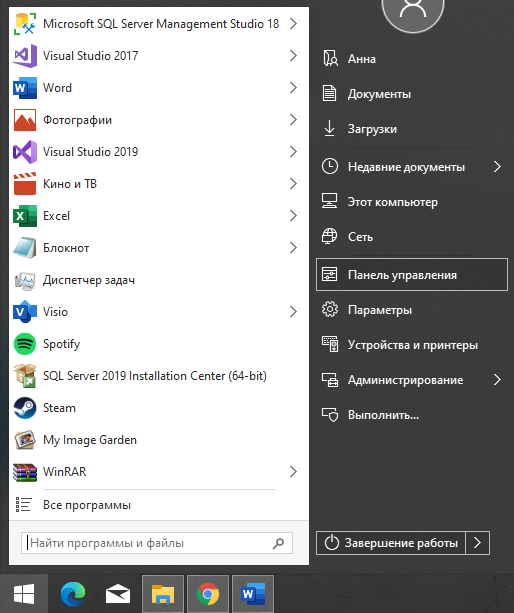


Рисунок 1 Меню Пуск

Далее Администрирование ->Управление компьютером -> Локальные пользователи (Рис. 2-4)

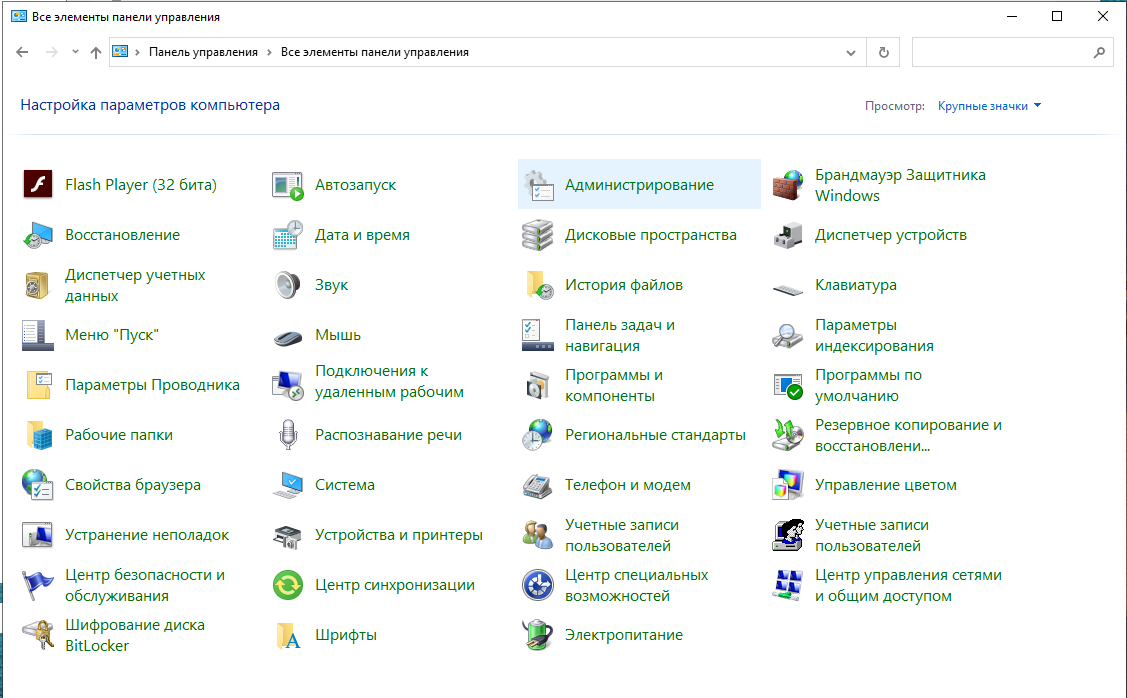


Рисунок 2 Администрирование

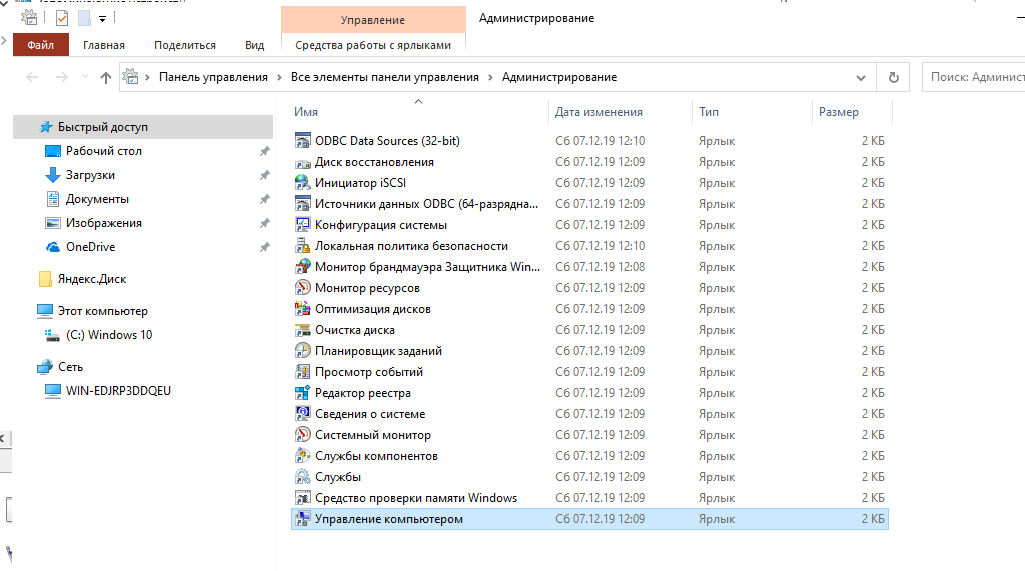


Рисунок 3 Управление компьютером

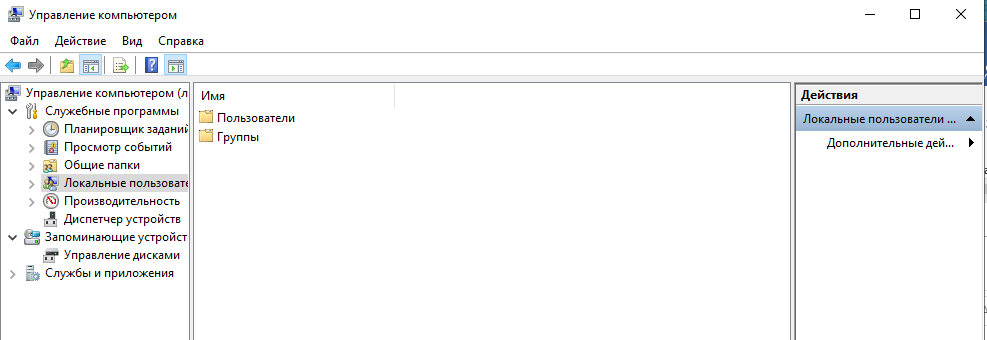


Рисунок 4 Локальные пользователи

Создадим группу новых пользователей (Рис.5)

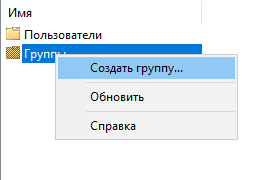


Рисунок 5 Создание группы пользователей

Укажем имя и пароль для пользователя (Рис. 6)

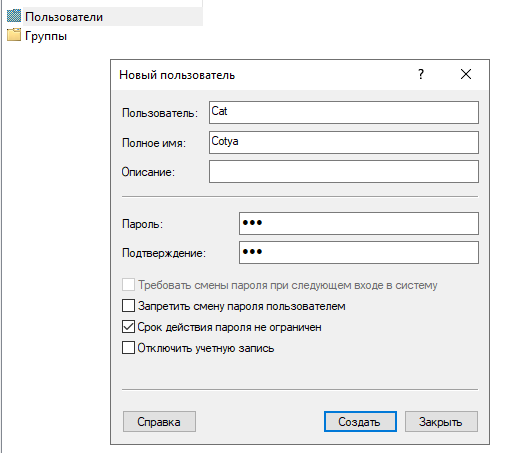


Рисунок 6 Создание пользователя

Теперь новый пользватель появился в списке (Рис. 7)

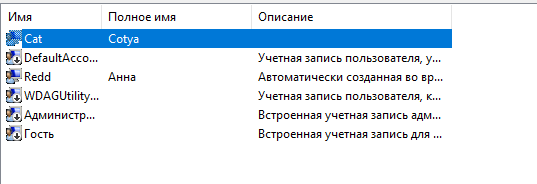


Рисунок 7 Список пользователей

**Задание 1.** Изучите:

* 1. настройку Политики безопасности на своем ПК.

В окне Администрирования выберем пункт Локальная политика безопасности (Рис. 8)

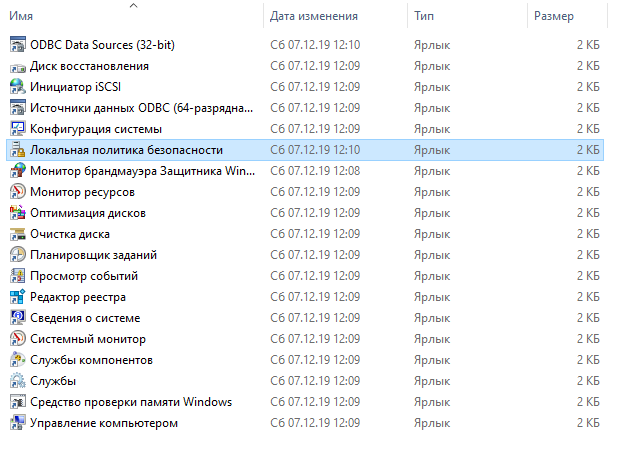


Рисунок 8 Локальная политика безопасности

В папке Локальные политики->Назначение прав аользователя можно настроить права для каждого пользователя (Рис. 9)

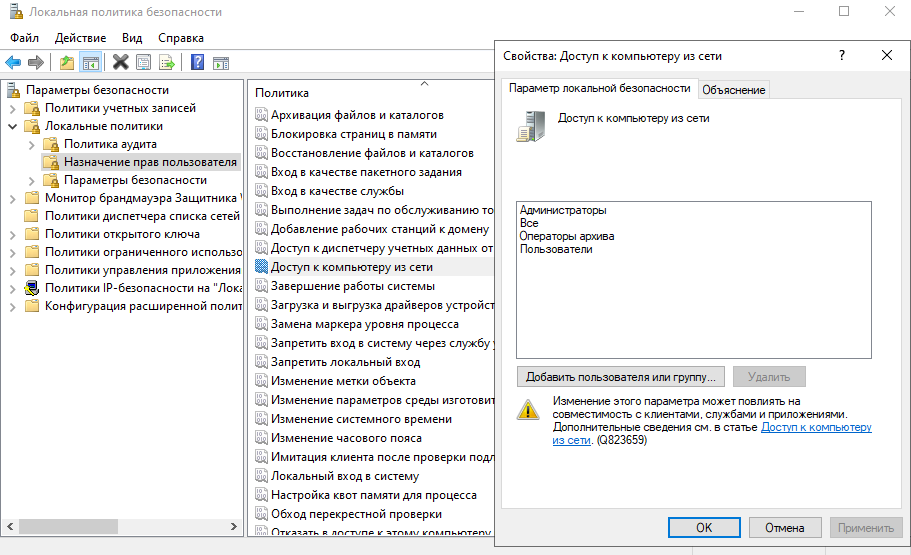


Рисунок 9 Предоставление доступа к компьютеру из сети

Нажав кнопку Добавить пользователя или группу..->Дополнительно (Рис. 10)

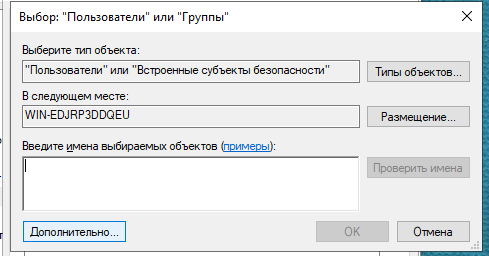


Рисунок 10 Добавление пользователя

Из списка можно выбрать пользовательей которым нужно предоставит доступ (Рис. 11)

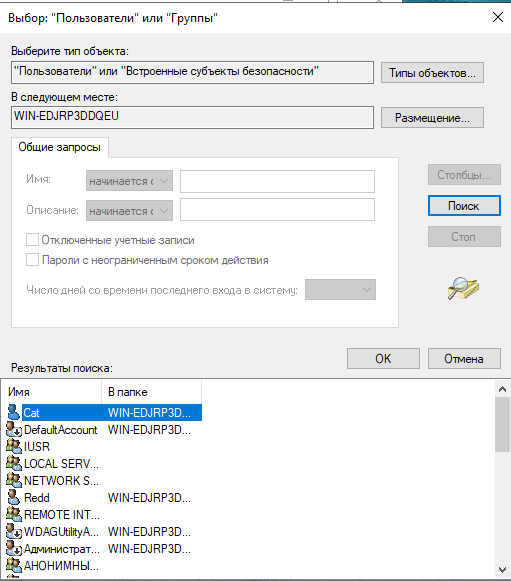


Рисунок 11 Выбор пользователей

Можно установить отдельным пользователям Локальный вход в систему(Рис. 12)

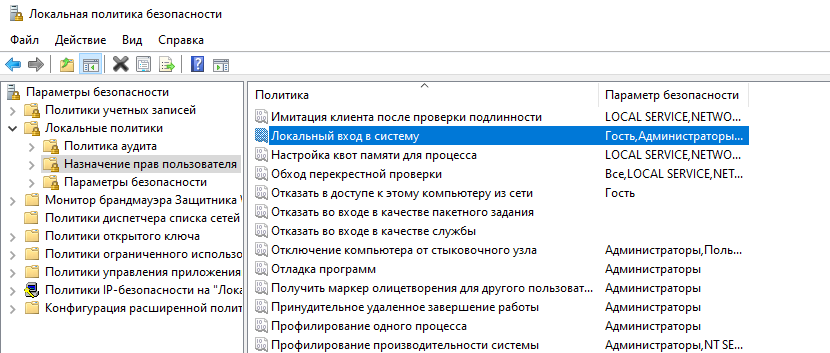


Рисунок 12 Назначение прав

Так же можно указать состояние учетных записей (Рис. 13)

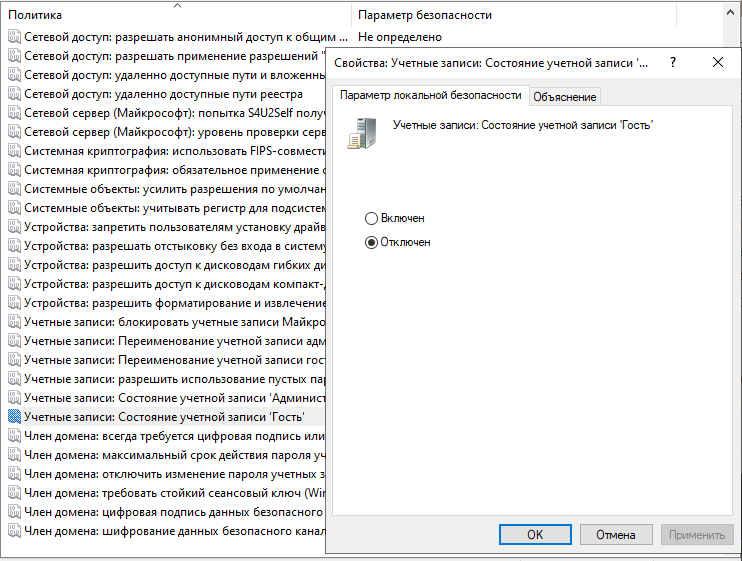


Рисунок 13 Состояние записи

* 1. настройку Параметров безопасности на своем ПК.

В параметрах безопасности можно установить стктус политики (Рис. 13)

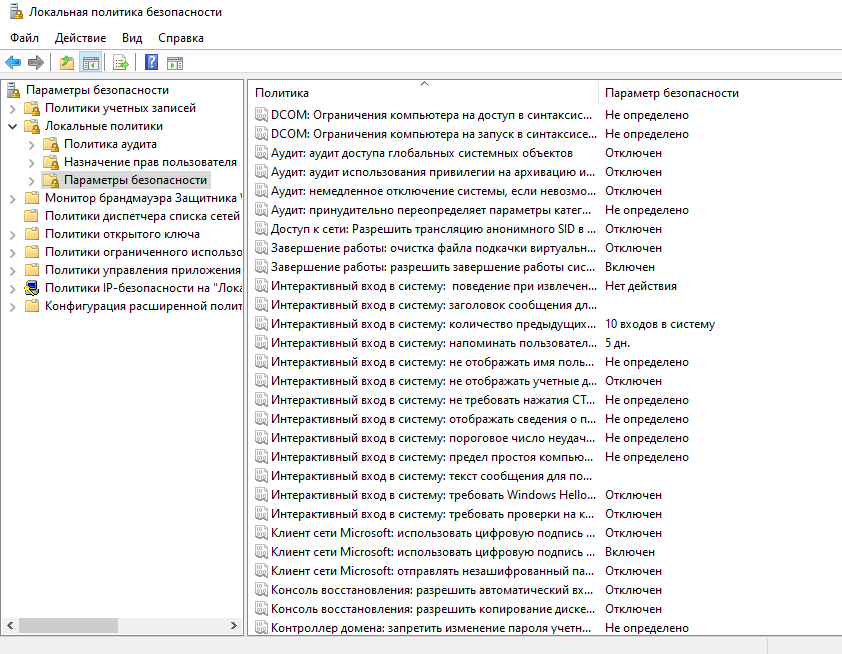


Рисунок 14 Параметры безопасности

* 1. настройку Политики обновления на своем ПК.

В параметрах Windows выберем Обновление безопасности (Рис. 15)

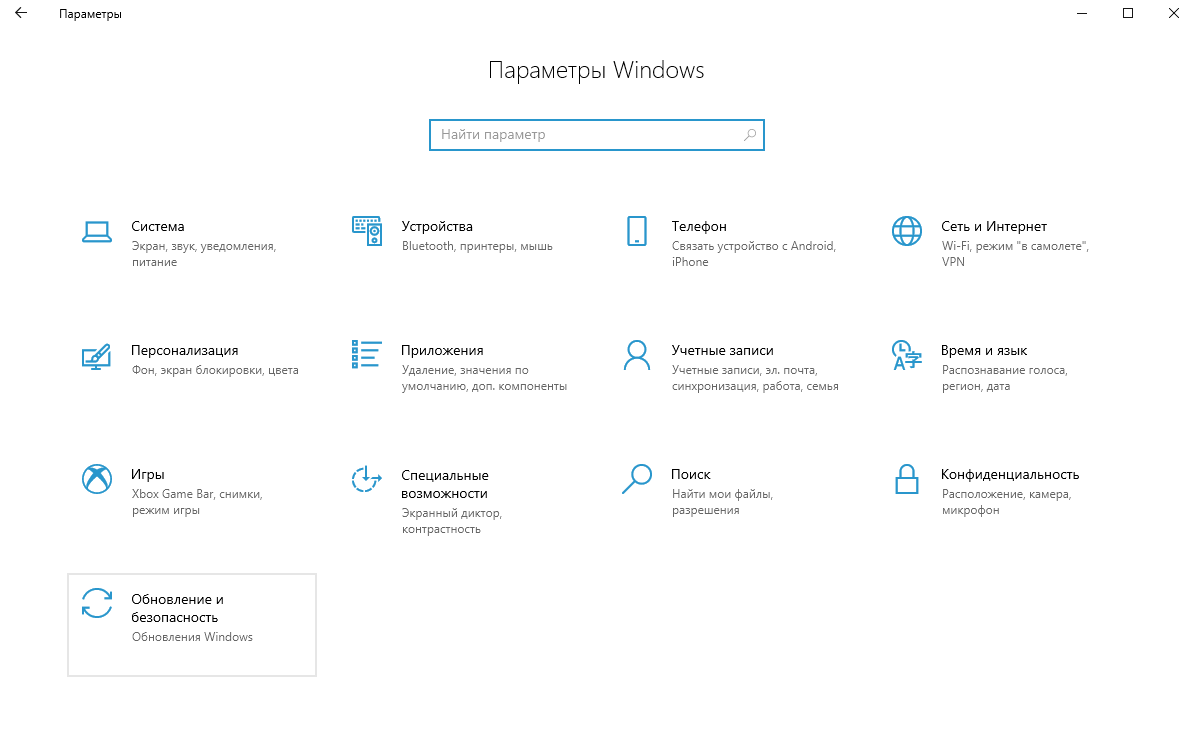


Рисунок 15 Обновление безопасности

В центре обновления можно проверить наличие обновлений системы (Рис. 16)

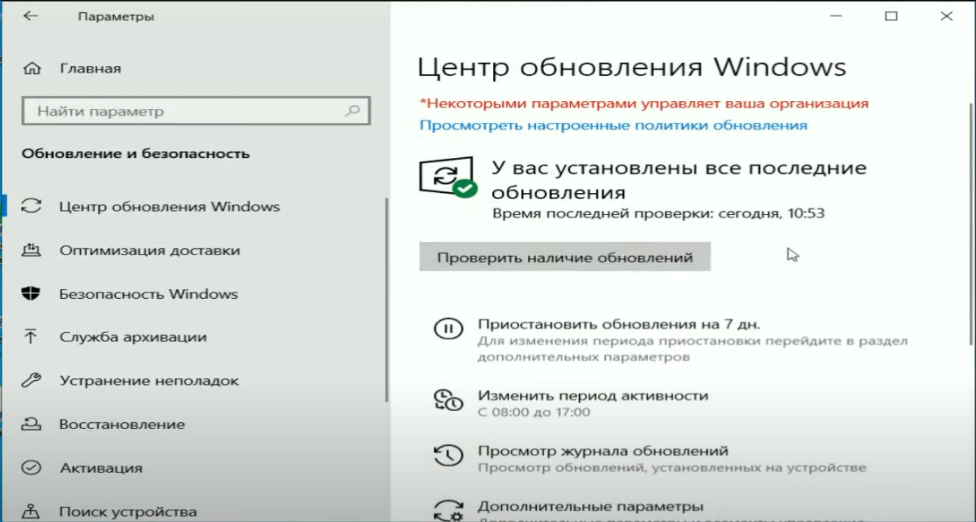


Рисунок 16 Центр обновлений

Запустив проверку на наличие обновлений, программа либо не обнаружит их либо начнет обновление системы (Рис.17)

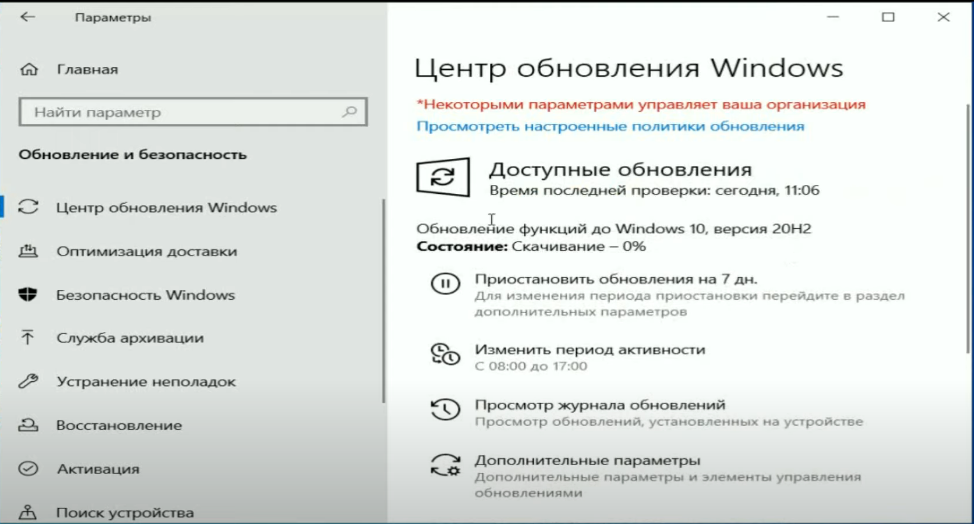


Рисунок 17 Поиск обновлений системы

После программа предложит перезагрузить систему для применения обновлений (Рис. 18)

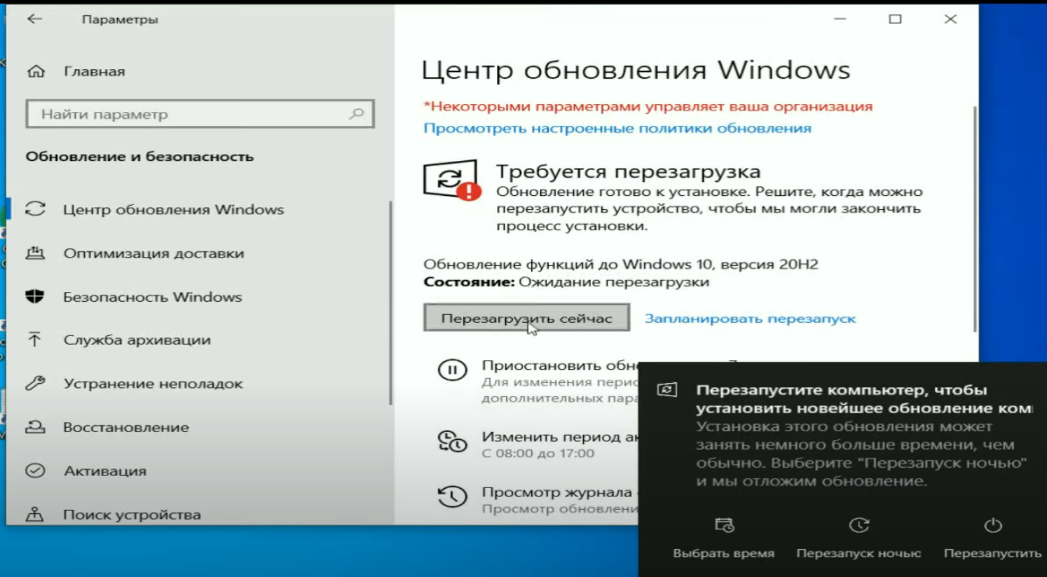


Рисунок 18 Обновление Windows

**Задание 2.** Ответьте на вопросы:

1. Определите назначение политики безопасности системы.

Политика безопасности определяет, что необходимо защитить и что вы ожидаете от пользователей системы. Она обеспечивает основу для планирования безопасности при разработке новых объектов или расширения вашей текущей сети.

1. Где производится настройка политики безопасности системы?

Пуск | Панель управления | Администрирование | Локальная политика безопасности | Параметры безопасности

1. Как запретить доступ сетевых пользователей к компьютеру?

Запретить доступ сетевым пользователям к компьютеру можно через Локальные политики->Назначение прав пользователя

1. Как разрешить доступ сетевым пользователям, которым разрешено работать в системе к компьютеру?

Разрешить доступ сетевым пользователям к компьютеру можно через Локальные политики->Назначение прав пользователя

1. Определите назначения пункта политики безопасности «Разрешать вход в систему через службу терминалов».

Пункт «Разрешать вход в систему через службу терминалов» определяет, какие именно пользователи и группы пользователей могут получать доступ к данному компьютеру по компьютерной сети, но вход пользователей в систему осуществляется в качестве клиентов терминал- сервера. Если данный сервис не используется, то рекомендуется аналогичным методом запретить вход в систему всех пользователей, убрав их из значения данного пункта как клиентов терминал- сервера.

1. Как предоставить определенной группе пользователей вносить изменения в системное время?

Для разрешения пользователям выполнять такое действие следует их внести в список данного пункта политики безопасности при помощи кнопки «Добавить пользователя или группу».

1. Определите назначение пункта политики безопасности Отладка программ.

Пункт «Отладка программ» позволяет указать пользователей, которые смогут подсоединять свой отладчик к процессам и производить их отладку. Следует включать в этот пункт только тех пользователей, которым это действительно нужно, например, системный администратор и системные программисты.

1. Каким образом запретить вход определенной группе пользователей в систему по локальной сети?

Запретить вход сетевым пользователям к компьютеру можно через Локальные политики->Назначение прав пользователя

1. Определите назначение пункта политики безопасности Принудительное удаленное завершение.

Пункт «Принудительное удаленное завершение» является очень важным в настройке локальной политики безопасности, так как если его не настроить соответствующим образом, то система может получить команду на выключение или перезагрузку от удаленно пользователя.

1. Как установить пользователей и их группы, которые могут локально входить в систему?

Можно через Локальные политики->Назначение прав пользователя->Локальный вход в систему

1. Как запретить определенной группе пользователей завершать работу системы, и в каких случаях это актуально?

Пункт «Завершение работы системы» указывает, кто из локальных пользователей, имеющих учетные записи в системе, имеет право на ее выключение или перезагрузку. По умолчанию на это имеют право все пользователи. Однако, в ряде случаев, может потребоваться запретить выполнять данные функции некоторым пользователям. Например, если нужно, чтобы компьютеры работали в то время, когда некоторые пользователи их пытаются отключить. В этом случае нужно убрать этих пользователей из данного пункта. Особенно это может быть полезно, если определенные пользователи пытаются выключить компьютер, на котором находится информация, используемая удаленно другими пользователями.

1. В каком разделе производится настройка глобальных параметров безопасности?

Глобальные параметры безопасности устанавливаются в разделе локальной политики безопасности Параметры безопасности.

Пуск\Панель управления\Администрирование\Локальная политика безопасности\ Параметры безопасности

1. Определите назначение политики обновления.

простой метод, который позволяет практически со стопроцентной вероятностью избавиться от ошибок в конечных продуктах, находящихся у пользователей. Этим методом является периодическое обновление программных продуктов.

1. Как произвести настройку политики обновления?

Все операции настройки политики обновления ОС, а также выполнения процедуры обновления и получения от нее различных сообщений возможны только под учетной записью администратора системы. После запуска программы появится окно, в котором нужно выбрать закладку Автоматическое обновление

1. Какие события безопасности должны фиксироваться в журнале аудита?

регистрацию в журнале аудита успешных и неудачных попыток:

* входа в систему;
* доступа к объектам;
* доступа к службе каталогов;
* изменения политики;
* использования привилегий;
* отслеживания процессов;
* системных событий;
* событий входа в систему;
* управления учетными записями.

1. Какие параметры определяют политику аудита?

Основные параметры политики аудита в области безопасности:

* Аудит событий входа в систему
* Аудит управления учетными записями
* Аудит доступа к службе каталогов
* Аудит события входа
* Аудит доступа к объектам
* Аудит изменения политики
* Аудит использования привилегий

1. Какие факторы влияют на определение размеров доменов безопасности?

Следующие факторы определяют размеры доменов:

* гибкость и простота механизма переключения доменов
* размер защищаемых объектов
* наличие разных способов изменения матрицы доступа
* гибкость в определении произвольных типов доступа к объектам

1. Какие дополнительные возможности разграничения доступа к информационным ресурсам предоставляет шифрующая файловая система?

Для выполнения операции шифрования файлов и папок нужно выполнить команду «Свойства» контекстного меню Вашей папки или файла, и на вкладке «Общие» окна свойств нажать кнопку «Другие». Далее включить выключатель «Шифровать содержимое для защиты данных», нажать кнопку «Применить» и в окне подтверждения изменения атрибутов нажать кнопку «Ok».

При шифровании данных на компьютере необходимо предусмотреть способ восстановления этих данных на случай, если что-то произойдет с ключом шифрования. Если ключ шифрования потерян или поврежден и способ восстановления данных отсутствует, данные будут потеряны. Данные будут также потеряны, если повреждена или утеряна смарт-карта, на которой хранился ключ шифрования. Чтобы гарантировать постоянный доступ к зашифрованным данным, нужно сделать резервные копии сертификата и ключа шифрования.

**Вывод**

В ходе выполнения практической работы были освоены средства администрирования системы Windows и изучены политики безопасности и обновления системы.

# **Лабораторная работа №2**

**Создание резервных копий базы данных, восстановление базы данных**

**Цель работы:** ознакомиться с основными конструкциями SQL, технологиями среды MS SQL Server Management, объектами SMO (среды MS Visual Studio) для резервного копирования и восстановления БД

**Задание №1.** Необходимо создать резервные копии базы данных «МММ» с использованием полного резервного копирования, разностного резервного копирования и резервного копирования журнала транзакций.

**Ход работы:**

1. Запустим SQL Server Management Studio (SSMS), подключимся к своему экземпляру SQL .
2. Создадим папку (Рис. 19)

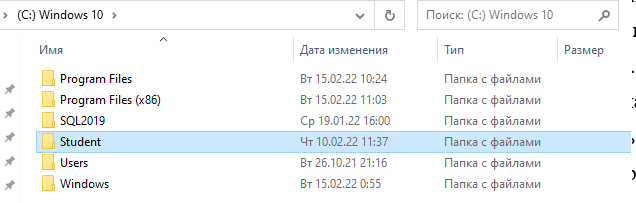


Рисунок 19 Созданная папка

В MS SQL создадим БД (Рис. 20)

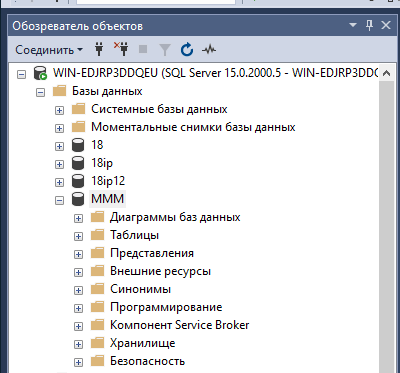


Рисунок 20 БД

1. Откроем окно нового запроса. Изменим контекст на базу данных master (Рис. 21). Наберем и исполним следующую команду, чтобы создать полную резервную копию базы данных:

BACKUP DATABASE МММ TO DISK = 'C:\........TEST\AW.ВАК’ (Рис. 22)

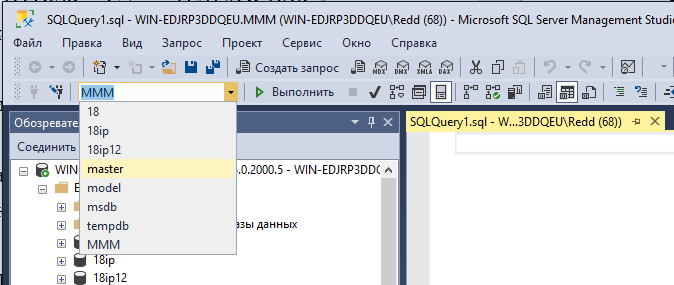


Рисунок 21 Создание запроса

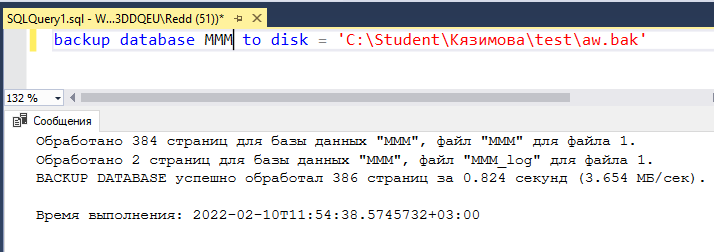


Рисунок 22 Выполнение запроса

1. Внесем изменение в таблицу «Модель» базы данных МММ (Рис.23)

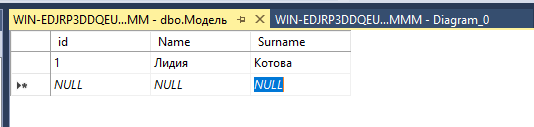


Рисунок 23 Добавленная строка

1. Откроем окно нового запроса и наберем следующую команду, чтобы создать резервную копию журнала транзакций и сохранить только что внесенное изменение (Рис.24):

BACKUP LOG МММ TO DISK = ‘С:\.......TEST\AW1.TRN'

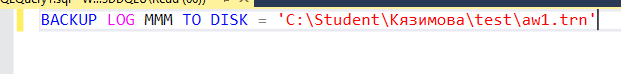


Рисунок 24 Созданный запрос

1. Внесем еще одно изменение в таблицу «Модель». (Рис.25)

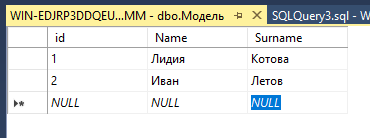


Рисунок 25 Добавление новой записи

1. Откроем окно нового запроса и наберем следующую команду, чтобы создать разностную резервную копию базы данных (Рис.26):

BACKUP DATABASE MMM TO DISK = ‘C:\.....\TEST\AWDIFF1.ВАК' WITH DIFFERENTIAL

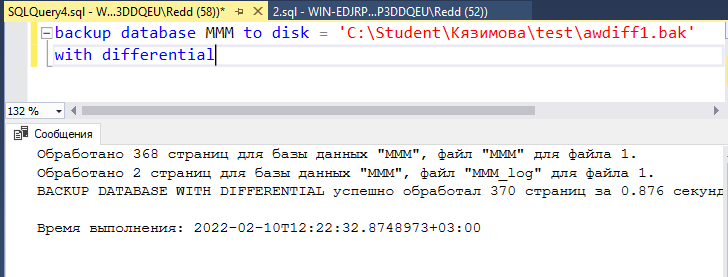


Рисунок 26 Новый запрос

1. В папке появился новый файл бэкапа (Рис. 27)

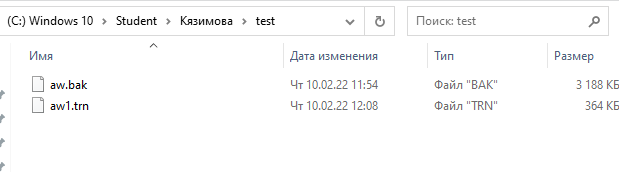


Рисунок 27 Созданные файлы

Внесите еще одно изменение в таблицу «Модель». (Рис.28)

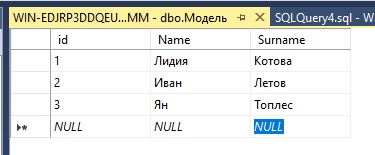


Рисунок 28 Добавление новой записи

1. Откроем окно нового запроса наберем и исполним следующую команду, чтобы создать полную резервную копию базы данных в указанном месте на диске(Рис.29):

BACKUP LOG MMM TO DISK = ‘С:\....TEST\AW2.TRN'

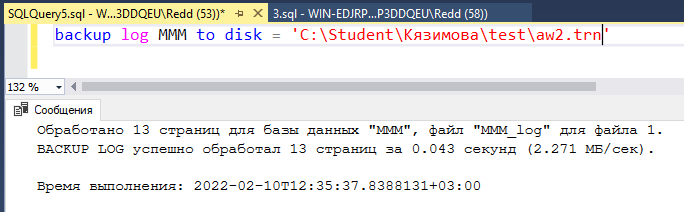


Рисунок 29 Новый запрос

В результате запроса появился новый файл полной резервной копии в папке (Рис.30)

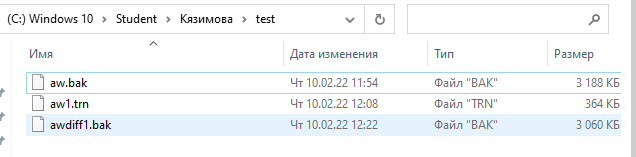


Рисунок 30 резервные копии

**Задание №2.** Необходимо провести восстановление базы данных «МММ» из сделанных в задании №1 резервных копий.

**Ход работы:**

1. Подключимся к базе МММ (Рис.) Выполним восстановление БД из первой полной резервной копии (C:\...TEST\AW.BAK) средствами оболочки SSMS. Для этого выполним:

В обозревателе объектов вызовем контекстное меню на БД и выберем задачу восстановления базы данных (Рис. 31).

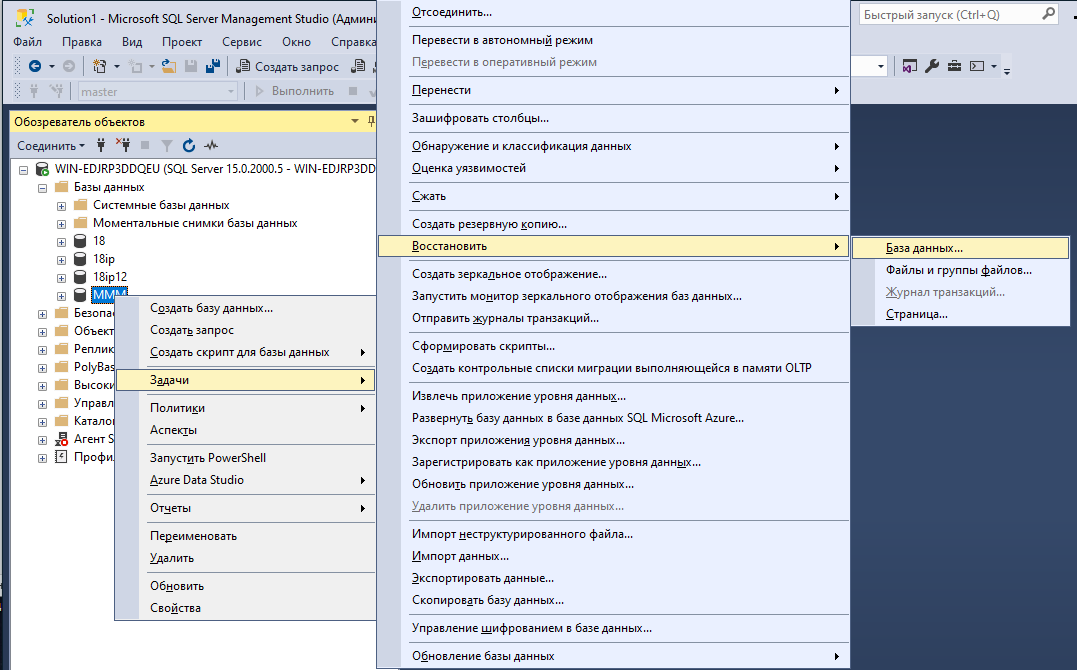


Рисунок 31 Контекстное меню

В открывшемся окне зададим следующие параметры восстановления: на закладке «Общие» необходимо выбрать базу данных для восстановления (Рис. 31).

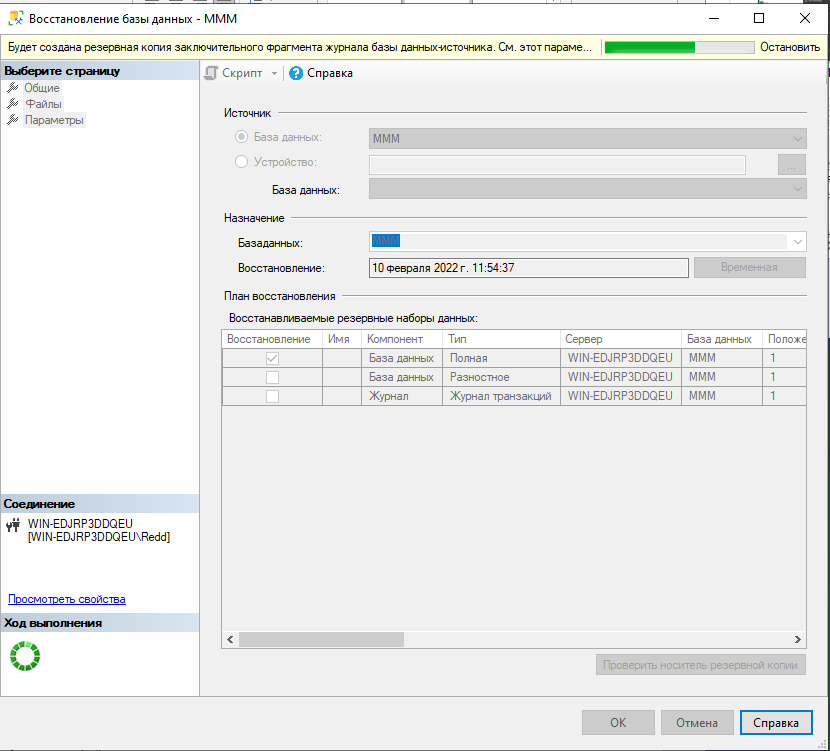


Рисунок 32 Восстановление БД

1. Запустим восстановление (Рис. 33)

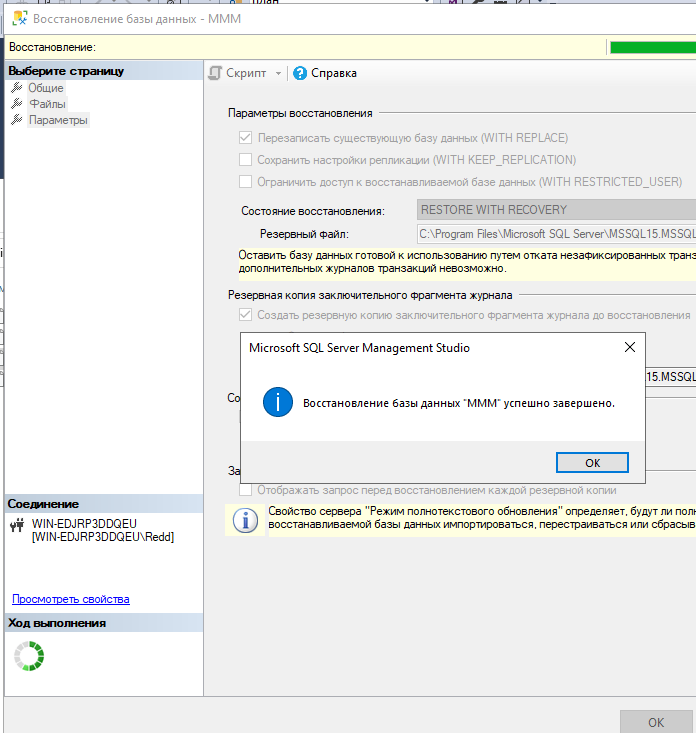


Рисунок 33 Восстановление базы

* После восстановления БД, откроем таблицу «Модель» и убедимся, что она не содержит всех добавлений, вносимых ранее в процессе выполнения упражнения, так как восстановление происходило из первой резервной копии (без изменений) (Рис. 34)

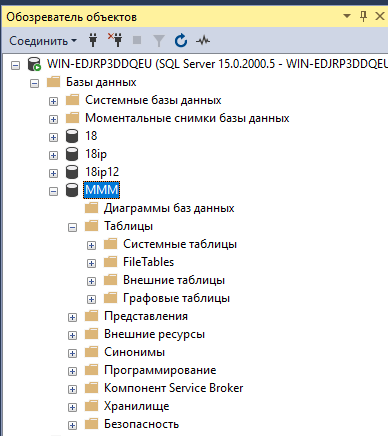


Рисунок 34 Пустая БД

**Задание №3.** Необходимо организовывать со стороны клиентского приложения, созданного в Visual Studio удаленное администрирование БД (резервное копирование).

**Ход работы:**

1. В Visual Studio создадим новый проект MS Visual Studio (Рис. 35-36).

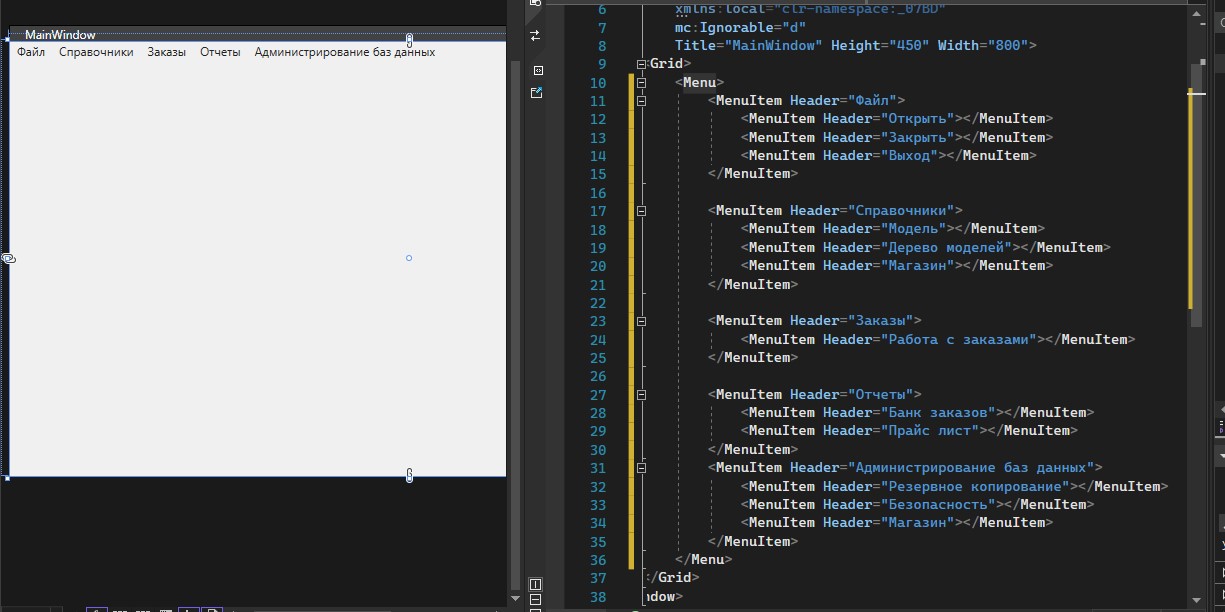


Рисунок 35 Xaml разметка для элемента Menu

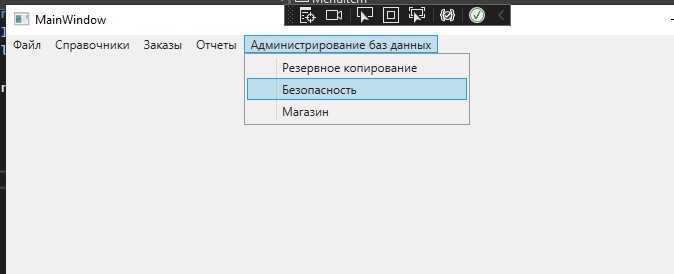


Рисунок 36 Окно работающей программы

1. Добавим новую форму в проект (Рис. 37).

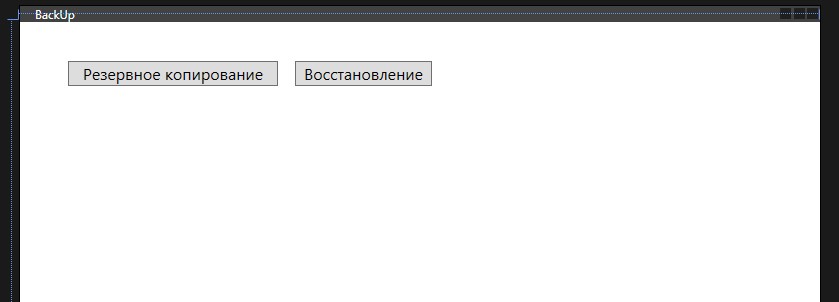


Рисунок 37 Новое окно

1. Соединяем БД с приложением (Рис. 38).

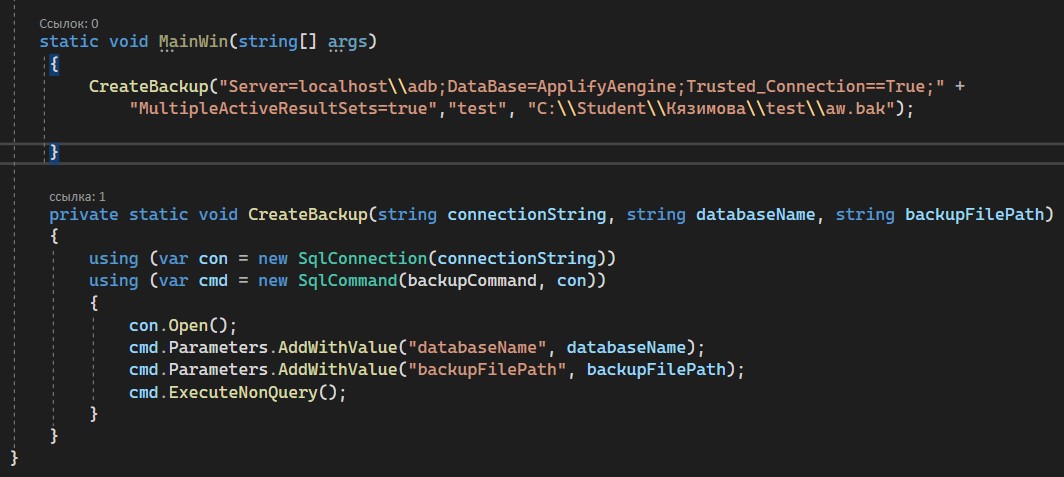


Рисунок 38 Фрагмент кода

**Задание №4.** Ответьте на вопросы и представьте результаты преподавателю.

1. Вы выполняете разностное резервное копирование базы длимых AdveniurtWorks каж­дые четыре часа, начиная с 04:00. полная резервная копия создается в полночь. Ка­кие данные будут содержаться в разностной резервной копии, сделанной в полдень?

А Страницы данных, измененные после полуночи.

B. Экстенты, измененные после полуночи.

C. Страницы данных, измененные после 08:00

D. Экстенты. измененные после 08:00.

1. Вы выполняете полное резервное копирование 6азы данных Adventure Wortks, которое завершается в полночь. Разностное резервное копирование выполняется по распи­санию каждые четыре часа, начиная с 04:00. Резервное копирование журнала транзакций происходит по расписанию каждые пять минут. Какую информацию будет содержать резервная копия журнала транзакций, созданная в 09:15?

А. Все транзакции, начатые после 09:10.

B. Транзакции, завершенные после 09:10.

C. Страницы, измененные после 09:10.

D. Экстенты, измененные после 09:10

**Вывод**

В ходе выполнения практической работы были изучены конструкции SQL для создания резервных копий, объекты SMO (среды MS Visual Studio) для резервного копирования и восстановления БД.

# **Лабораторная работа №3**

**Восстановление носителей информации, восстановление удаленных файлов**

**Цель работы:** научиться осуществлять восстановление жесткого диска после сбоев.

**Выполнение работы**

Изучить ПО по восстановлению носителей информации, удаленных файлов и ответить на вопросы:

* 1. В чем назначение программы Partition Magic?

Power Quest @ Partition Magic – это утилита, которая позволяет быстро и легко создавать, удалять, объединять или преобразовывать файловые системы и разделы на жестком диске, не уничтожая существующие данные.

* 1. Какие действия необходимо выполнить перед началом работы с программой Partition Magic?

Прежде чем начать работу с программой Partition Magic обязательно нужно выполнить следующие рекомендации:

* Установить самые последние обновления для операционных систем Windows 95/98/Me/NT Workstation/2000/XP Professional. Удостовериться, что самые последние исправления для операционных систем Windows 95/98/Me/NT Workstation/2000/XP Professional установлены и запущены.
* Сделайте копию вашего жесткого диска
* Создать загрузочный диск Windows.
* Запустить опцию проверки ошибок на диске.
* Закрыть все запущенные приложения. Нельзя запускать Partition Magic вместе с другими приложениями, включая вирусные сканеры
* Использовать UPS (Источник бесперебойного питания
* Совет. Из-за несовместимости аппаратной и системной конфигурации одного компьютера с другим, не рекомендуется переносить с одного на другой компьютер, жесткий диск, разделенный с помощью программы Partition Magic, во избежание потери данных.
  1. Как осуществляется проверка целостности жесткого диска с помощью программы Partition Magic?

Программа Partition Magic проверяет целостность диска сложной системой анализа и проверки достоверности, которая скрыто начинает свою работу, каждый раз, когда запускается программа или завершается операция.

* 1. Назначение программы Paragon Partition Manager?

Функции программы во многом совпадают с возможностями предыдущей программы - любые разделы можно создавать, удалять, форматировать, перемещать, конвертировать между файловыми системами, объединять и изменять их атрибуты, уменьшать или увеличивать размер разделов - и все это без потери данных.

5. Перечислите известные вам программы по обслуживанию жестких дисков в процессе их эксплуатации и определите их назначение.

Victoria HDD – программа для диагностики жесткого диска, а также восстановления данных на нем. Она предназначается для продвинутых пользователей, самостоятельно занимающихся ремонтом компьютера, а также IT-специалистов. С помощью программы Victoria можно оценить работоспособность HDD, решить проблему с битыми секторами.

Возможности Victoria HDD:

* измерение производительности диска;
* форматирование HDD;
* предоставление подробных данных о винчестере;
* скрытие поврежденных секторов;
* устранение сбоев в работе жесткого диска;
* управление акустическим шумом.

Большим плюсом Victoria HDD является то, что она имеет небольшой размер и не требует инсталляции. В отличие от остальных программ для диагностики жестких дисков и восстановления данных, Victoria умеет контролировать температуру HDD, тестировать поверхность в DMA и PIO, измерять скорость вращения вала на новых винчестерах. Victoria HDD работает не только с обычными ПК, но и с ноутбуками.

Запускаем программу (Рис. 39)

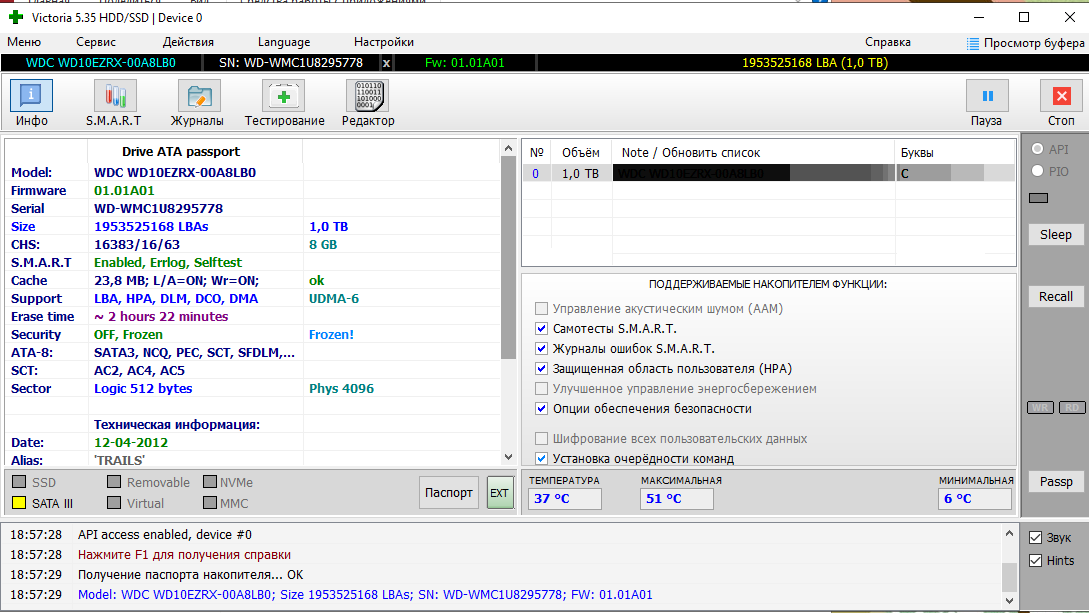


Рисунок 39 Запущенная программа

Далее переходим в «**SMART**» и нажимаем кнопку «**Получить атрибуты SMART**» (Get Smart). В таблице будут отображены 242 параметра вашего устройства. Они записываются с первого дня использования носителя, и программа Victoria считывает их из системы (Рис. 40).

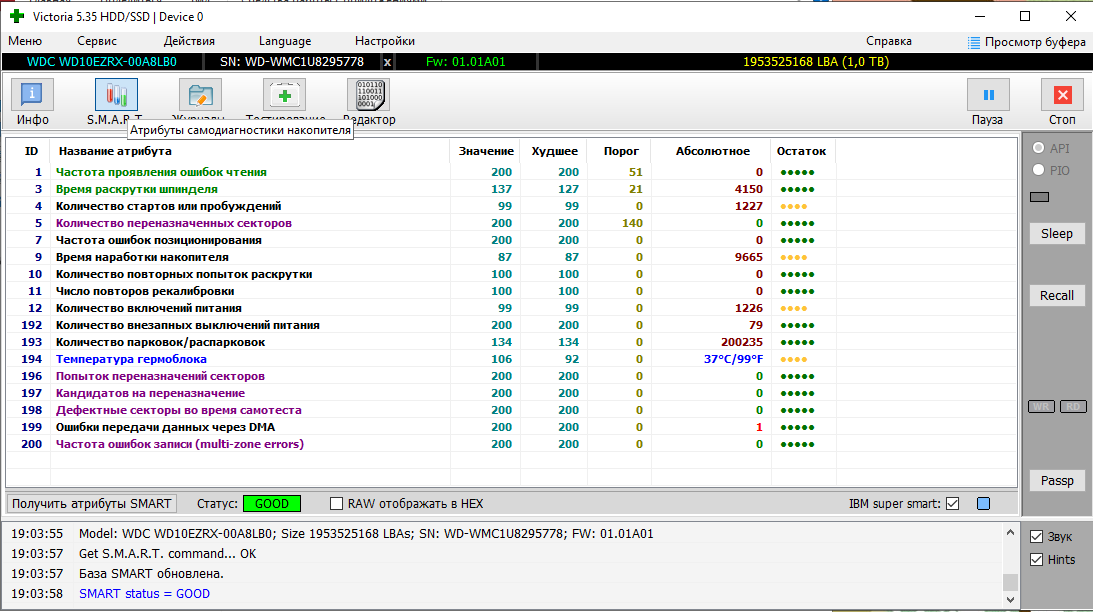


Рисунок 40 SMART

Если винчестер исправен, то переходим во вкладку «Тестирование» (Test). При первом использовании не рекомендуется изменять установленные по умолчанию настройки. В этом случае будет проведена обычная диагностика жесткого диска, без применения каких-либо действий к поврежденным секторам. Убедитесь, что активирован режим «Игнор» (Ignore) и нажмите на кнопку «Scan» (Рис. 41).

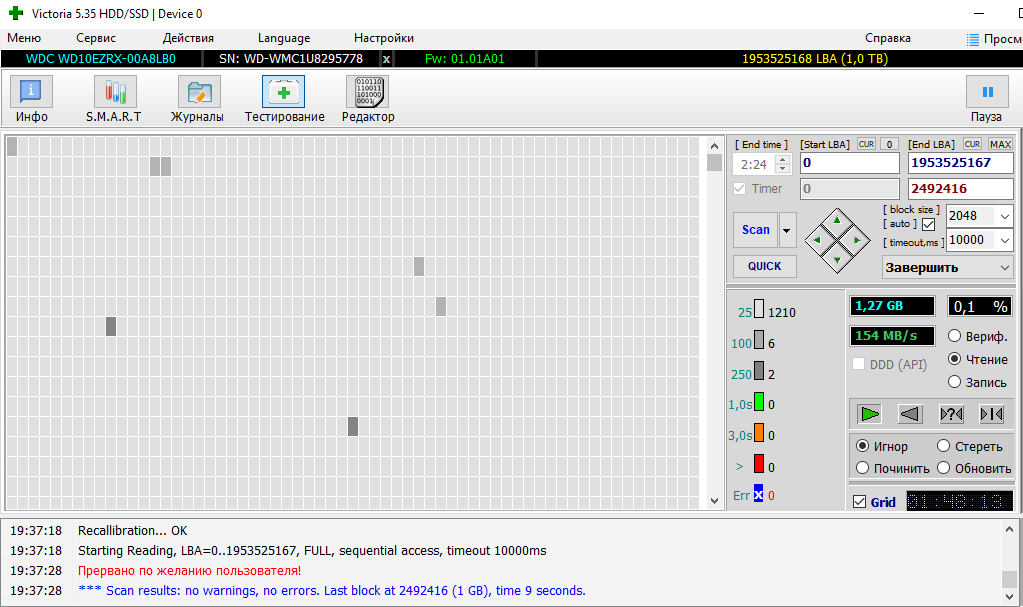


Рисунок 41 Вкладка тестирования

6. Опишите последовательность восстановления удаленной информации, если:

1. файл удален в корзину.

На рабочем столе либо в меню пуск нужно найти файл «Корзина»



Кликнув и открыв его, ищем удаленный файл. Щелкнув правой кнопкой мыши и выберите «Восстановить».

1. файл удален в корзину и затем очистили корзину.

Удаленные файлы из корзины, можно восстановить с помощью программного обеспечения для восстановления данных.

Windows обозначает пространство на жестком диске, которое было занято удаленными файлами, как доступное для использования, но файл не записывается до тех пор, пока это пространство не потребуется. Запись потерянного файла не будет отображаться на компьютере или иметь доступ с помощью командной строки DIR, но содержимое файла по-прежнему физически существует на жестком диске. Программное обеспечение для восстановления данных способно сканировать жесткий диск для поиска подобных файлов, позволяя извлекать и сохранять их.

**Вывод**

В ходе выполнения практической работы были приобретены навыки по восстановлению жесткого диска после сбоев.

# **Лабораторная работа №4**

**Мониторинг активности портов, блокирование портов**

**Цель работы:** формирование умений и навыков блокировки и разблокировки портов подключения устройств

**Выполнение работы**

Изучить материал по мониторингу активности и блокированию портов и ответить на вопросы:

1. Какие виды мониторинга рабочих операций пользователя существуют?

* Мониторинг рабочего стола
* Мониторинг процессов
* Мониторинг доступа к USB.
* Мониторинг интернет активности
* Мониторинг локальных действий

1. Дайте характеристику современным программным средств мониторинга действий пользователей. Какое программное средство вы порекомендовали бы нашей организации? Почему?

Основными целями контроля являются: обеспечение информационной безопасности, выявление случаев некорректного, непрофессионального или нецелевого использования ресурсов, оценка характеристик функционирования корпоративной сети и параметров использования ресурсов.

Основной задачей обеспечения информационной безопасности является «раннее обнаружение» внутренних вторжений, т.е. выявление действий пользователей, которые могут предшествовать внутренним вторжениям. Чем крупнее организация, тем актуальней является для нее проблема предотвращения внутренних вторжений, в частности кражи информации, так как именно кража является конечной целью большинства внутренних вторжений. Связано это с тем, что в больших организациях затрудняется контроль над обращением информации и существенно возрастает цена ее утечки. Указанные обстоятельства определяют высокий уровень озабоченности данной проблемой со стороны крупного бизнеса и правительственных организаций. Решение данной проблемы заключается в применении «жесткой» политики информационной безопасности в организации и использовании средств мониторинга действий пользователей.

При помощи Spector 360 вы можете сгенерировать высококачественные отчеты для руководства, которые могут регулярно распечатываться или рассылаться по почте.

Spector 360 разработан для коммерческих, образовательных и правительственных организаций, использующих сети на платформе Windows.

Определенно, Spector 360 незаменим в крупных организациях, где решаются задачи оперативного мониторинга огромного количества рабочих станции.

1. Какие уязвимости ОС Windows были устранены в данной работе и какими путями?

Был установлен пароль для входа в систему и поле пользователя пустое, для усложнения входа посторонним лица

1. Как узнать закрытые порты? Как открыть нужный порт?

С помощью PowerShell можно проверить открытые порты в Windows

Чтобы вывести список открытых портов, используйте опцию -State со значением Listen: Get-NetTcpConnection -State Listen

Открыть порт можно через Мастера создания правила для нового входящего подключения в Брандмаузере Windows (Рис.42-44)

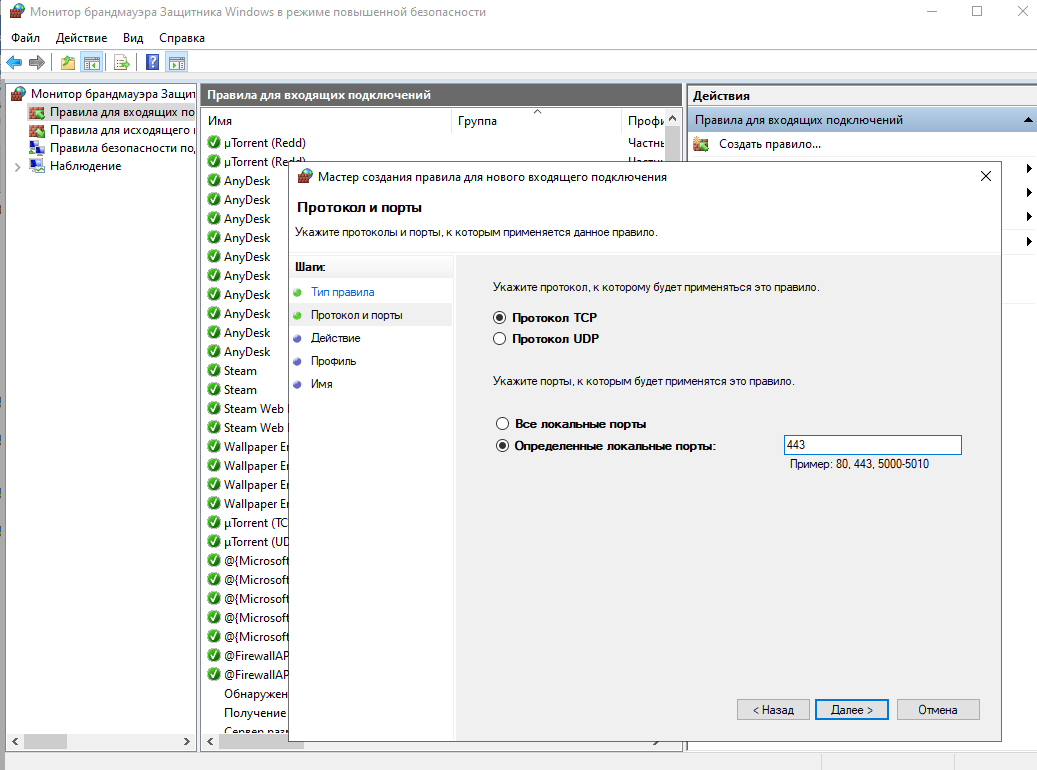


Рисунок 42 открытие портов

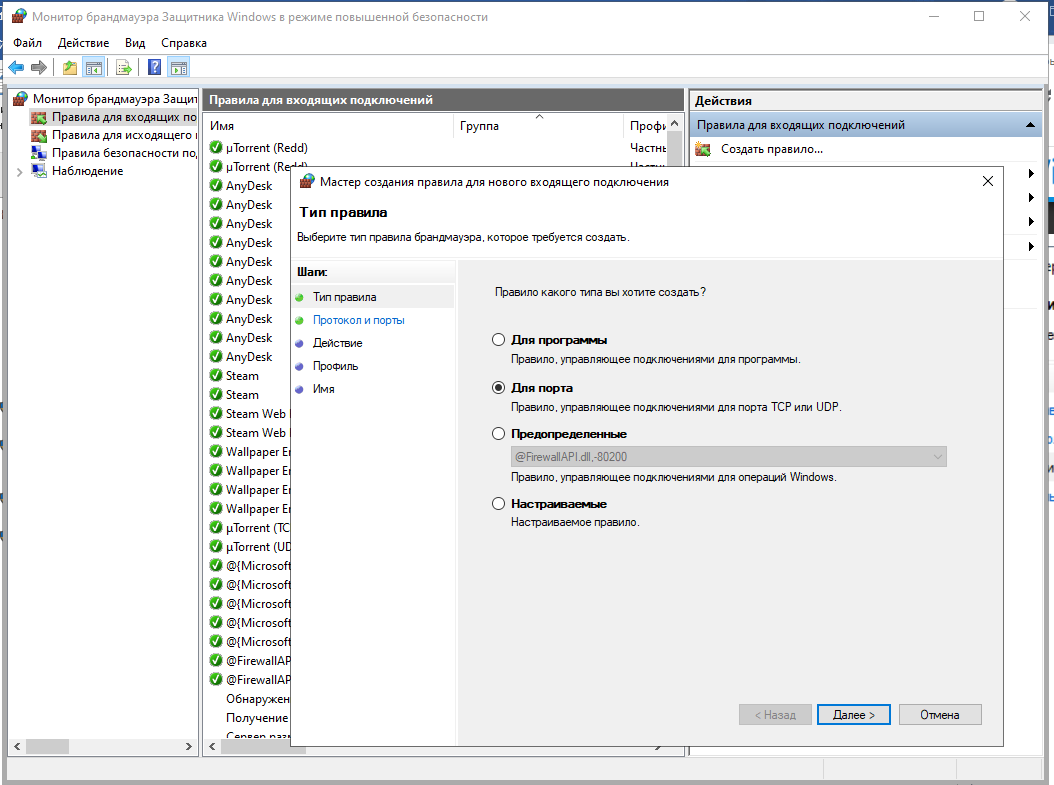


Рисунок 43 Открытие портов

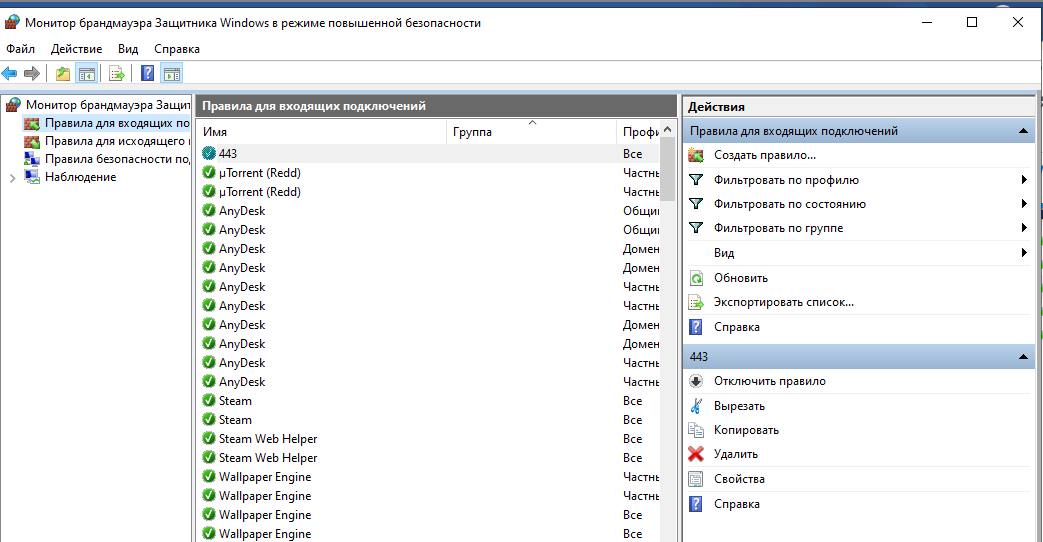


Рисунок 44 открытый порт

1. Для чего используется программа NetStat Agent? Nmap? TCPView?

NetStat Agent — полезный набор инструментов для мониторинга Интернет соединений и диагностики сети. Программа позволяет отслеживать TCP и UDP соединения на ПК, закрывать нежелательные соединения, завершать процессы, обновлять и освобождать DHCP настройки адаптера, просматривать сетевую статистику для адаптеров и TCP/IP протоколов, а также строить графики для команд Ping иTraceRoute

Nmap — популярный сканер портов, который обследует сеть и проводит аудит защиты. Cканером портов nmap можно определить открытые порты компьютера, а для безопасности сети пользователям рекомендуется закрыть доступ к этим портам с помощью брандмауэра

TCPView — показывает все процессы, использующие Интернет-соединения. Запустив TCPView, можно узнать, какой порт открыт и какое приложение его использует, а при необходимости и немедленно разорвать соединение.

**Вывод:**

В результате выполнения практической работы были приобретены навыки блокировки и разблокировки портов подключения устройств

# **Лабораторная работа №5**

**Проверка наличия и сроков действия сертификатов**

**Цель работы:** изучить структуру типовой политики информационной безопасности и научиться составлять частную политику информационной безопасности.

**Практическое задание**

Написать политику безопасности для выбранного предприятия.

**Контрольные вопросы**

1. Дайте определение политики информационно безопасности. Из каких основных документов состоит политика информационной безопасности?

Политика безопасности (информации в организации) (Organizational security policy) – это совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

1. Назовите общее содержание политики разрешения доступа к технологическим ресурсам.

Подразделения, службы, отделы, чья деятельность связана с использованием ИТ ресурсов компании, выдачей разрешений доступа к этим ресурсам.

Описывает процедуры, которые должны быть выполнены всеми участниками процесса разрешения доступа к ИТ ресурсам компании.

1. Что включает в себя политика пользования электронной почтой?

Политика пользования электронной почтой предоставляет персоналу разрешенные правила пользования ресурсами электронной почты (e-mail) компании. Политика охватывает e-mail, приходящий или отправляемый через все принадлежащие компании персональные компьютеры, сервера, ноутбуки, терминалы, карманные переносные компьютеры, сотовые телефоны и любые другие ресурсы, способные посылать или принимать e-mail по протоколам SMTP, POP3, IMAP.

1. Назовите общее содержание антивирусная политика.

Антивирусная политикаприменяется ко всем компьютерам сети компании, каталогам общего пользования, к которым относятся настольные компьютеры, ноутбуки, file/ftp/proxy серверы, терминалы, любое сетевое оборудование, генерирующее трафик. Источниками вирусов могут быть email, Интернет-сайты со скрытыми вредоносными активными элементами, носители информации (флоппи-диски, CD-диски, flash-диски и пр.), открытые для общего доступа папки и файлы и т.д.

1. Назовите общее содержание политика подготовки, обмена и хранения документов.

Политика подготовки, обмена и хранения документов охватывает все подразделения, службы, отделы, чья деятельность связана с подготовкой, копированием, хранением, обменом документами, информацией, данными с использованием информационно-технологических ресурсов компании.

1. Что включает в себя политика информационно-технической поддержки?

Политика информационно-технической поддержки охватывает и описывает все уровни поддержки персонала, выполняемые по заявкам через службу HelpDesk - единой точки контакта с персоналом. Выделяется уровень самопомощи и три уровня поддержки:

1. Самопомощь – когда конечный пользователь самостоятельно выполняет действия по устранению проблемы, не нарушающие безопасности сети и других пользователей, такие как перезапуск приложения или компьютера, проверка подключения все кабелей и сетевых ресурсов, антивирусное сканирование и пр.
2. HelpDesk 1-го уровня – выполняет поддержку заявок общего профиля: решение оперативных проблем персонала, задач доступа и безопасности; первичная диагностика сложных проблем, причин не работы программ; устранение проблемы или переадресация по сложности на следующий уровень. 3.
3. HelpDesk 2-го уровня – выполняет поддержку заявок по работе приложений и систем: − углубленные, содержательные консультации и обучение; поиск решений имеющимися средствами (без вмешательства в логику приложений), помощь в выборке и восстановлении данных и документов , в бизнес анализе, (раз)доработка отчетных форм; обслуживание контента и администрирование Интернет-сайта компании; формулирование задач для изменяющихся бизнес-процессов, составление нормативных документов.
4. HelpDesk 3-го уровня:

* выполняет поддержку заявок по развитию приложений, систем, инфраструктуры:
* исследования, доработка, лабораторное тестирование, выработка решений;
* работа с поставщиками приложений и разработчиками; планирование и развертывание новых приложений, реорганизация процессов и пр.

1. Что включает в себя политика серверной безопасности?

Политика серверной безопасности применяется к серверному оборудованию, принадлежащему и используемому в компании, и к серверам, зарегистрированным в принадлежащих компании внутренних сетевых доменах.

Все внутренние сервера, развернутые в компании, должны быть в ведении ИТ подразделения, а именно группы системного администрирования (СА). Группа СА должна установить и поддерживать правила разрешенных серверных конфигураций, основанных на потребностях бизнеса и утвержденных службой ИБ. Группа СА должна следить за соответствием конфигурации и проводить политику ограничения, наложенную на сетевое окружение.

**Вывод**

В ходе выполнения практической работы была изучена структура типовой политики информационной безопасности и научились составлять частную политику информационной безопасности.

# **Лабораторная работа №6-7**

**Разработка политики безопасности корпоративной сети.**

**Получение сертификата**

**Цель работы:** изучение видов сертификации объектов информатизации.

Откроем сайт погоды. В строке поиска, перед ссылкой появился замочек. Кликнув по нему появиться окошко указывающее на безопасность (Рис. 45)

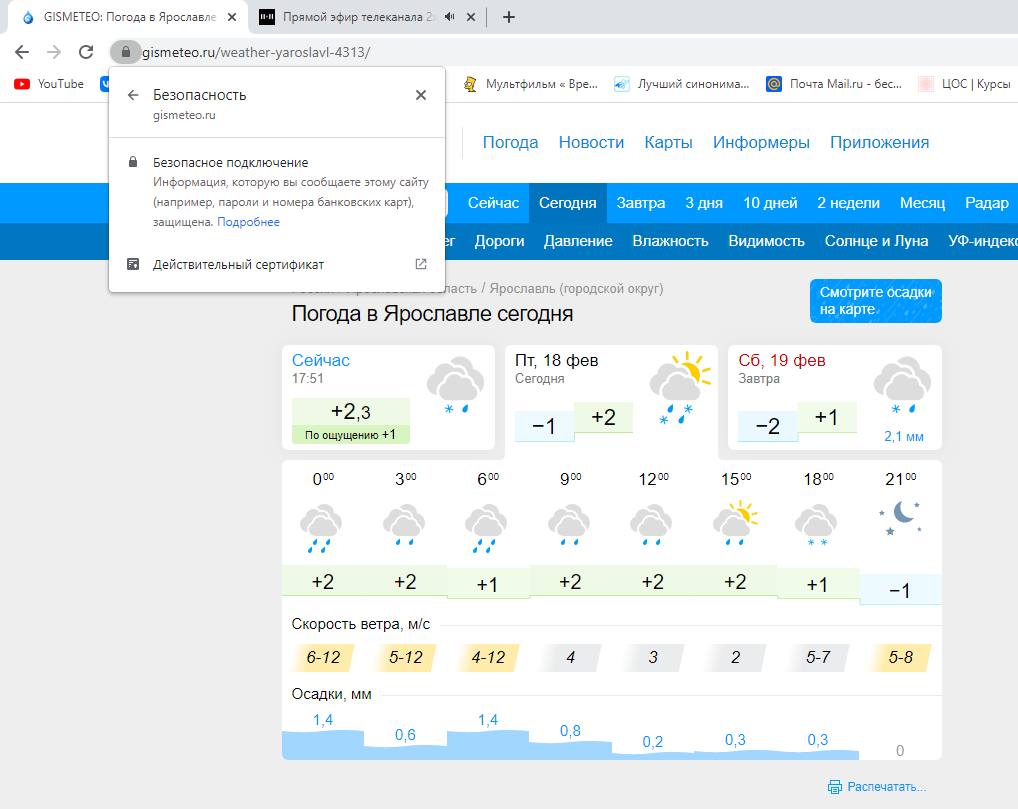


Рисунок 45 Сайт с сертификатом

Нажав на Подробнее появилось окно сертификата сайта с информацией (Рис.46)

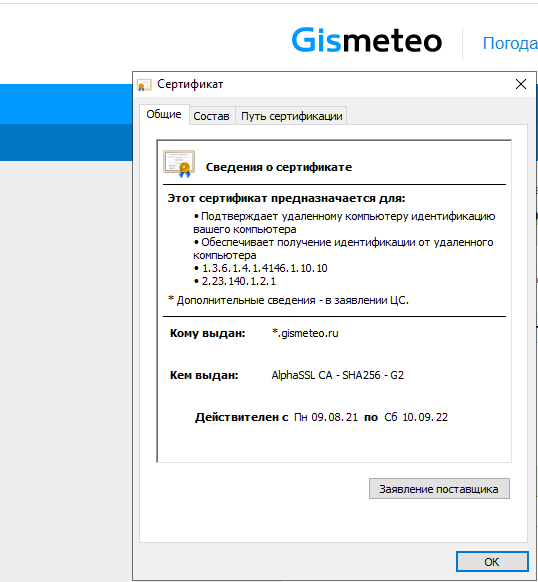


Рисунок 46 Сертификат сайта

Перейдя по вкладкам можно узнать о действии сертификата (Рис.)

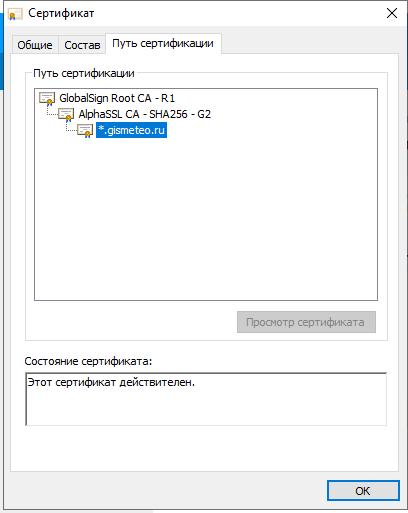


Рисунок 47 Путь сертификации

**Выполнение работы**

* + 1. Укажите объекты информатизации, подлежащие обязательной сертификации.

Указанным документом к продукции, подлежащей обязательной сертификации в рассматриваемом направлении, отнесены следующие средства информатизации:

* + - вычислительные машины и комплексы;
    - персональные ЭВМ;
    - устройства внешней памяти, ввода-вывода и отображения информации;
  + устройства подготовки и телеобработки данных.
    1. Какие требования безопасности, предъявляются к ПЭВМ?

К работе с персональными электронно-вычислительными машинами (ПЭВМ) допускаются лица, обученные работе на них, имеющие I группу по электробезопасности, прошедшие вводный инструктаж (при приеме на работу) и первичный инструктаж по охране труда на рабочем месте

* + 1. На какой срок выдаются сертификаты безопасности?

Срок действия сертификата безопасности устанавливает орган по сертификации с учетом результатов сертификации работ по охране труда в организациях, а также с учетом даты завершения организацией аттестации рабочих мест по условиям труда (Постановление Минтруда России от 24 апреля 2002 г. N 28), но не более пяти лет

* + 1. Как можно проверить наличие и действие сертификата безопасности?

Онлайн-сервисы проверки SSL— это простой и понятный инструмент, который быстро определяет, можно ли доверять веб-ресурсу. С его помощью вы узнаете: установлен или нет на сайте сертификат безопасности, какие дополнительные имена защищает сертификат, а также дату начала и окончания действия SSL.

* + 1. По каким причинам может быть приостановлено действие сертификата безопасности?
    2. Назначение и получение SSL-сертификата. Опишите схему действия SSL.

Наличие статуса «приостановлен» (круг в виде оранжевого оттенка) – отображает, что документ на текущий момент приостановлен по каким- либо причинам. Возможная причина этого и дата приостановки действия документа будет указана внутри описания сертификата. Допускается вероятность того, что после устранения причин, действие документа будет возобновлено в полном объеме. Статус «аннулирован» (круг в виде красного оттенка) – отображает факт того, что данный документ является недействительным и восстановлению не подлежит. Сама причина и дата аннуляции указываются внутри описания этого сертификата

* + 1. Как определить использует сайт SSL-сертификаты?

Адресная строка становится зелёной, показывая, что на веб-сайте используется Extended Validation SSL.

Жёлтый замок с закрытой дужкой означает, что соединение между сервером и браузером защищено. Если замок открыт или отсутствует, то соединение не использует SSL.

**Вывод**

В ходе выполнения практической работы были изучены основные виды сертификации объектов информатизации, используемые стандарты и методы.