СОДЕРЖАНИЕ

[1 ЦЕЛИ И ЗАДАЧИ УЧЕБНОЙ ПРАКТИКИ. ИЗУЧЕНИЕ ИНСТРУКЦИЯ ПО ТЕХНИКЕ БЕЗОПАСНОСТИ ПРИ РАБОТЕ НА ПК. 5](#_Toc105831986)

[2 ОСУЩЕСТВЛЕНИЕ АДМИНИСТРИРОВАНИЕ БАЗ ДАННЫХ В РАМКАХ СВОЕЙ КОМПЕТЕНЦИИ 12](#_Toc105831987)

[2.1 Создание резервных копий баз данных. Восстановление базы данных. 12](#_Toc105831988)

[2.2 Мониторинг активности портов. Блокирование портов. 14](#_Toc105831989)

[3 ПРОВЕДЕНИЕ АУДИТ СИСТЕМ БЕЗОПАСНОСТИ БАЗ ДАННЫХ И СЕРВЕРОВ, С ИСПОЛЬЗОВАНИЕМ РЕГЛАМЕНТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ. 17](#_Toc105831990)

[3.1 Проверка наличия и сроков действия сертификатов 17](#_Toc105831991)

[3.2 Планирование автоматизированных систем для обслуживания баз данных. Планирование автоматизированных систем для обслуживания серверов. 18](#_Toc105831992)

1 ЦЕЛИ И ЗАДАЧИ УЧЕБНОЙ ПРАКТИКИ. ИЗУЧЕНИЕ ИНСТРУКЦИЯ ПО ТЕХНИКЕ БЕЗОПАСНОСТИ ПРИ РАБОТЕ НА ПК.

Цели, задачи и содержание учебной практики определяются требованиями к результатам практики, установленными ФГОС в части общих, и профессиональных компетенций.

Целью учебной практики является формирование у студента практических профессиональных умений, приобретение первоначального практического опыта, реализуемых в рамках модуля ОПОП СПО ПМ.07 по виду профессиональной деятельности код 09.02.07 для последующего освоения ими общих и профессиональных компетенций по специальности «Информационные системы и программирование».

Задачами учебной практики выступают:

- систематизация, конкретизация, обобщение и закрепление теоретических знаний на основе изучения опыта работы конкретной организации;

- приобретение навыков и умений в области профессиональной деятельности;

- овладение необходимым набором общих и профессиональных компетенций.

Учебная практика направлена на развитие практических умений и формирование у обучающихся первоначального практического опыта. Практика реализуется в рамках профессионального модуля для последующего освоения обучающимися профессиональных компетенций и развития общих компетенций по выбранной специальности.

С целью овладения указанным видом деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения учебной практики должен:

иметь первоначальный практический опыт:

- в участии в соадминистрировании серверов;

- разработке политики безопасности SQL сервера, базы данных и отдельных объектов базы данных;

- применении законодательства Российской Федерации в области сертификации программных средств информационных технологий;

уметь:

- проектировать и создавать базы данных;

- выполнять запросы по обработке данных на языке SQL;

- осуществлять основные функции по администрированию баз данных; разрабатывать политику безопасности SQL сервера, базы данных и отдельных объектов базы данных;

- владеть технологиями проведения сертификации программного средства.

Инструктаж по охране труда проводится для ознакомления сотрудников компании с правилами безопасности на рабочем месте. В соответствии со ст. 212 Трудового кодекса РФ работодатель должен организовать подготовку сотрудников для обеспечения безопасности выполнения работ.

Вводный инструктаж по охране труда проводится со всеми вновь принимаемыми на работу независимо от их образования, стажа работы по данной профессии или должности, с временными работниками, командированными, учащимися и студентами, прибывшими на производствен­ное обучение или практику.

Вводный инструктаж на предприятиях проводит инженер по охране труда или лицо, на которое приказом работодателя возложены эти обязанности. Для проведения вводного инструктажа разрабатывают­ся программа и инструкция, которые утверждаются работодателем.

О проведении вводного инструктажа делается запись в журнале регистрации вводного инструктажа с обязательной подписью инструктируемого и инструктирующего, а также в документы о приеме на работу.

От последующих инструктажей на рабочем месте освобождаются лица, не связанные с обслуживанием, испытанием, наладкой оборудования и инструментом. Составляется Перечень профессий и должностей работников, освобожденных от инструктажей на рабочем месте, который утверждается работодателем.

Нормативная база

Признаком того, что сотрудникам необходимо соблюдать правила техники безопасности при использовании компьютера, становится то, что эти вопросы зафиксированы и в действующем законодательстве. Основными нормативными документами, которые содержат обязательные требования, можно считать:

* Трудовой кодекс;
* санитарно-гигиенические нормы и правила СанПиН 2.2.2/2.4.1340-03, утвержденные постановлением Главного государственного санврача от 13 июня 2003 года N 118;
* межгосударственный стандарт ГОСТ 12.0.003-2015, который содержит список основных вредных и опасных производственные факторов и их классифицирующие признаки;
* типовая инструкция ТОИ Р-45-084-01, в которой содержатся основные правила для работников, использующих компьютер;
* другие нормативные документы.

Требования перечисленных правовых актов, в которых содержатся общие правила защиты персонала при выполнении трудовых обязанностей и техника безопасности во время работы за компьютером, обязательны к исполнению всеми работниками этой категории.

Вредоносные факторы

Использование персонального компьютера совсем не так безопасно, как можно подумать. Это убедительно подтверждается информацией, содержащейся в стандарте ГОСТ 12.0.003-2015, описывающем основные вредные и опасные факторы такого трудового процесса. В их список входят:

* высокая температура, характерная для отдельных элементов компьютерной техники и создающая общий повышенный температурный фон в рабочем помещении;
* высокая степень монотонности рабочего процесса;
* значительный уровень зрительный нагрузок, испытываемых работником;
* риск поражения статическим электричеством при случайном контакте с отдельными элементами техники;
* недостаточная освещенность рабочей зоны;
* повышенный уровень напряженности электрического и магнитного полей, генерируемых работающей техникой;
* высокий уровень блесткости и контрастности рабочего экрана, негативно влияющий на зрение работника в длительной перспективе;
* другие факторы.

1. Гигиенические требования

В связи с наличием воздействия большого списка вредоносных факторов на работника, требования техники безопасности при работе с компьютером охватывают не только сам процесс труда, но и сопровождающие его обстоятельства, которые также влияют на работоспособность и сохранность здоровья сотрудника на длинных временных горизонтах. Соответствующие правила организации рабочего процесса приведены в СанПиН 2.2.2/2.4.1340-03. Они включают ряд нормативов, которые касаются следующих моментов:

* общие правила организации работы с использованием компьютерной и офисной техники;
* требования к персональному компьютеру, используемому для постоянной работы сотрудника;
* требования к помещениям, в которых выполняется работа с применением офисной техники;
* требования к микроклимату для соответствующих рабочих мест, включая содержание в воздухе рабочей зоны аэроионов и вредных химикатов;
* допустимый уровень шума, генерируемого рабочим оборудованием;
* правила организации освещения рабочей зоны;
* разрешенные нормативы в отношении параметров электромагнитных полей на рабочих местах;
* техника безопасности при пользовании компьютером, которая связана с организацией рабочих мест сотрудников;
* медицинский контроль за здоровьем персонала;
* порядок организации государственного санитарно-эпидемиологического надзора и выполнения производственного контроля.

В приложении к интересующему нас нормативному документу в табличном виде приводится список максимально допустимых значений по каждому из перечисленных параметров.

Инструктаж по технике безопасности за компьютером

Чтобы донести до работника требования, которые устанавливает техника безопасности при использовании компьютера, работодатель обязан организовать инструктаж. Он проводится на основании специально составленной инструкции, которую обычно разрабатывает специалист по охране труда или непосредственный руководитель работника. Проведение инструктажа нужно организовать до начала самостоятельной работы: специалист допускается к работе только после его прохождения. Это значит, до него донесены правила техники безопасности при работе с компьютером.

Инструкция-памятка по технике безопасности за компьютером должна быть выдана каждому работнику в бумажном или электронном виде. Ей можно дать вид легко читаемой инфографики – например, 10 правил техники безопасности за компьютером.

1. Меры безопасности перед началом работы

В рамках проведения инструктажа до работника доводятся сведения о необходимых действиях, выполняемых на каждом этапе рабочего процесса. Техника безопасности в начале работы на компьютере требует выполнения следующих операций:

* проверить исправность элементов электросистемы, обеспечивающей питание компьютера, включая электропроводку, выключатели, вилки и розетки, при помощи которых аппаратура подключается к сети;
* проконтролировать заземление компьютера;
* проверить его работоспособность.

Техника безопасности возле компьютера в процессе работы

При выполнении работ нужно соблюдать следующие правила:

* запрещается класть на корпус и дисплей компьютера посторонние предметы, прикасаться к элементам аппаратуры мокрыми руками, производить чистку корпуса оборудования, находящегося под напряжением, располагать технику близко к жилищно-коммунальным инженерным системам;
* в случае обнаружения неисправности компьютера немедленно прекратить работу и сообщить об этом непосредственному руководителю;
* эксплуатировать компьютер только с соблюдением инструкции, установленной производителем;
* избегать частого и необоснованного включения и выключения компьютера во время работы.

1. Техника безопасности по окончанию работы за компьютером

После завершения работы сотруднику нужно выполнить следующие действия:

* выключить компьютер с использованием алгоритма, установленного производителем;
* обесточить периферийное оборудование;
* убедиться в отключении техники;
* выполнить очистку рабочих поверхностей влажной тканью.

1. Правильное расположение за компьютером

Требования к расположению работника за компьютером нацелены на обеспечение его комфорта в течение всей рабочей смены и отсутствие негативных следствий длительной работы.

Они действуют для любых рабочих мест, будь то бухгалтерия, обучающий класс или кабинет информатики. Они включают следующие правила:

* полная опора ступнями на пол при посадке;
* использование компьютерной мебели, отвечающей нормам СанПиН 2.2.2/2.4.1340-03;
* отказ от скрещивания конечностей, способного затруднить кровообращение;
* соблюдение расстояние до монитора компьютера не меньше 45 сантиметров;
* правильная установка освещения, которое не должно светить в глаза и оставлять блики на рабочем мониторе.

Для облегчения длительной работы эксперты рекомендуют использовать вспомогательное оборудование, например, особые очки, антибликовые мониторы, коврики для мыши и проч. Нарушения техники безопасности при работе на компьютере способны вызвать стойкие расстройства здоровья, которые потом будет трудно ликвидировать.

1. Режим труда и отдыха

Длительность непрерывного труда и отдыха для сотрудников, постоянно работающих за персональной офисной техникой, регламентирована на законодательном уровне. Соответствующие нормы приводятся в СанПиН 2.2.2/2.4.1340-03, который устанавливает обязательную продолжительность перерывов в такой работе. Они зависят от длины рабочей смены сотрудника и определяются так:

* при 8-часовой рабочей смене в зависимости от тяжести и напряженности труда работника общая продолжительность перерывов за рабочий день должна составлять от 50 до 90 минут;
* при 12-часовой рабочей смене – от 80 до 140 минут.

Проводить такие перерывы за монитором, тратя их на чтение новостей или онлайн-игры, нельзя. Работнику нужно посвятить их физическим упражнениям, короткой прогулке, гимнастике для глаз и другой активности.

Продолжительность указанных перерывов, согласно действующему Трудовому кодексу, включается в общую длительность рабочего времени: рабочий день сотрудника не продлевается за счет таких периодов отдыха. Также в этом время сотрудник не может привлекаться к другой работе.

2 ОСУЩЕСТВЛЕНИЕ АДМИНИСТРИРОВАНИЕ БАЗ ДАННЫХ В РАМКАХ СВОЕЙ КОМПЕТЕНЦИИ

## 2.1 Создание резервных копий баз данных. Восстановление базы данных.

Что бы произвести резервное копирование нужно:

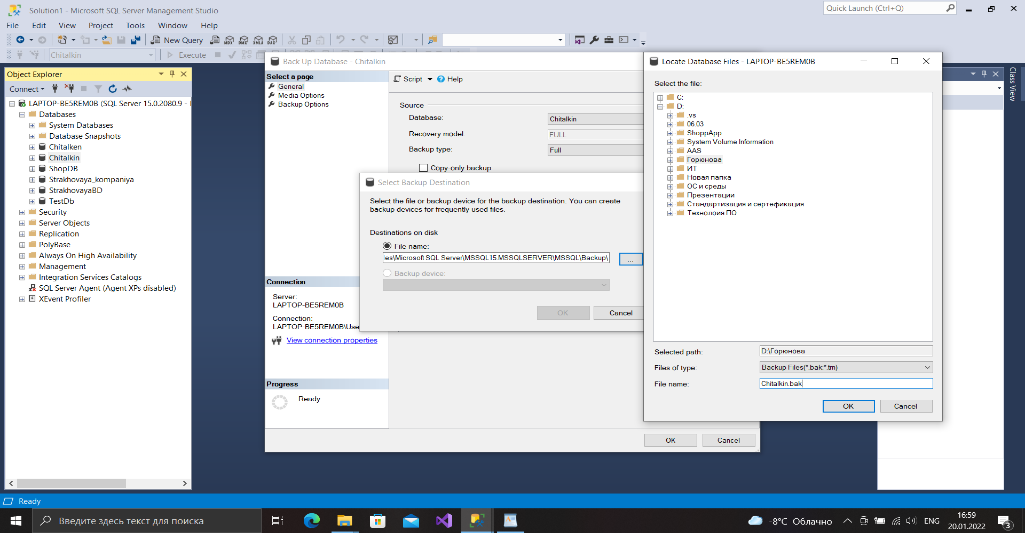
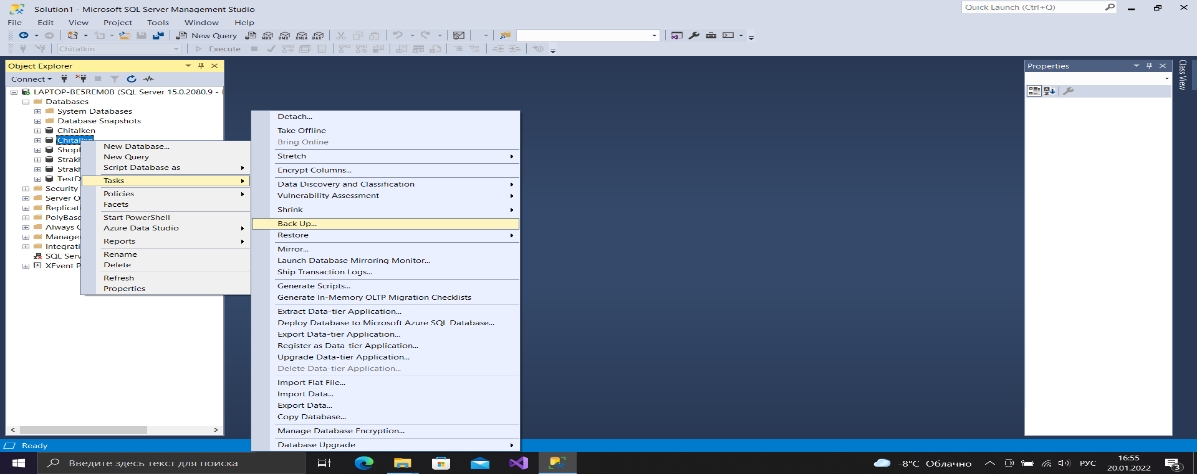


Рисунок 1– Расположение кнопки «Backup» в MSQL. Окно выбора расположение файла.

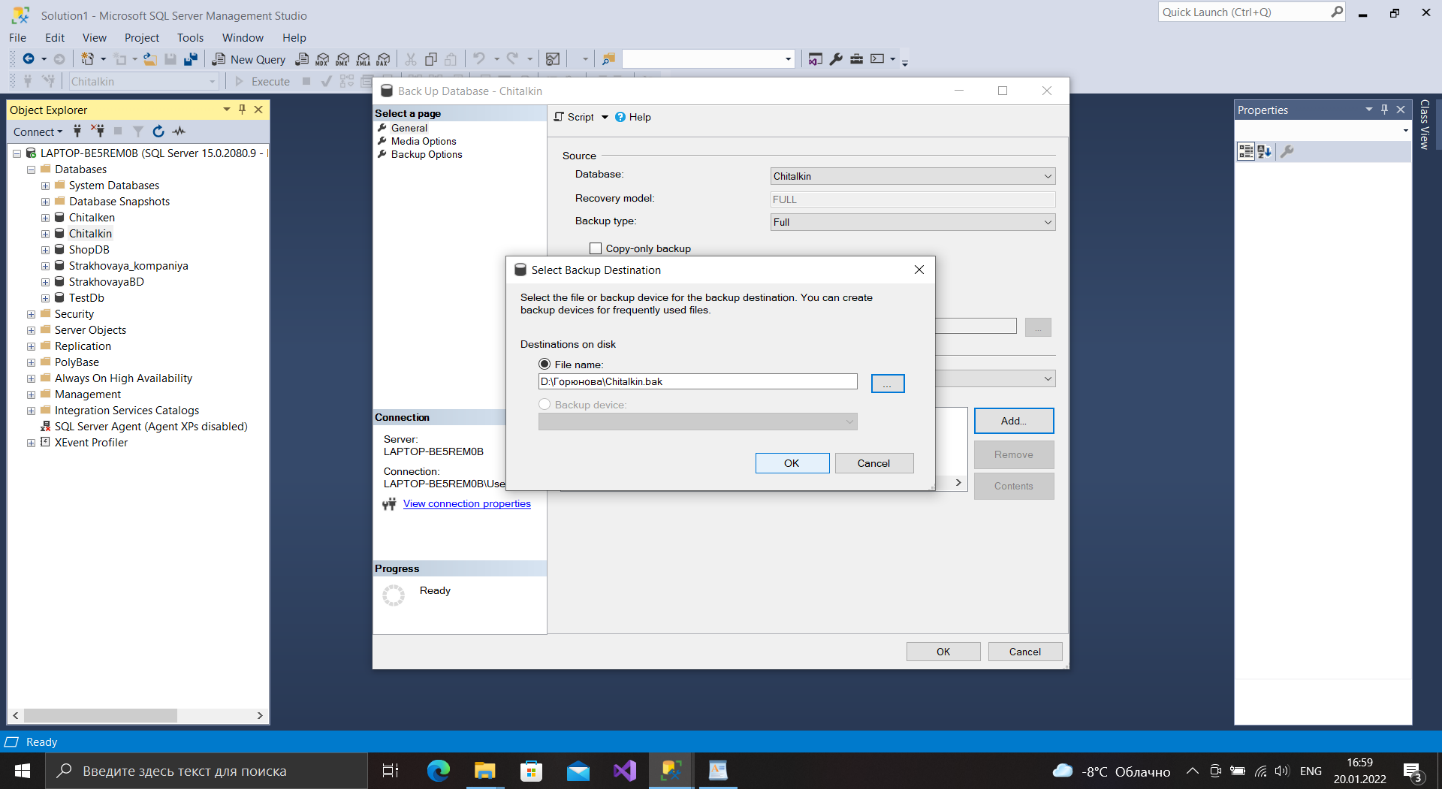
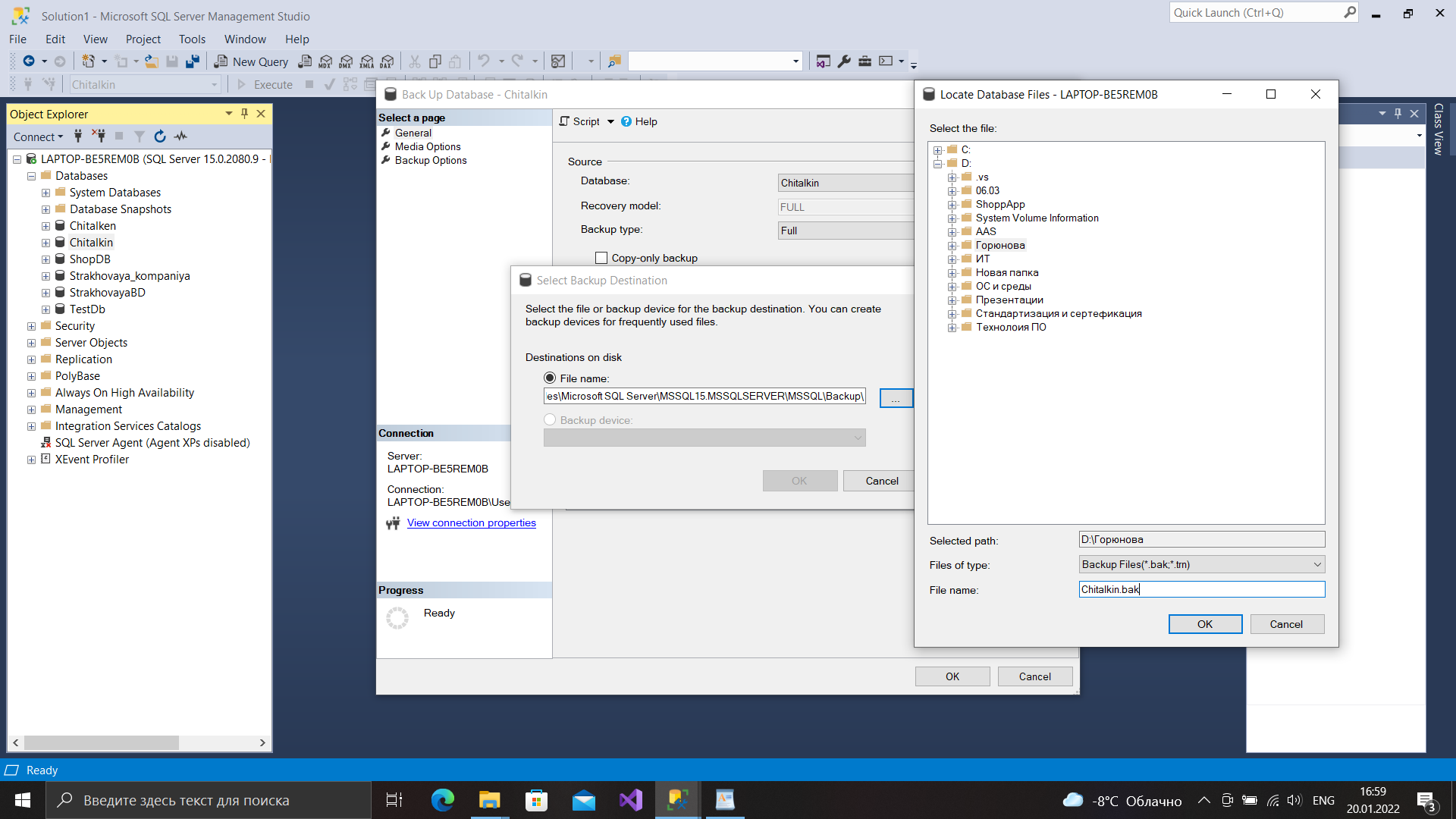


Рисунок 2 – Выбор расположения файла вручную. Окно списка файлов, которые являются резервными.

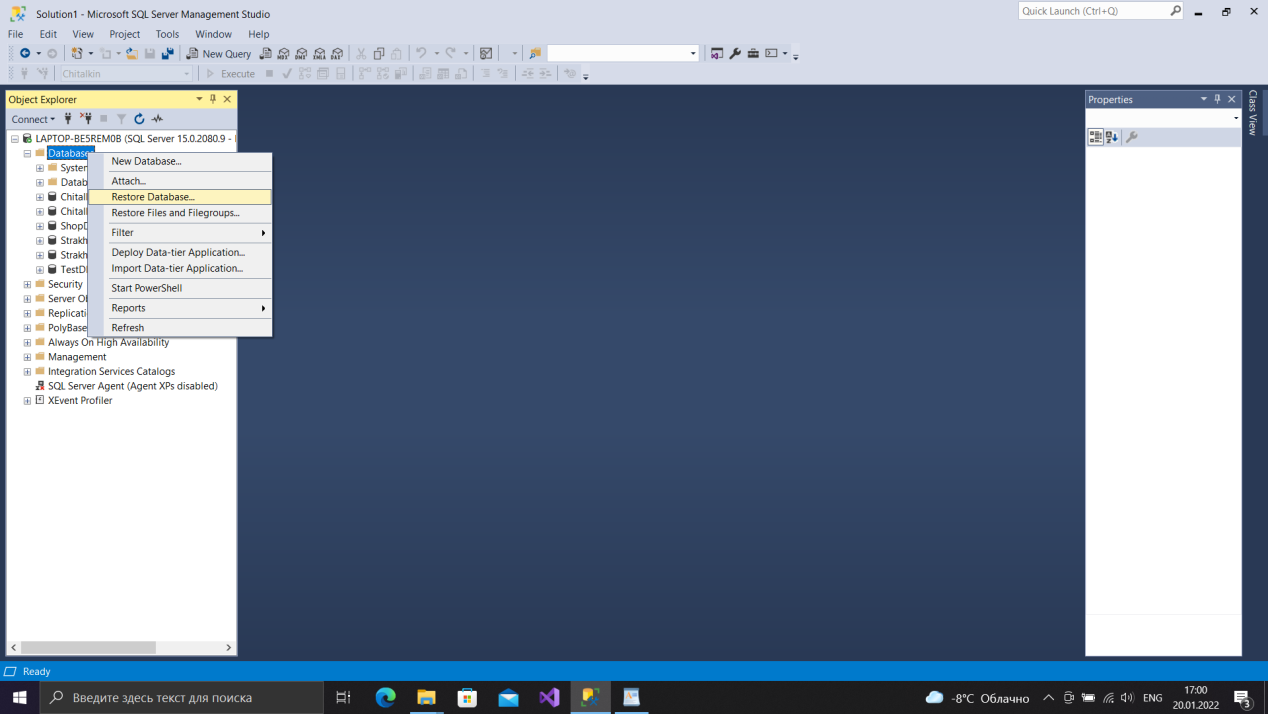
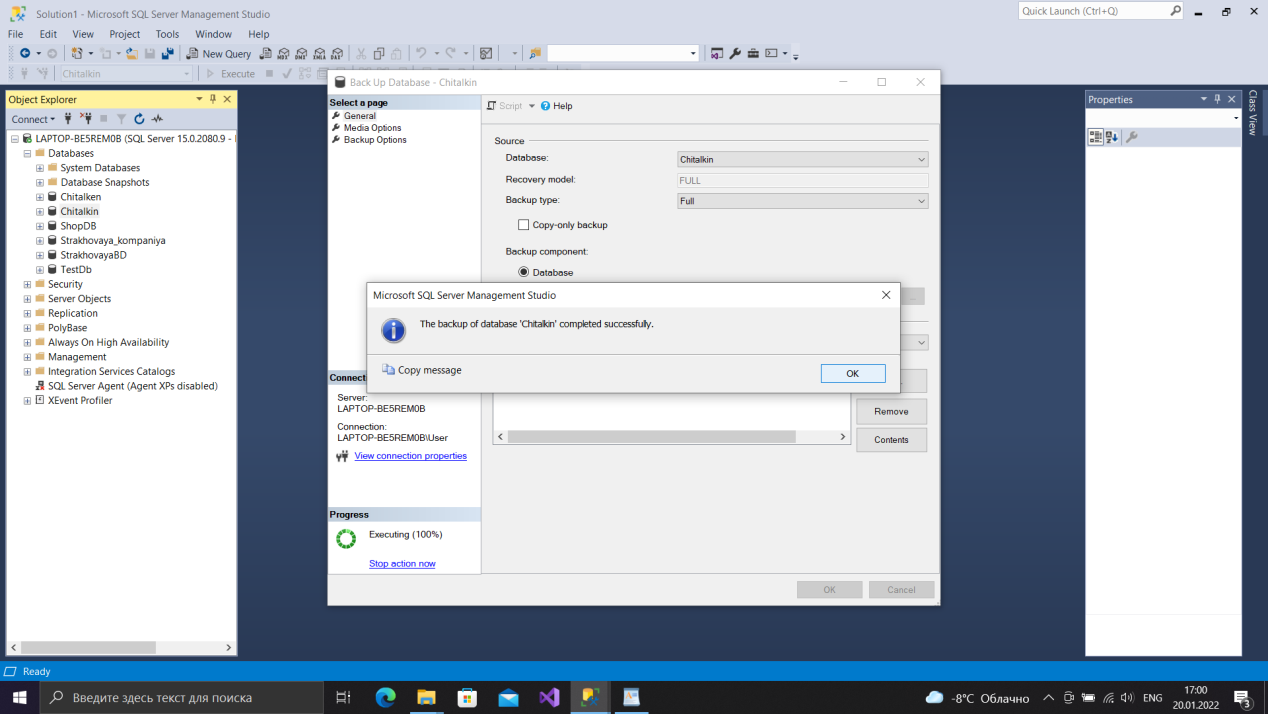


Рисунок 3 – Подтверждение создания файла резервного копирования. Вкладка «Restore DataBase».

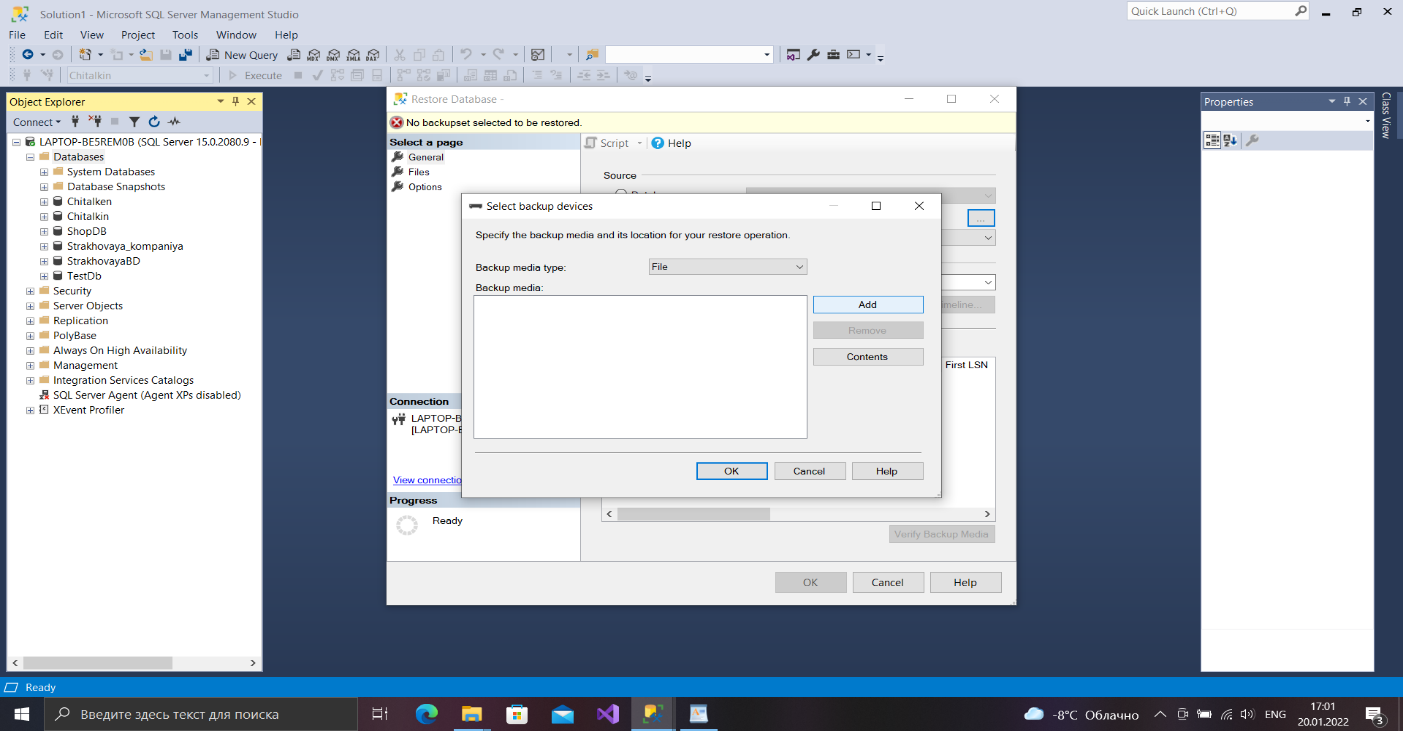
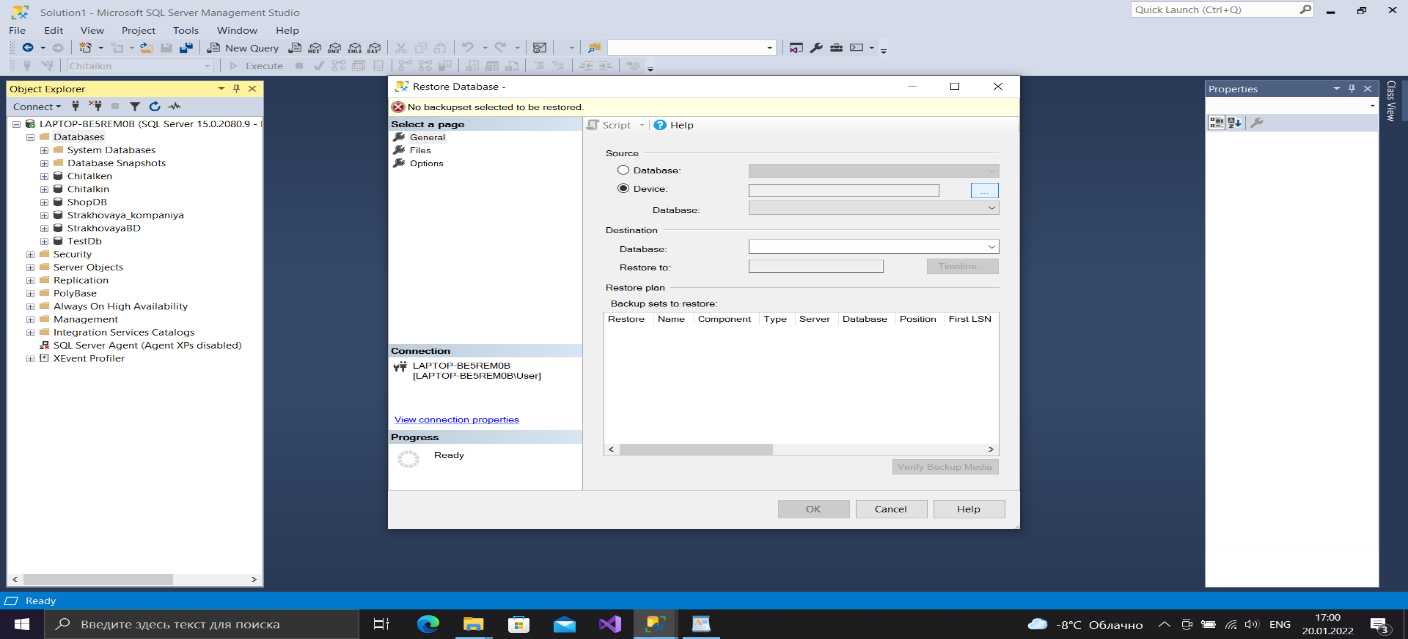


Рисунок 4 –Выбор местоположения файла на устройстве. Окно добавления файла.

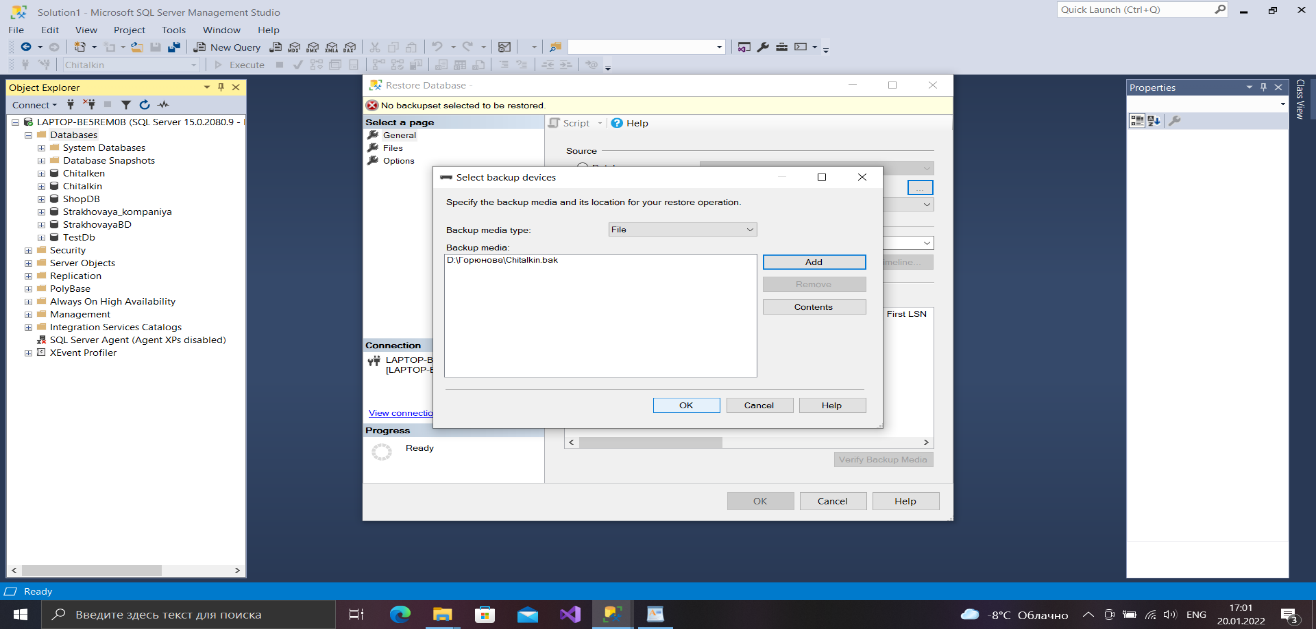
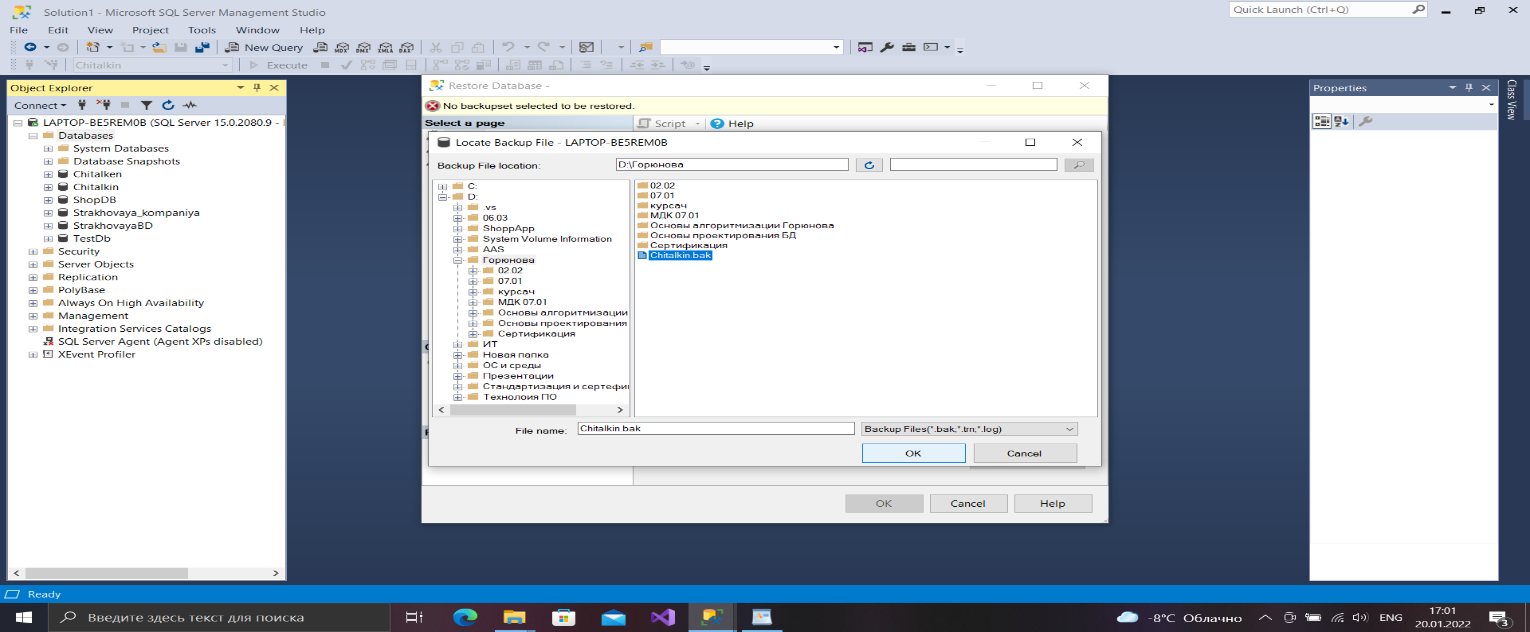


Рисунок 5 – Ручной выбор местоположения файла. Окно подтверждения выбора файла.

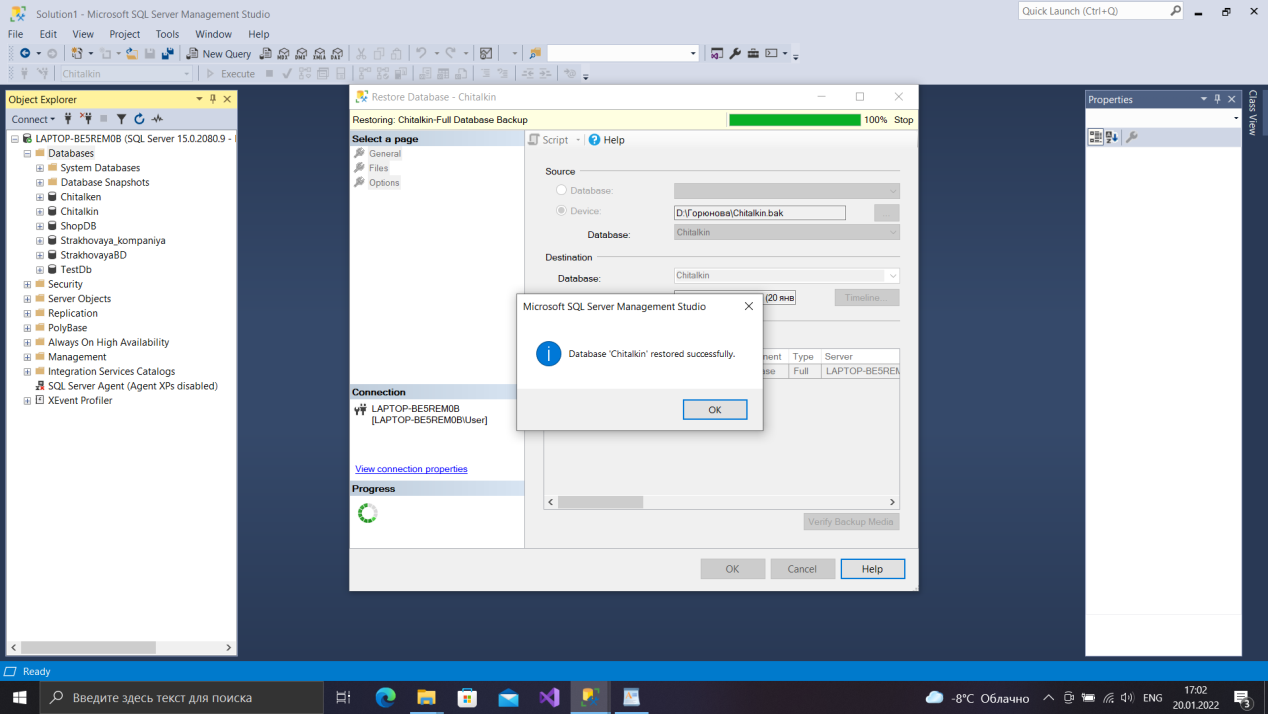
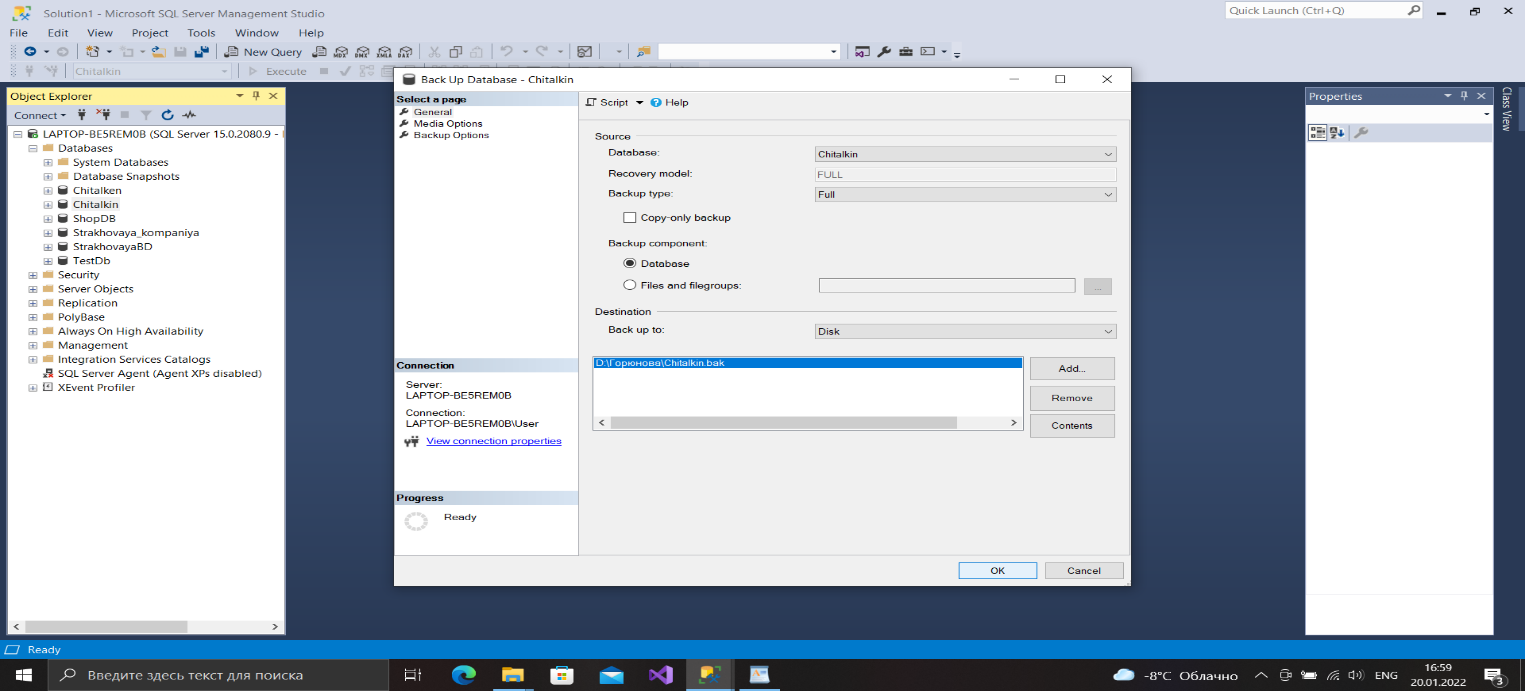


Рисунок 6 – Выбор файлов, отведённых для восстановления. Окно подтверждения восстановления БД.

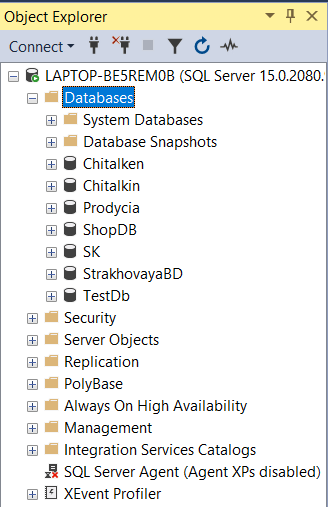


Рисунок 7 – БД находящаяся в меню

## 2.2 Мониторинг активности портов. Блокирование портов.

Нам необходимо выполнить команду Пуск-Выполнить. Откроется окно Запуск программы, в нем вводим команду «cmd». Чтобы вывести все активные подключения TCP и прослушиваемые компьютером порты «TCP/ UDP» вводим команду «netstat».

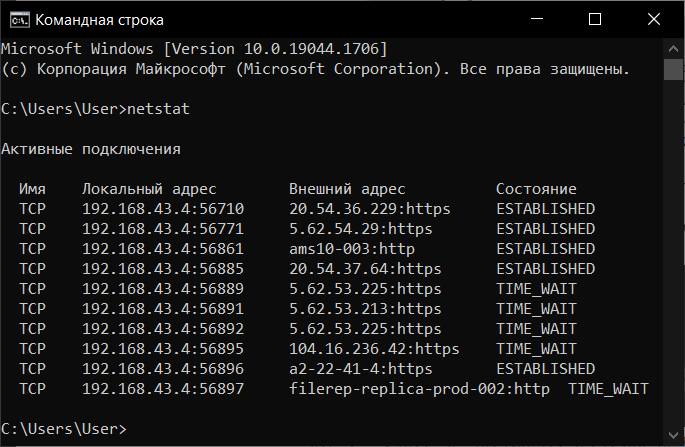


Рисунок 8 – Список активных подключений на тестируемом ПК

Далее был запущен браузер Google Chrome, потом открыл страницу поисковой системы Яндекс. На пяти портах мы видим режим ESTABLISHED — соединения установлены, т.е. сетевые службы работают (используются). Четыре порта используются в режиме TIME\_WAIT — соединение ожидает разрыва.

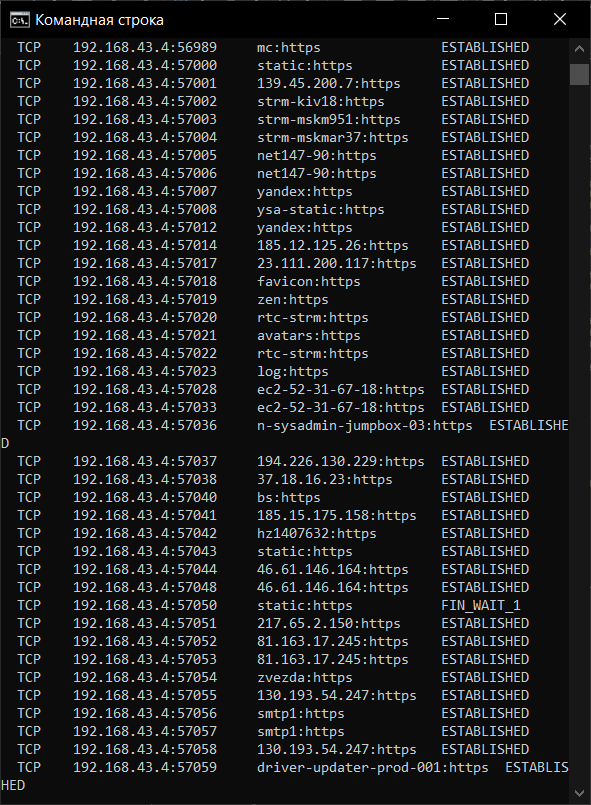
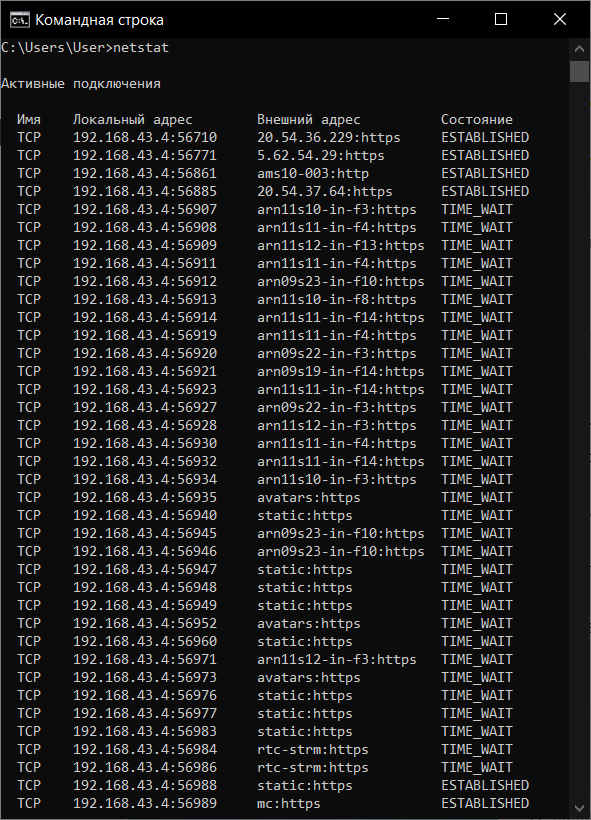


Рисунок 9 – Активные подключения при работе ПК в Интернет

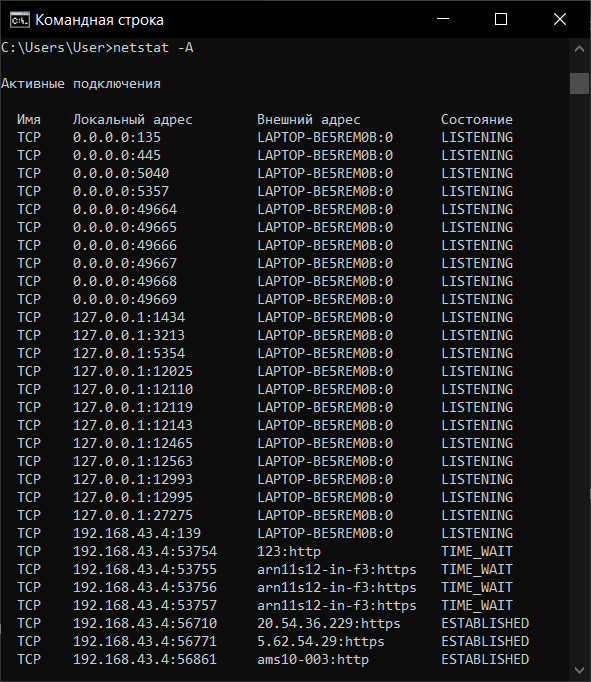
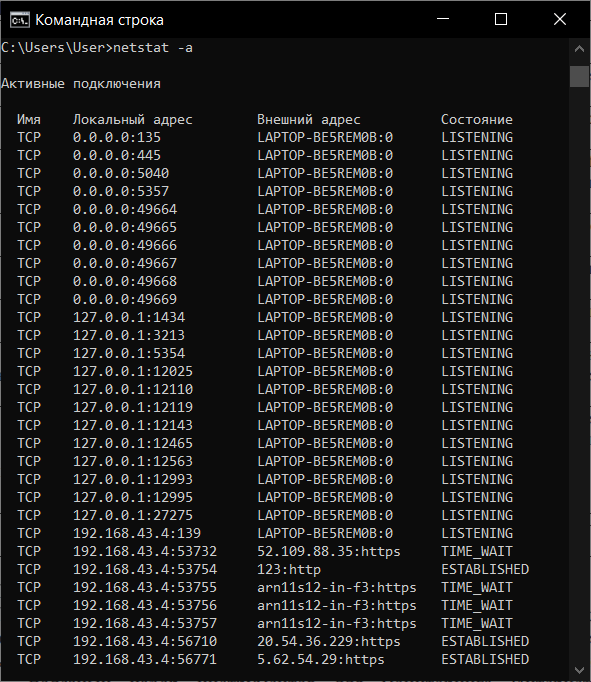


Рисунок 10 – Состояние всех сокетов. Адреса управляющих блоков протокола.

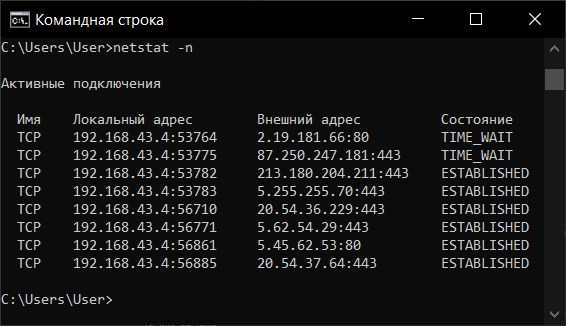
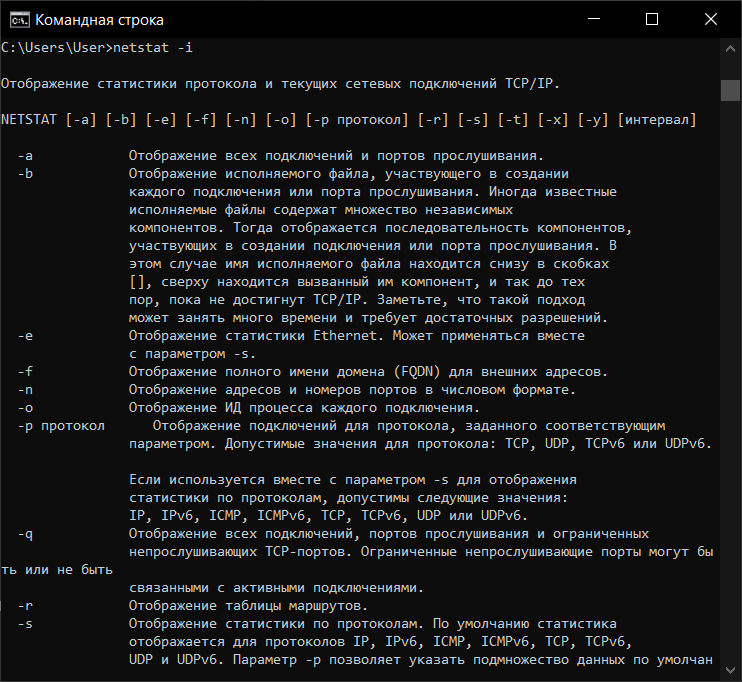


Рисунок 11 – Состояние автоматически сконфигурированных интерфейсов. Сетевые адреса как числа.

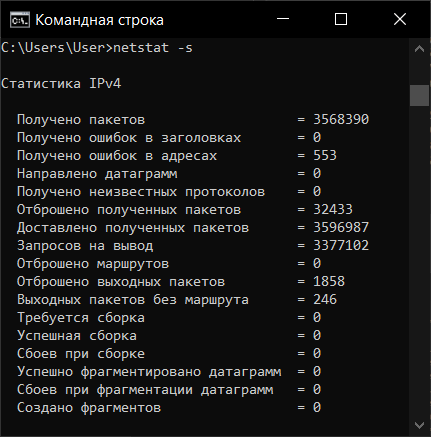
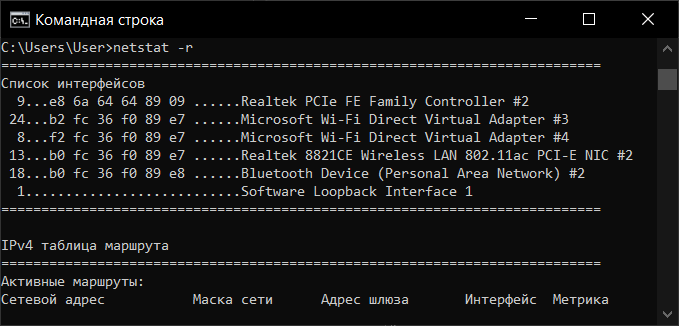


Рисунок 12 – Таблицы маршрутизации. Статистическая информация по протоколам.

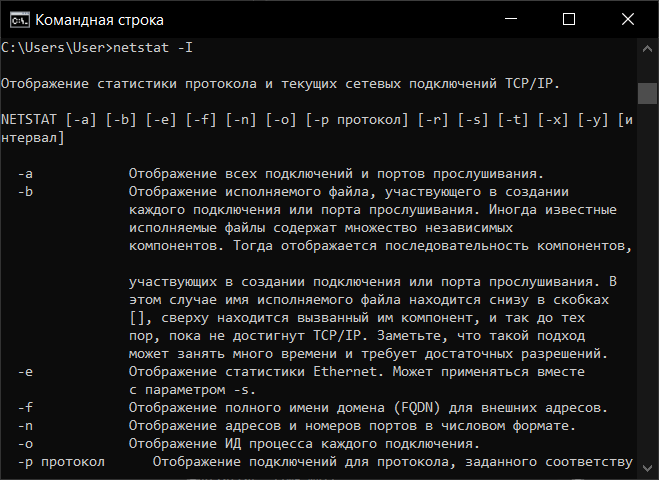
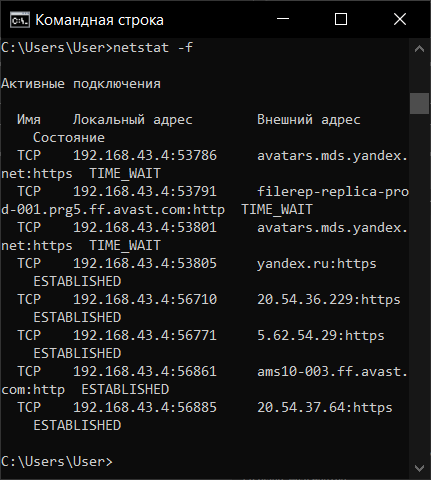


Рисунок 13 – Статистики или адреса управляющих блоков. Информация об указанном интерфейсе в отдельном столбце.

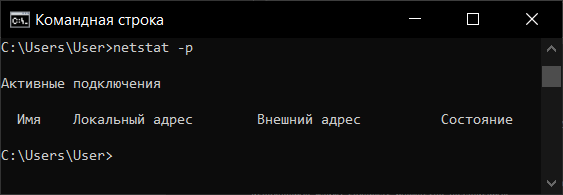


Рисунок 14 – Идентификатор/название процесса, создавшего сокет

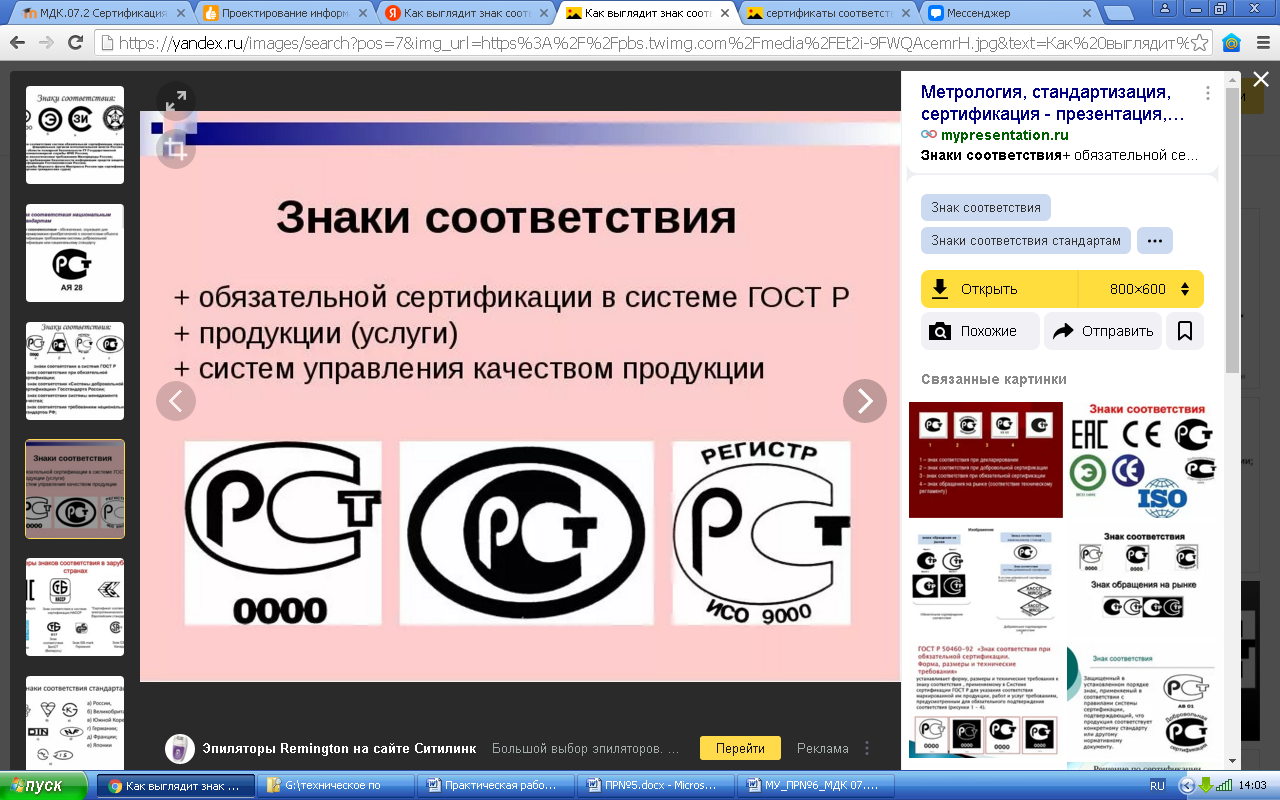
## 3 ПРОВЕДЕНИЕ АУДИТ СИСТЕМ БЕЗОПАСНОСТИ БАЗ ДАННЫХ И СЕРВЕРОВ, С ИСПОЛЬЗОВАНИЕМ РЕГЛАМЕНТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ.

## 3.1 Проверка наличия и сроков действия сертификатов



Рисунок 15 – Сертификат системы менеджмента в области информационной системы

1. Орган, создающий систему: ООО «Экспертно-правовое Бюро»
2. Орган, создающий систему: ООО «Экспертно-правовое Бюро»



1. Закрытое акционерное общество «БИОНТ»

4.614015, г. Пермь, ул. Краснова, д.24

1. 3.11.2020
2. Проектирование разработки, внедрение, тестирование и техническое обслуживания ПО, проектированию объектов, поставке оборудования и программного ПО, технической поддержке и сервисному обслуживанию
3. А.К.Андрианов, Е.В.Лантух.
4. Соответствует требованиям ГОСТ Р ИСО/МЭК 27001-2006(ISO/IEC
5. Сертификат выдан на основание решения экспертной комиссии
6. «Рст» расшифровывается маркировка, как «Российский стандарт». Может применяться только в том случае, если производитель имеет документальное подтверждение – сертификат или декларацию соответствия ГОСТ Р., выданные на основании ПП РФ №982.
7. Основной целью обязательной сертификации является защита прав потребителей от приобретения (использования) товаров, работ, услуг, которые опасны для их жизни, здоровья, имущества, а также для окружающей среды.

## 3.2 Планирование автоматизированных систем для обслуживания баз данных. Планирование автоматизированных систем для обслуживания серверов.

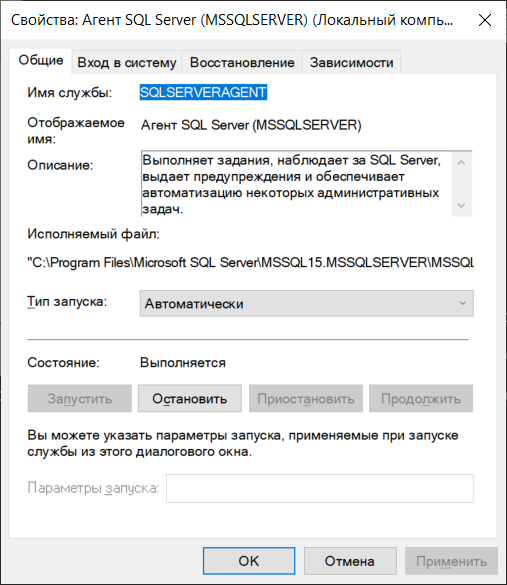
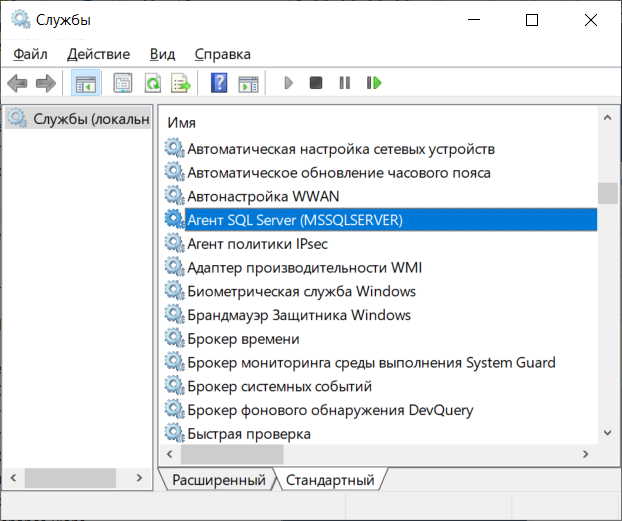


Рисунок 16 – Свойства службы «Агент SQL Server»

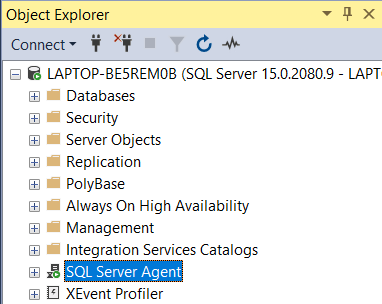


Рисунок 17 – Вкладка «Агент SQL Server» (SQL Server Agent)

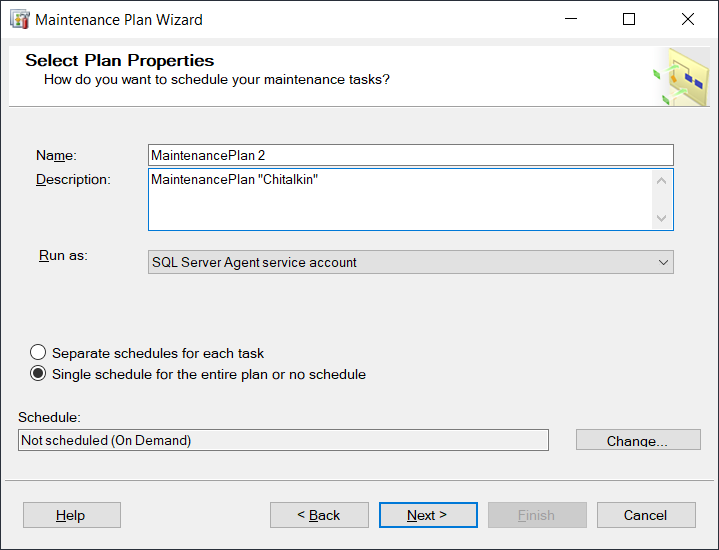
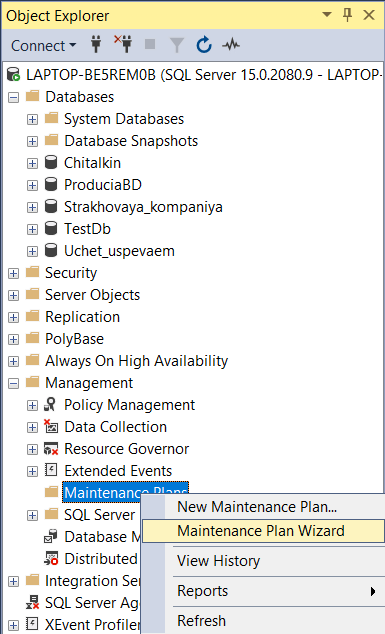


Рисунок 18 – Мастер планов обслуживания. Назначение расписания.

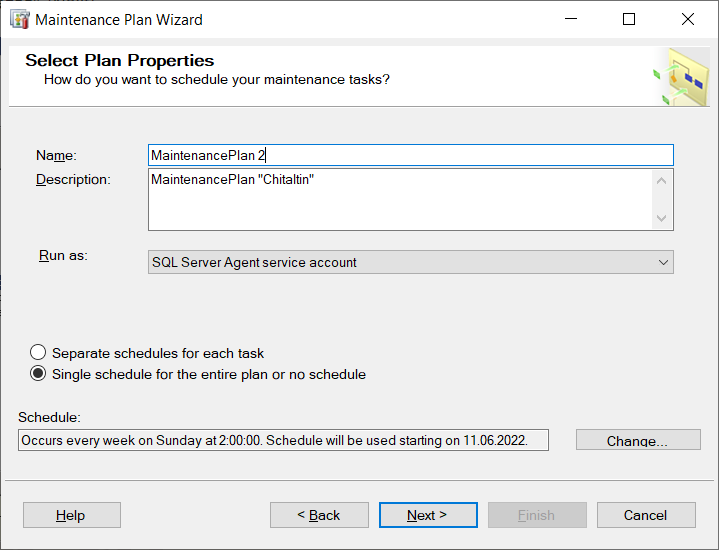
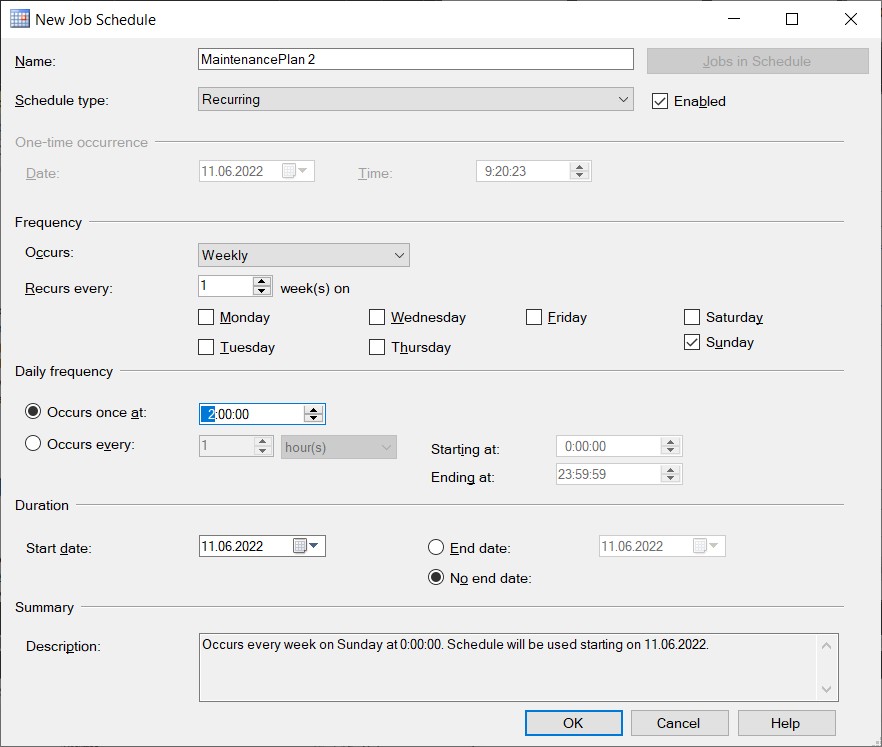


Рисунок 19 – Свойства расписания задания

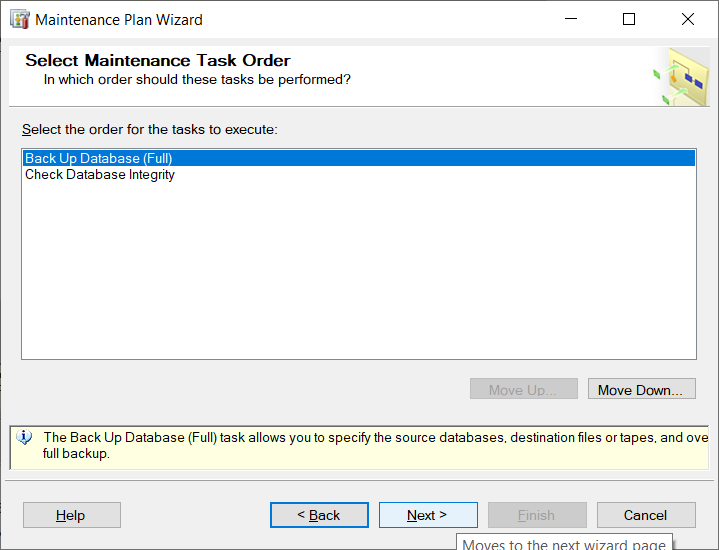
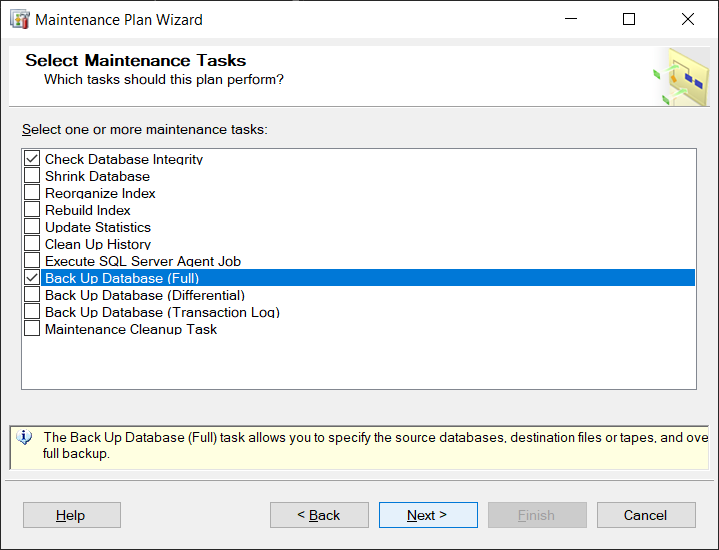


Рисунок 20 – Выбор задачи. Порядок выполнения задач.

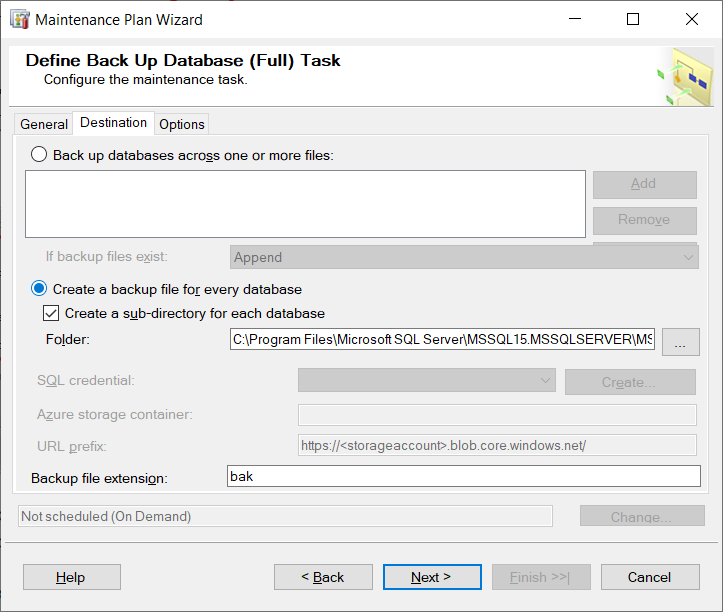
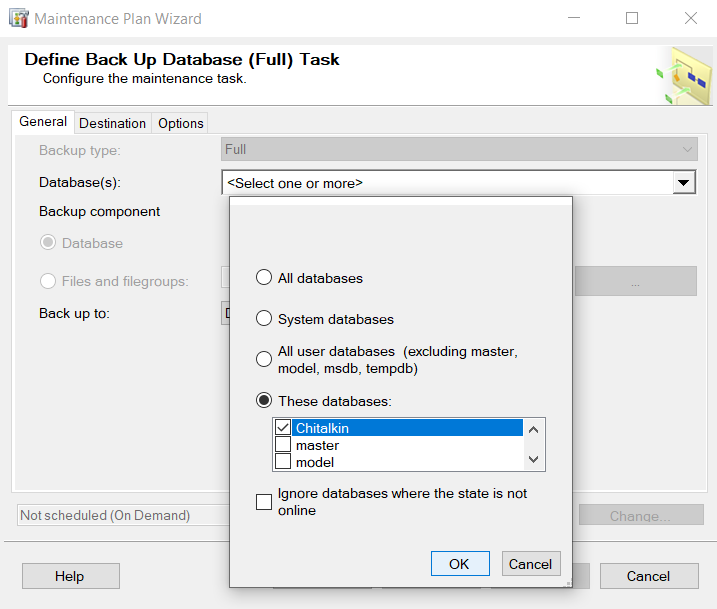


Рисунок 21 – Параметры задачи «Копирование БД (полное)» (Back Up Database (Full))

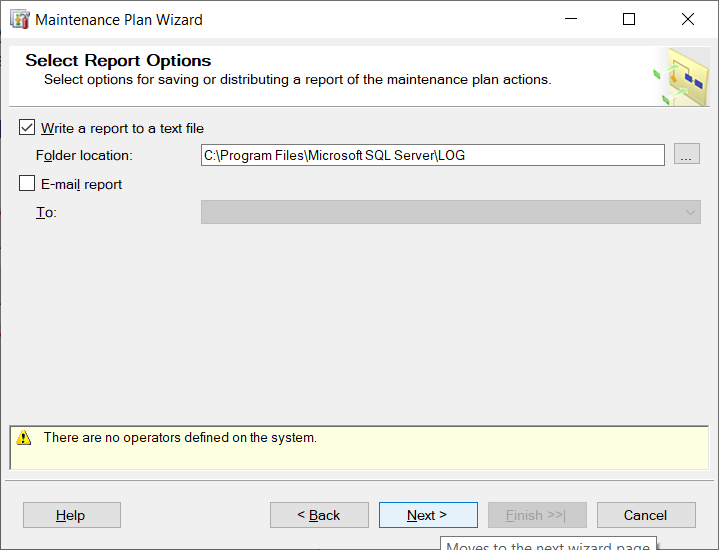
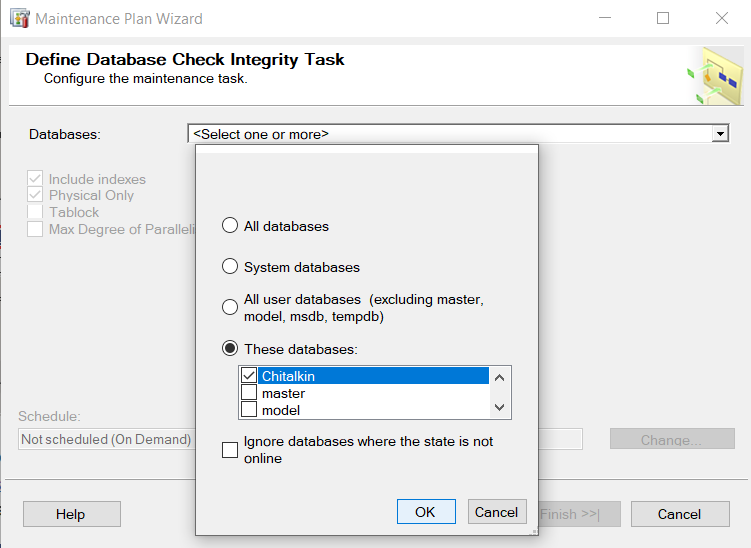


Рисунок 22 – Параметры задачи «Проверка целостности базы данных» (Database Check Integrity)

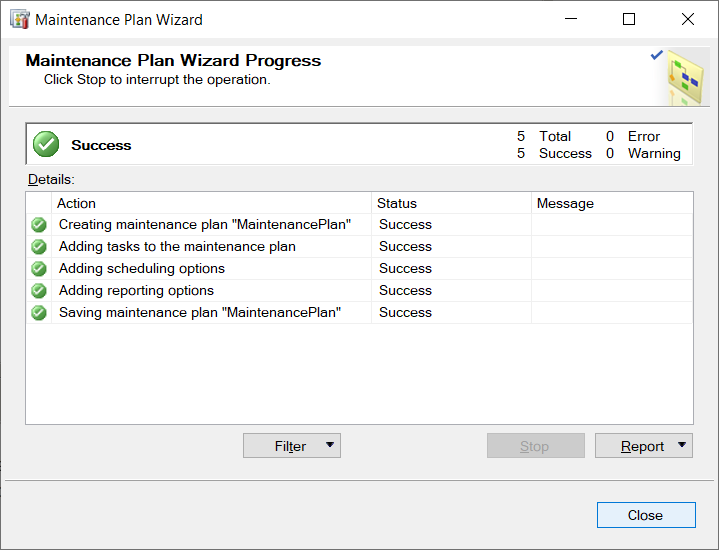
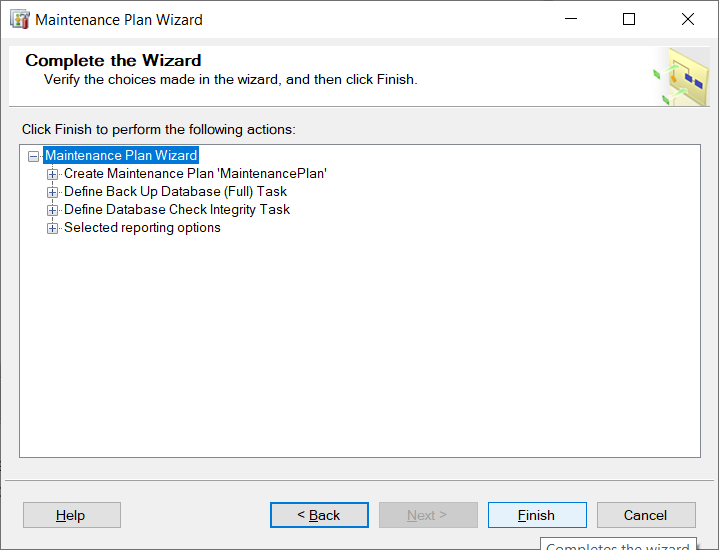


Рисунок 23 – Построение плана обслуживания

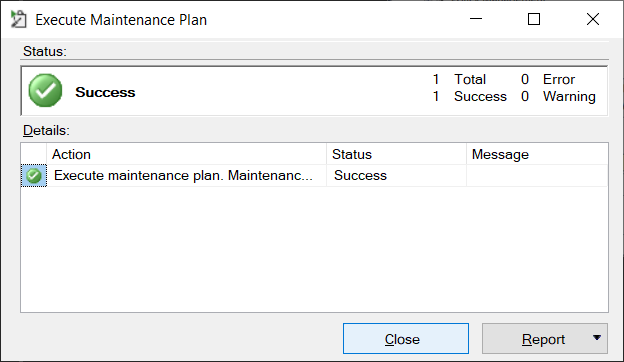
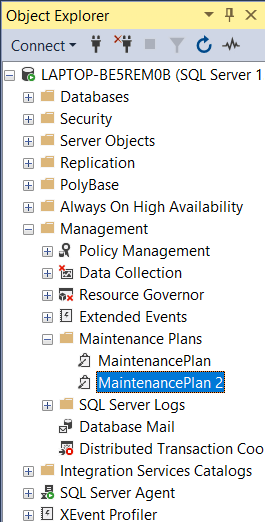


Рисунок 24 – Выполнение плана



Рисунок 25 – Файл резервной копии