**Отчет**

**по учебной практике УП 05.01**

**профессионального модуля**

**ПМ 05. Соадминистрирование баз данных и серверов**

**Специальность 09.02.07 Информационные системы и программирование**

**Квалификация: специалист по информационным системам**

|  |  |  |
| --- | --- | --- |
|  |  | Студента группы 4ИС1-20  Фамиля Имя Отчество  Оценка\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Групповой руководитель практики:  \_\_\_\_\_\_\_\_\_\_\_\_ М.К. Полянский |

2024

Утверждаю

Зам. директора по УПР

\_\_\_\_\_\_\_\_\_\_\_Жилкина Е.Н.

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_20\_\_\_г.

**Задание**

по учебной практике УП 05.01

профессионального модуля

ПМ 05. Соадминистрирование баз данных и серверов

Выдано студенту группы 4ИС1-19 Фамилия Имя Отчество

на период с «05» февраля 2024 г. по «17» февраля 2023 г.

**Виды работ:**

**Обязательная**

* инструктаж по прохождению практики и правилам безопасности работы;
* ознакомление с техническим парком СВТ и существующей системой сетевых телекоммуникаций;
* ознакомление с используемым системным программным обеспечением, корпоративными стандартам;
* проектирование и создание базы данных;
* формирование необходимых для работы информационной системы требований к конфигурации локальных компьютерных сетей и серверного оборудования;
* выполнение запросов по обработке данных на языке SQL;
* осуществление основные функции по администрированию баз данных;
* выявление технических проблем, возникающих в процессе эксплуатации баз данных;
* участие в администрировании отдельных компонент серверов;
* участие в соадминистрировании серверов;
* участие в администрировании отдельных компонент серверов;
* осуществление основных функций по администрированию баз данных;
* разработка политики безопасности SQL сервера, базы данных и отдельных объектов базы данных;
* проверка наличия сертификатов на информационную систему или бизнес-приложения;
* оформление отчетов.

В отчете отражается:

1. Титульный лист.
2. Дневник прохождения практики, заверенный подписью руководителя.
3. Аттестационный лист прохождения практики с характеристикой.
4. Приложение.

**Дневник**

**учебной практики УП 05.01**

**профессионального модуля**

**ПМ 05. Соадминистрирование баз данных и серверов**

**Специальность 09.02.07 Информационные системы и программирование**

**Квалификация: специалист по информационным системам**

Студента группы 4ИС1-20

Фамилия Имя Отчество

Сроки прохождения практики с 05.02.2024 по 17.02.2024

|  |  |  |
| --- | --- | --- |
| **Дата** | **Выполняемые работы** | **Подпись группового руководителя** |
| **05.02.24** | Инструктаж по прохождению практики и правилам безопасности работы.  Ознакомление с техническим парком СВТ и существующей системой сетевых телекоммуникаций. |  |
| **06.02.24** | Ознакомление с используемым системным программным обеспечением, корпоративными стандартами.  Проектирование и создание базы данных. |  |
| **07.02.24** | Формирование необходимых для работы информационной системы требований к конфигурации локальных компьютерных сетей и серверного оборудования. |  |
| **08.02.24** | Выполнение запросов по обработке данных на языке SQL.  Осуществление основные функции по администрированию баз данных. |  |
| **09.02.24** | Выявление технических проблем, возникающих в процессе эксплуатации баз данных. |  |
| **10.02.24** | Участие в администрировании отдельных компонент серверов. Участие в соадминистрировании серверов. |  |
| **12.02.24** | Участие в администрировании отдельных компонент серверов. |  |
| **13.02.24** | Осуществление основных функций по администрированию баз данных. |  |
| **14.02.24** | Разработка политики безопасности SQL сервера, базы данных и отдельных объектов базы данных. |  |
| **15.02.24** | Проверка наличия сертификатов на информационную систему или бизнес-приложения. |  |
| **16.02.24** | Оформление отчетов. Оформление дневника и отчета по практике |  |
| **17.02.24** | Оформление отчетов. Оформление дневника и отчета по практике |  |

**Общие сведения об организации базы практики**

Полное наименование: Государственное Бюджетное Профессиональное Образовательное Учреждение «Брянский Профессионально Педагогический Колледж»

Адрес: 241016 г. Брянск, ул. Почтовая, дом 4.

Сроки проведения практики: с 05.02.24 по 17.02.24

Директор учебного заведения: Яковлева Светлана Степановна

Зам директора по УПР: Жилкина Елена Николаевна

Руководитель практики: Прошкина Светлана Викторовна

Групповой руководитель Полянский Максим Константинович



Рисунок 1 – ГБПОУ «БППК»

**Инструкция по технике безопасности**

**1. ОБЩИЕ ТРЕБОВАНИЯ ОХРАНЫ ТРУДА**

1.1. Студенты, проходящие практику (далее – студенты), допускаются к выполнению работ только при наличии соответствующих документов для прохождения практики (задания), прохождения вводного инструктажа по охране труда, инструктажа по охране труда на рабочем месте.

1.2. Проведение всех видов инструктажей должно регистрироваться в журналах регистрации инструктажей с обязательными подписями получившего и проводившего инструктажи.

1.3. Каждому студенту необходимо:

— знать место хранения аптечки первой помощи;

— уметь оказать первую помощь;

— уметь правильно действовать при возникновении пожара.

1.4. Студенту следует:

— оставлять верхнюю одежду, обувь, головной убор в гардеробной или иных местах, предназначенных для хранения верхней одежды;

— иметь опрятный вид в соответствии с требованиями делового этикета;

— не принимать пищу на рабочем месте.

1.5. Работа студентов при прохождении практики может сопровождаться наличием следующих опасных и вредных факторов:

— работа на персональных компьютерах – ограниченной двигательной активностью, монотонностью и значительным зрительным напряжением;

— работа с электроприборами (приборы освещения, бытовая техника, принтер, сканер и прочие виды офисной техники) – повышенным значением напряжения электрической цепи.

1.6. Помещения, предназначенные для размещения рабочих мест, оснащенных персональными компьютерами, следует оснащать солнцезащитными устройствами (жалюзи, шторы и пр.).

1.7. Все помещения с персональными компьютерами должны иметь естественное и искусственное освещение.

1.8. Запрещается применение открытых ламп (без арматуры) в установках общего и местного освещения.

1.9. Искусственное освещение на рабочих местах в помещениях с персональными компьютерами следует осуществлять в виде комбинированной системы общего и местного освещения.

1.10. Для борьбы с запыленностью воздуха необходимо проводить влажную ежедневную уборку и регулярное проветривание помещения.

1.11. Рабочее место должно включать: рабочий стол, стул (кресло) с регулируемой высотой сиденья.

1.12. Студенты несут ответственность в соответствии с действующим законодательством за соблюдение требований настоящей инструкции.

**2. ТРЕБОВАНИЯ ОХРАНЫ ТРУДА ПЕРЕД НАЧАЛОМ РАБОТЫ**

2.1. Прибыть на практику заблаговременно для исключения спешки и, как следствие, падения и случаев травматизма, при этом:

— не подниматься и не спускаться бегом по лестничным маршам;

— не садиться и не облокачиваться на ограждения и случайные предметы;

— обращать внимание на знаки безопасности, сигналы и выполнять их требования;

— не приступать к работе в состоянии алкогольного или наркотического опьянения.

2.2. Осмотреть рабочее место и оборудование. Проверить оснащенность рабочего места необходимым для работы оборудованием, инвентарем, приспособлениями и инструментами. Убрать все лишние предметы.

2.3. Очистить экран дисплея персонального компьютера от пыли. Отрегулировать высоту и угол наклона экрана.

2.4. Отрегулировать уровень освещенности рабочего места.

2.5. Отрегулировать кресло по высоте. Проверить исправность оборудования.

2.6. О замеченных недостатках и неисправностях немедленно сообщить руководителю практики и до устранения неполадок и разрешения руководителя к работе не приступать.

**3. ТРЕБОВАНИЯ ОХРАНЫ ТРУДА ВО ВРЕМЯ РАБОТЫ**

3.1. На рабочих местах, оснащенных персональными компьютерами:

3.1.1. Экран должен находиться ниже уровня глаз на 5 град, и располагаться в прямой плоскости или с наклоном на оператора (15 град.).

3.1.2. Расстояние от глаз оператора до экрана должно быть в пределах 60-80 см.

3.1.3. Местный источник света по отношению к рабочему месту должен располагаться таким образом, чтобы исключить попадание в глаза прямого света, и должен обеспечивать равномерную освещенность на поверхности 40 х 40 см, не создавать слепящих бликов на клавиатуре и других частях пульта, а также на экране видеотерминала в направлении глаз работника.

3.1.4. Для снижения зрительного и общего утомления после каждого часа работы необходимо делать перерывы.

3.1.5. Необходимо в течение всего рабочего дня содержать в порядке и чистоте рабочее место.

3.1.6. Во время работы запрещается:

— прикасаться к задней панели системного блока (процессора) при включенном питании;

— производить переключение разъемов интерфейсных кабелей периферийных устройств при включенном питании;

— загромождать верхние панели устройств бумагами и посторонними предметами;

— допускать захламленность рабочего места;

— производить отключение питания во время выполнения активной задачи;

— допускать попадание влаги на поверхность системного блока (процессора), монитора, рабочую поверхность клавиатуры, дисководов, принтеров и др. устройств;

— производить самостоятельно вскрытие и ремонт оборудования.

3.2. При работе с электроприборами и оргтехникой (персональные компьютеры, принтеры, сканеры, копировальные аппараты, факсы, бытовые электроприборы, приборы освещения):

3.2.1. Автоматические выключатели и электрические предохранители должны быть всегда исправны.

3.2.2. Изоляция электропроводки, электроприборов, выключателей, штепсельных розеток, ламповых патронов и светильников, а также шнуров, с помощью которых включаются в электросеть электроприборы, должны быть в исправном состоянии.

3.2.3. Электроприборы необходимо хранить в сухом месте, избегать резких колебаний температуры, вибрации, сотрясений.

3.2.4. Запрещается:

— пользоваться неисправными электроприборами и электропроводкой;

— очищать от загрязнения и пыли включенные осветительные аппараты и электрические лампы;

— ремонтировать электроприборы самостоятельно;

— прикасаться одновременно к персональному компьютеру и к устройствам, имеющим соединение с землей (радиаторы отопления, водопроводные краны, трубы и т.п.), а также прикасаться к электрическим проводам, неизолированным и неогражденным токоведущим частям электрических устройств, аппаратов и приборов (розеток, патронов, переключателей, предохранителей).

3.3. При перерыве в подаче электроэнергии и уходе с рабочего места выключать оборудование.

3.4. По пути к месту практики и обратно:

3.5. Избегать экстремальных условий на пути следования.

3.6. Соблюдать правила дорожного движения и правила поведения в транспортных средствах.

3.7. Соблюдать осторожность при обходе транспортных средств и других препятствий, ограничивающих видимость проезжей части.

3.8. В период неблагоприятных погодных условий (гололед, снегопад, туман) соблюдать особую осторожность.

**4. ТРЕБОВАНИЯ ОХРАНЫ ТРУДА В АВАРИЙНЫХ СИТУАЦИЯХ**

4.1. Немедленно прекратить работу, отключить персональный компьютер, иное электрооборудование и доложить руководителю работ, если:

— обнаружены механические повреждения и иные дефекты электрооборудования и электропроводки;

— наблюдается повышенный уровень шума при работе оборудования;

— наблюдается повышенное тепловыделение от оборудования;

— мерцание экрана не прекращается;

— наблюдается прыганье текста на экране;

— чувствуется запах гари и дыма;

— прекращена подача электроэнергии.

4.2. Не приступать к работе до полного устранения неисправностей.

4.3. В случае возгорания или пожара студенты, проходящие практику) должны немедленно прекратить работу, отключить электроприборы, вызвать пожарную бригаду по телефону 101, сообщить руководителю работ и приступить к ликвидации очага пожара имеющимися средствами огнетушения.

4.4. При обнаружении запаха газа в помещении:

— предупредить работников, находящихся в помещении, о недопустимости пользования открытым огнем, курения, включения и выключения электрического освещения и электроприборов;

— открыть окна (форточки, фрамуги) и проветрить помещение;

— сообщить об этом администрации организации, а при необходимости – вызвать работников аварийной газовой службы по телефону 104.

4.5. При несчастном случае:

— освободить пострадавшего от травмирующего фактора,

— поставить в известность руководителя работ,

— оказать пострадавшему первую доврачебную помощь,

— по возможности сохранить неизменной ситуацию до начала расследования причин несчастного случая, если это не приведет к аварии или травмированию других людей,

— при необходимости вызвать бригаду скорой помощи по телефону 101 или помочь доставить пострадавшего в медучреждение.

**5. ТРЕБОВАНИЯ ОХРАНЫ ТРУДА ПО ОКОНЧАНИИ РАБОТЫ**

5.1. Привести в порядок рабочее место.

5.2. Отключить и обесточить оборудование.

5.3. При выходе из здания организации (предприятия):

— убедиться в отсутствии движущегося транспорта;

— ходить по тротуарам и пешеходным дорожкам.

**Технический парк СВТ и система сетевых телекоммуникаций**

**в ГБПОУ «БППК»**

В современных условиях работы, важной областью стало информационное обеспечение, которое состоит в сборе и переработке информации, необходимой для принятия обоснованных управленческих решений на предприятии или организации.

Вся информация о хозяйственной деятельности предприятия или организации фиксируется в первичных документах. Согласно законодательству, формирование этих документов обязательно, они служат подтверждением совершенных хозяйственных операций.

Технический парк организации содержит следующие элементы:

**Компьютер:**

|  |  |
| --- | --- |
| Тип компьютера | ACPI компьютер на базе x64 (Mobile) |
| Операционная система | Microsoft Windows 10 Home |
| Пакет обновления ОС | v.1909 |
| Google Chrome | 88.0.4324.190 |
| DirectX | DirectX 12.0 |
| Имя компьютера | DESKTOP-DASTB3B |
| Имя пользователя | ROOT |
| Вход в домен | Администратор |

**Дисплей:**

|  |  |
| --- | --- |
| Видеоадаптер | AMD Radeon 530 (2ГБ) |
| 3D-акселератор | AMD Radeon 530 |
| Монитор | Универсальный монитор PHP |

**Системная плата:**

|  |  |
| --- | --- |
| ЦП | AMD Ryzen 3 2200G (2x2.2GHz) |
| Системная плата | HP 84AF |
| Чипсет системной платы | AM4 |
| Оперативная память | 8GB 2133MHz |
| Тип BIOS | UEFI (AHCI) |

**Хранение данных:**

|  |  |
| --- | --- |
| IDE-контроллер | Стандартный контроллер SATA AHCI |
| Контроллер хранения данных | Контроллер дискового пространства (Майкрософт) |
| Контроллер хранения данных | Стандартный контроллер NVM Express |
| Дисковый накопитель | ST1000LM035 (1 ТБ) |

**Разделы:**

|  |  |
| --- | --- |
| C: (NTFS) | 430 ГБ (329 ГБ свободно) |
| D: (NTFS) | 499 ГБ (365 ГБ свободно) |

**Сеть:**

|  |  |
| --- | --- |
| Первичный адрес IP | 192.168.4.199 |
| Первичный адрес MAC | 74-40-BB-68-FD-C7 |
| Сетевой адаптер | Realtek RTL8723DE 802.11b/g/n PCIe Adapter |

**Используемое системное и программное обеспечение ГБПОУ «БППК», корпоративные стандарты**

Вводное слово

1. Windows 10

Описание краткое

1. Google Chrome

Описание краткое

1. Virtual-Box

Описание краткое

1. CentOS7

Описание краткое

1. Apache HTTP Server

Описание краткое

1. Asterisk

Описание краткое

1. FreePBX

Описание краткое

1. PHP 7.4

Описание краткое

1. Fail2Ban

Описание краткое

**Проектирование и создание базы данных**

Описать что такое и зачем нужна БД.

Как и зачем БД проектируется.

Как управлять БД.

**Формирование необходимых для работы информационной системы, требований к конфигурации локальных компьютерных сетей и серверного оборудования**

Описать какие системные требования предъявляется к оборудованию, на котором можно развернуть информационную систему на примере Asterisk

**Выполнение запросов по обработке данных на языке SQL**

Что такое SQL запрос, зачем нужен как выглядит, как строиться, абстрактный пример. Какие SQL запросы использовали мы, описать подробно, что почему и зачем.

**Основные функции по администрированию баз данных**

Администратор данных отвечает за корпоративные информационные ресурсы, включая и некомпьютеризированные данные. На практике это часто связано с управлением данными, которые являются совместно используемым ресурсом для различных пользователей и прикладных программ данной организации. В разных организациях количество сотрудников, выполняющих функции АД, может отличаться и обычно определяется размерами самой организации. Основная обязанность АД состоит в обмене консультациями и советами со старшими менеджерами, а также в слежении за тем, чтобы применение технологий баз данных продолжало соответствовать корпоративным целям. Должность АД обычно принадлежит отделу информационных систем организации. В одних случаях администрирование данных может представлять собой отдельную функциональную задачу, а в других — совмещаться с администрированием базы данных.

Основными функциями по администрированию созданной базы данных являются:

* Распределение доступа к базе данных через форму авторизации;
* Добавление записей;
* Изменение записей;
* Удаление записей.

Распределение доступа к базе данных через форму авторизации:

Подключение к форме администрирования базы данных происходит через форму авторизации пользователя:

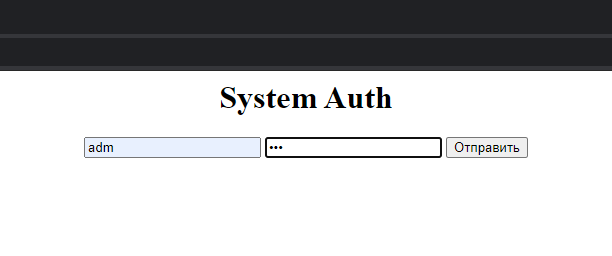


Рисунок 2 - форма авторизации

Эта форма предназначена для работы локальных администраторов или пользователей. Для входа в систему, необходимо подать заявку на регистрацию системному администратору и запрос на свои идентификационные данные (в форме логина и пароля). После этого необходимо ввести свои логин и пароль в соответствующие поля и нажать Отправить. Далее будет совершен переход на форму работы с базой данных.

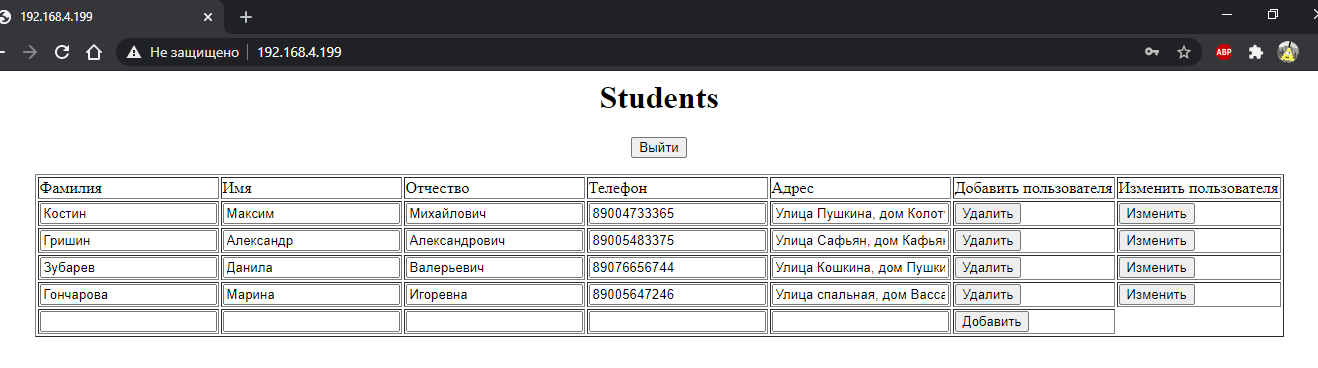


Рисунок 3 - форма администрирования БД

Добавление, изменение, удаление данных из БД:

Для администрирования базы данных предусмотрена форма, на которой выдана таблица с которой происходит работа. В ней имеется следующий функционал для работы с данными:

* Добавить – добавление данных в отдельную запись в таблицу;
* Изменить – изменения данных, в уже созданной записи;
* Удаление – удаление записи.

Для добавления новой записи, необходимо ввести в самую нижнюю строку нужные нам данные и нажать кнопку Добавить. Форма обновиться и в таблице будет отображена новая запись.

Для изменения существующей записи необходимо выбрать тип данных, что нам нужно изменить, ввести новое значение и нажать кнопку Изменить. Форма обновиться и в таблице будут отображены новые данные.

Для удаления записи, необходимо выбрать нужную нам запись и нажать кнопку Удалить.

**Технические проблемы, возникающие в процессе эксплуатации баз данных**

Какие техническое проблемы могут возникать при установки, настройки и работе базы данных

**Администрирование отдельных компонент серверов**

Как происходит установка, настройка и процесс эксплуатации Asterisk и FreePBX

**Разработка политики безопасности SQL сервера, базы данных и отдельных объектов базы данных**

Системы безопасности SQL Server используют для поддержания и контроля защиты два основных компонента: пользователей, учётные записи. Проверка безопасности осуществляется на двух уровнях:

1. Идентификация пользователя согласно введенному логину и паролю. В случае подтверждения аутентификации пользователю становится доступным подключение к SQL Server. Однако это никак не связано с получением доступа непосредственно к базам данных.
2. Проверка на уровне базы данных. Авторизованные ранее пользователи и получившие доступ к серверу лица получают доступ к соответствующей базе данных. Это происходит на основании прав пользователя. Права доступа к БД могут носить общий или фиксированный тип, или быть никак не связанными с самими правами пользователя. То же самое касается приложений, которые получают права доступа: они связаны с пользователем и его персональными правами.

Платформа для SQL Server включает в себя физическое оборудование и сетевые компьютеры, с помощью которых клиенты соединяются с серверами базы данных, а также двоичные файлы, применяемые для обработки запросов базы данных.

Рекомендуется строго ограничивать доступ к физическим серверам и компонентам оборудования. Например, оборудование сервера базы данных и сетевые устройства должны находиться в закрытых охраняемых помещениях. Доступ к резервным носителям также следует ограничить. Для этого их рекомендуется хранить в отдельных охраняемых помещениях.

Реализация физической сетевой безопасности начинается с запрета доступа неавторизованных пользователей к сети.

В состав пакетов обновления и отдельных обновлений для операционной системы входят важные дополнения, позволяющие усилить безопасность. Все обновления для операционной системы необходимо устанавливать только после их тестирования с приложениями базы данных.

Кроме того, эффективную безопасность можно реализовать с помощью брандмауэров. Брандмауэр, распределяющий или ограничивающий сетевой трафик, можно настроить в соответствии с корпоративной политикой информационной безопасности. Использование брандмауэра повышает безопасность на уровне операционной системы, обеспечивая узкую область, на которой можно сосредоточить меры безопасности.

Уменьшение контактной зоны является мерой безопасности, предполагающей остановку или отключение неиспользуемых компонентов. Уменьшение контактной зоны повышает уровень безопасности за счет уменьшения числа возможных способов атаковать систему. Важную роль в ограничении контактной зоны SQL Server играет запуск необходимых служб по принципу «минимума прав доступа», согласно которому службам и пользователям предоставляются только необходимые для работы права.

### Безопасность файлов операционной системы SQL Server

SQL Server использует файлы операционной системы для работы и хранения данных. Оптимальным решением для обеспечения безопасности файлов будет ограничение доступа к ним.

С помощью приведенного ниже скрипта можно определить установленный в системе пакет обновления.

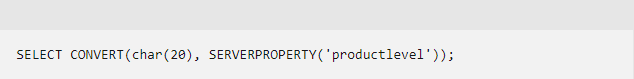


Рисунок 4 – Скрипт

## Безопасность участников и объектов базы данных

Участники — это отдельные пользователи, группы и процессы, которым предоставлен доступ к ресурсам SQL Server. Защищаемые объекты — это сервер, база данных и объекты, которые содержит база данных. У каждого из них существует набор разрешений, с помощью которых можно уменьшить контактную зону SQL Server .

## Роли приложений

Роль приложения – это объект базы данных (такой же, как и обычная роль базы данных), который позволяет с помощью аутентификации через пароль менять контекст безопасности в базе данных. В отличие от ролей баз данных, роли приложений по умолчанию находятся в неактивном состоянии и активируются, когда приложение выполняет процедуру sp\_setapprole и вводит соответствующий пароль.

В отличие от обычных ролей, роли приложений практически никогда не используются. Как исключение, их применение можно найти в multi-layer приложениях.

## Фильтрация данных в SQL Server

Фильтрация данных в SQL Server через хранимые процедур/представления/функции можно отнести к реализации принципу наименьших привилегий, так как вы предоставляете доступ не ко всем данным в таблице, а лишь к некоторой их части.

Например, можно предоставить пользователю права только на SELECT из представления и запретить прямой доступ к таблицам, которые используются в представлении. Таким образом вы предоставите доступ только к части данных из таблицы, задав фильтр where в представлении.

### Фильтрация данных через Row-Level Security

**Безопасность на уровне строк**или**Row-Level Security (RLS)** позволяет фильтровать данные таблицы для разных пользователей по настраиваемому фильтру. Это осуществляется через SECURITY POLICY в T-SQL

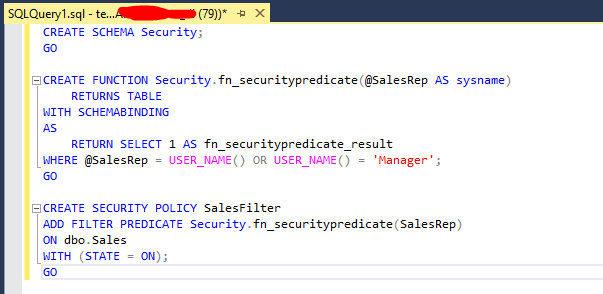


Рисунок 4 - SECURITY POLICY в T-SQL

На данном скриншоте политика настраивается таким образом, что пользователь Sales1 будет видеть строки таблицы, в которых значение столбца Sales равняется имени пользователя (Sales1), а пользователь Manager будет видеть все строки.

## Шифрование данных средствами SQL Server

Шифрование данных это одна из важных мер обеспечения безопасности, но шифрование может быть требовательно к ресурсам сервера и иногда может быть лишним.

SQL Server может шифровать данные, процедуры и соединения с сервером. Шифрование возможно с использованием сертификата, асимметричного или симметричного ключа. В SQL Server используется иерархичная модель шифрования, то есть каждый слой иерархии шифрует слой под ним. Поддерживаются все известные и популярные алгоритмы шифрования. Для реализации алгоритмов шифрования используется Windows Crypto API.

Самыми распространенными типами шифрования являются TDE (Прозрачное шифрование данных) и Always Encrypted.

### Прозрачное шифрование данных

**Прозрачное шифрование данных**или**Transparent Data Encryption** шифрует всю базу целиком. При краже физического носителя или .mdf/.ldf файла, злоумышленник не сможет получить доступ к информации в базе данных.

Диаграмма, для того чтобы представить весь процесс

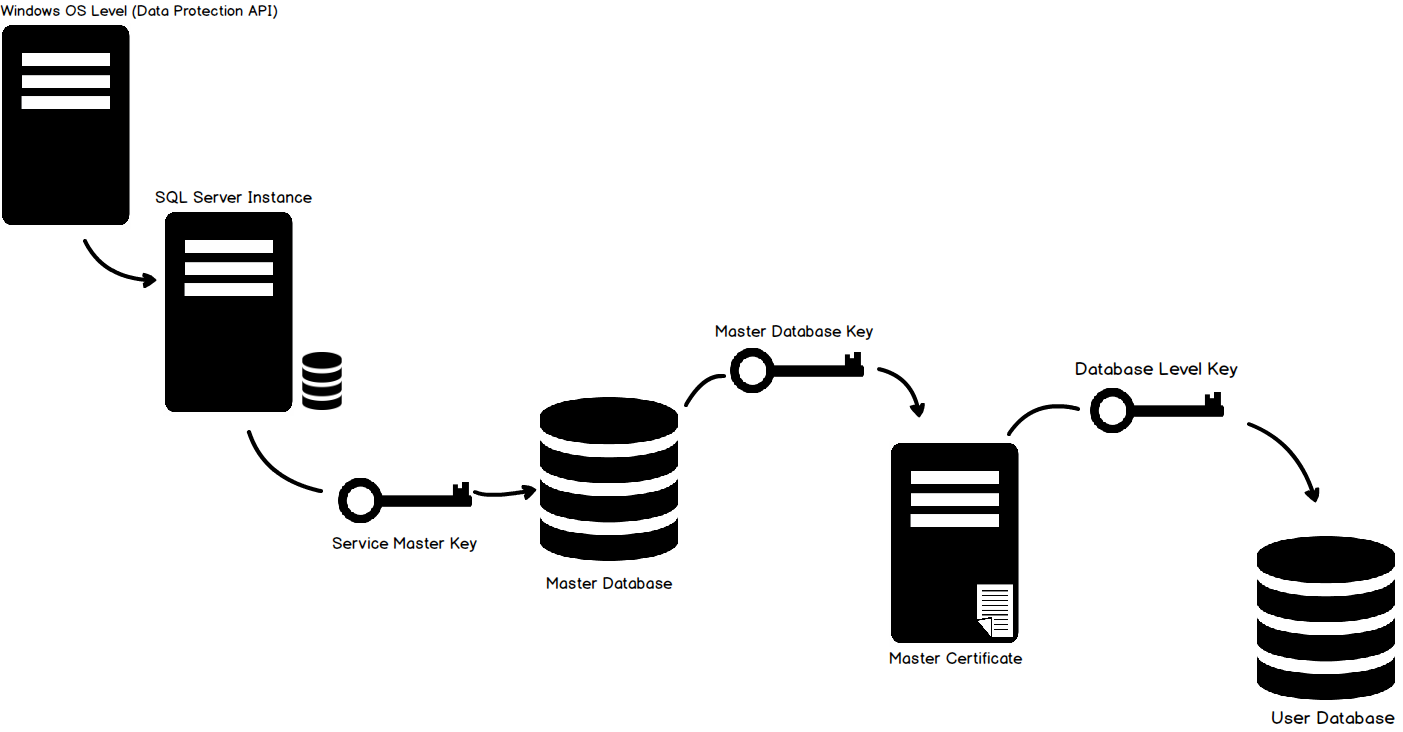


Рисунок 5 – Диаграмма баз данных

Базовое шифрование базы данных через T-SQL:

USE master;

GO

CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'password';

go

CREATE CERTIFICATE ServerCert WITH SUBJECT = 'DEK Certificate';

go

USE AdventureWorks2012;

GO

CREATE DATABASE ENCRYPTION KEY

WITH ALGORITHM = AES\_128

ENCRYPTION BY SERVER CERTIFICATE ServerCert;

GO

ALTER DATABASE AdventureWorks2012

SET ENCRYPTION ON;

GO

Если пользователи обращаются к данным через общедоступную сеть, то для обеспечения безопасности может потребоваться шифрование, но если данные передаются по защищенной интрасети или ВПН, то необходимости в шифровании данных нет. Так же стоит рассмотреть возможность шифрования данных, если есть угроза кражи физического носителя с базами данных.

Внедрение шифрования должно быть хорошо спланировано: нужно учесть дополнительную нагрузку на сервер, могут ли приложения, которые работают с вашим сервером внедрить поддержку шифрования данного типа на своей стороне и многие другие нюансы.

**Групповые управляемые учетные записи службы**или[**gMSA**](https://winitpro.ru/index.php/2014/03/28/group-managed-service-accounts-v-windows-server-2012/)– это специальная учетная запись, которая автоматически управляется Active Directory. gMSA это развитие технологии MSA, так как MSA было невозможно использовать в кластерных сценариях.

gMSA исключает необходимость вручную менять пароли для учетной записи. При настройке gMSA вы указываете на каких серверах будет работать gMSA аккаунт, как часто Active Directory будет менять пароль, и кто имеет право на просмотр пароля. На серверах, на которых будет установлен gMSA не нужно указывать пароль при указании соответствующей учетной записи gMSA.

В SQL Server Management Studio есть функция оценки уязвимостей для базы данных.

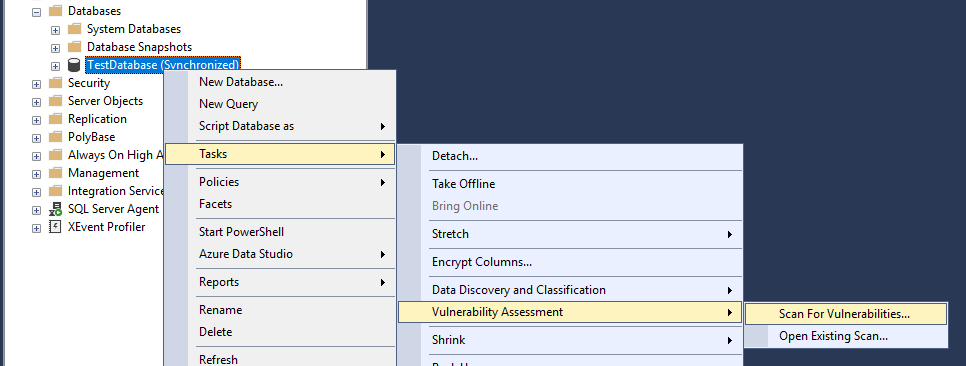


Рисунок 6 – **Tasks -> Vulnerability Assessment -> Scan For Vulnerabilities.**

.

**Проверка наличия сертификатов на информационную систему или**

**бизнес-приложения**

Сертификация - процедура, посредством которой третья сторона письменно удостоверяет, что продукция, процесс или услуга соответствуют заданным требованиям.

Сертификация программы — процедура, выполняемая третьей стороной, независимой от изготовителя (продавца) и потребителя программной продукции, по подтверждению соответствия определенной программы или программного комплекса установленным требованиям. Требования могут быть зафиксированы в стандарте или другом документе. В некоторых случаях сертификация проводится на соответствие требований, заявленных изготовителем программы или программного комплекса. Результатом выполнения процедуры сертификации является так называемый сертификат соответствия.

Сертификат соответствия — документ, выданный по правилам системы сертификации для подтверждения соответствия сертифицированной продукции установленным требованиям.

Сертификация программных средств и систем является элементом общей системы сертификации продукции в Российской Федерации.

Система сертификации — система, располагающая собственными правилами процедуры и управления для проведения сертификации.

Орган по сертификации — орган, проводящий сертификацию соответствия. Орган по сертификации может сам проводить испытания или же осуществлять надзор за этой деятельностью, проводимой по его поручению другими органами.

Испытательная лаборатория — лаборатория (центр), который проводит испытания в процессе сертификации.

Аккредитация (испытательной лаборатории или органа по сертификации) — процедура, посредством которой уполномоченный в соответствии с законодательными актами РФ орган официально признает возможность выполнения испытательной лабораторией или органом по сертификации конкретных работ в заявленной области.

Знак соответствия (в области сертификации) — защищенный в установленном порядке знак, применяемый или выданный в соответствии с правилами системы сертификации, указывающий, что обеспечивается необходимая уверенность в том, что данная продукция, процесс или услуга соответствуют конкретному стандарту или другому нормативному документу.

Технические условия (ТУ) — документ, устанавливающий технические требования, которым должна удовлетворять продукция, процесс или услуга. ТУ могут быть стандартом, частью стандарта или самостоятельным документом.

Организационная структура системы сертификации в России включает: государственный (национальный) орган по сертификации, ведомственные органы по управлению сертификацией продукции определенных классов, а также испытательные центры (лаборатории).

Вся деятельность по сертификации базируется на законодательстве Российской Федерации и принятых на его основе постановлений и других нормативных документов, регулирующих все аспекты деятельности в этой сфере.

В Российской Федерации принят ряд основополагающих законов, которые в разной степени призваны регулировать работы по сертификации в сфере информатизации:

Закон "О защите прав потребителей" - устанавливает обязательную сертификацию по требованиям безопасности всей продукции, продаваемой на территории РФ для личных нужд потребителя.

Закон "О поставках продукции для федеральных государственных нужд" устанавливает обязательность требований для продукции, поставляемой по государственному контракту.

Закон "Об информации, информатизации и защите информации", который регулирует отношения, возникающие при формировании и использовании информационных ресурсов и применения информационных технологий .

Закон "О сертификации продукции и услуг" устанавливает права и обязанности участников сертификации. Этим законом установлена обязательная и добровольная сертификация.

Общие правовые основы сертификации продукции и услуг в Российской Федерации установлены Федеральным Законом от 27.12.2002 № 184-ФЗ «О техническом регулировании».

Настоящий Федеральный закон регулирует отношения, возникающие:

* при разработке, принятии, применении и исполнении обязательных требований к продукции, в том числе зданиям и сооружениям (далее — продукция), или к продукции и связанным с требованиями к продукции процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации;
* разработке, принятии, применении и исполнении на добровольной основе требований к продукции, процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг;
* оценке соответствия.

Настоящий Федеральный закон также определяет права и обязанности участников регулируемых настоящим Федеральным законом отношений. В законе указано, что сертификация проводится в целях:

* создания условий для деятельности предприятий, учреждений, организаций и предпринимателей на едином товарном рынке РФ, а также для участия в международном экономическом, научно-техническом сотрудничестве и международной торговле;
* содействия потребителям в компетентном выборе продукции;
* защиты потребителя от недобросовестности изготовителя (продавца, исполнителя);
* контроля безопасности продукции для окружающей среды, жизни, здоровья и имущества;
* подтверждения показателей качества продукции, заявленных изготовителем.

Для созданной информационной системы использовались различные программы, приложения, позволяющие создать полноценную среду функционирования для информационной системы. Для работы с данным программным обеспечением необходимо принять различные условия лицензии, в зависимости от типа ПО. Для создания информационной системы использовалось следующие программное обеспечение (с указанием лицензий):

* Windows 10 (Соглашении Microsoft для сборщика, Условия лицензионного соглашения на использование программного обеспечения microsoft);
* CentOS 7 (CentOS 7 Linux EULA, GNU General Public License);
* Samba (GNU Lesser General Public License v3, GNU General Public License v3);
* MariaDB (GNU Lesser General Public License v3, GNU General Public License v3);
* PHP (PHP license);
* PhpMyAdmin (PHP license);
* Apache (Apache License, GNU General Public License v3);
* Oracle VM VirtualBox (GNU General Public License v2);

**ФОТООТЧЁТ**

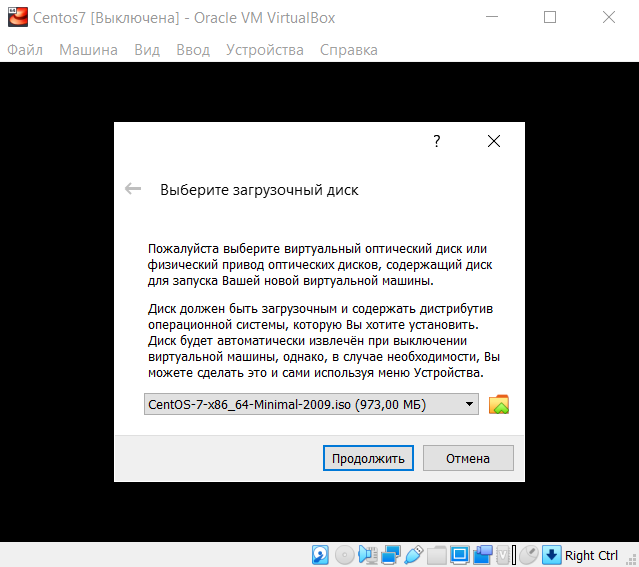


Рисунок 8 - установка CentOs7 на VirtualBox

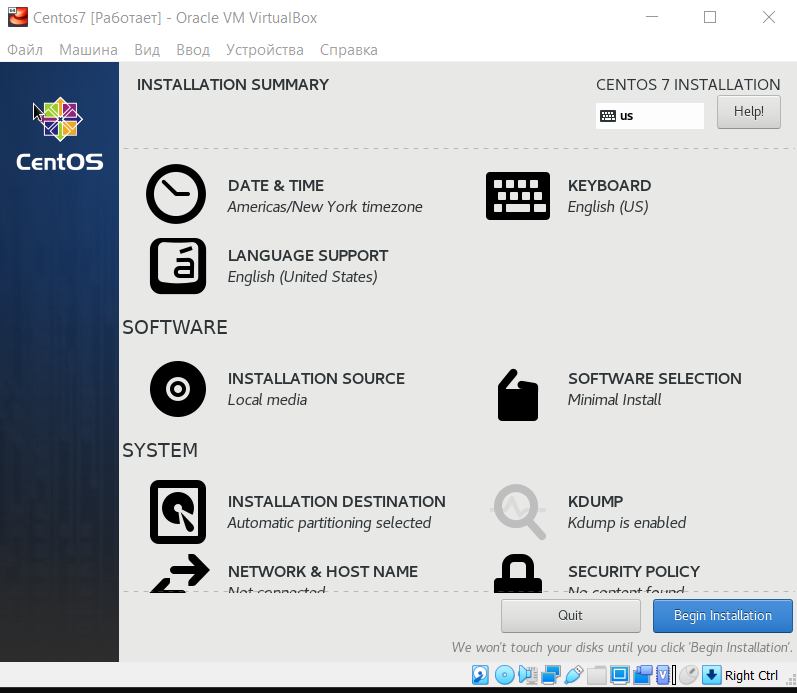


Рисунок 9 - настройка установки CentOs7 на VirtualBox

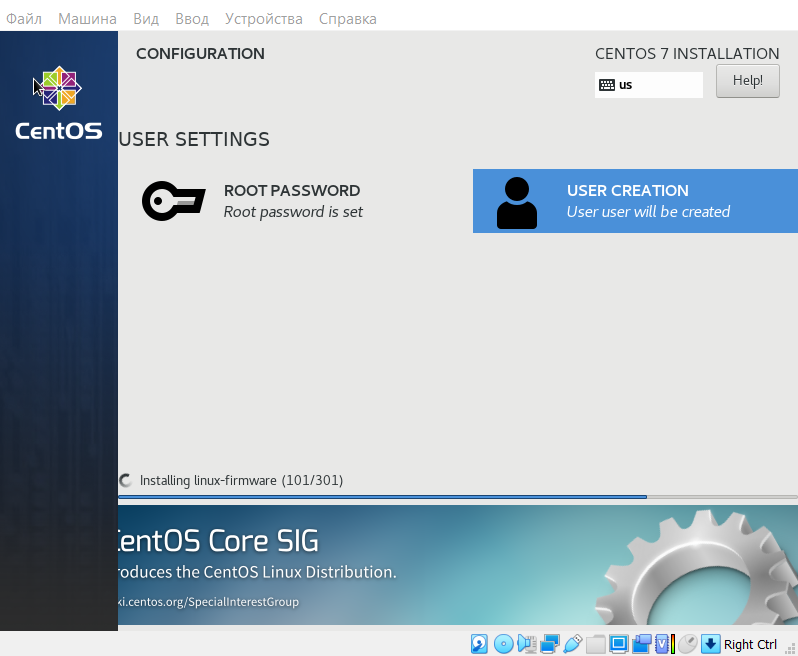


Рисунок 10 - создание пользователя



Рисунок 11 - добавление репозитория на установку MariaDB

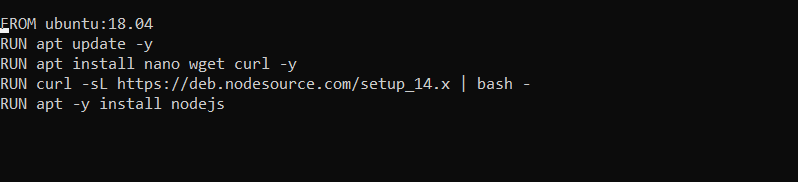


Рисунок 12 - содержимое файла dockerfile

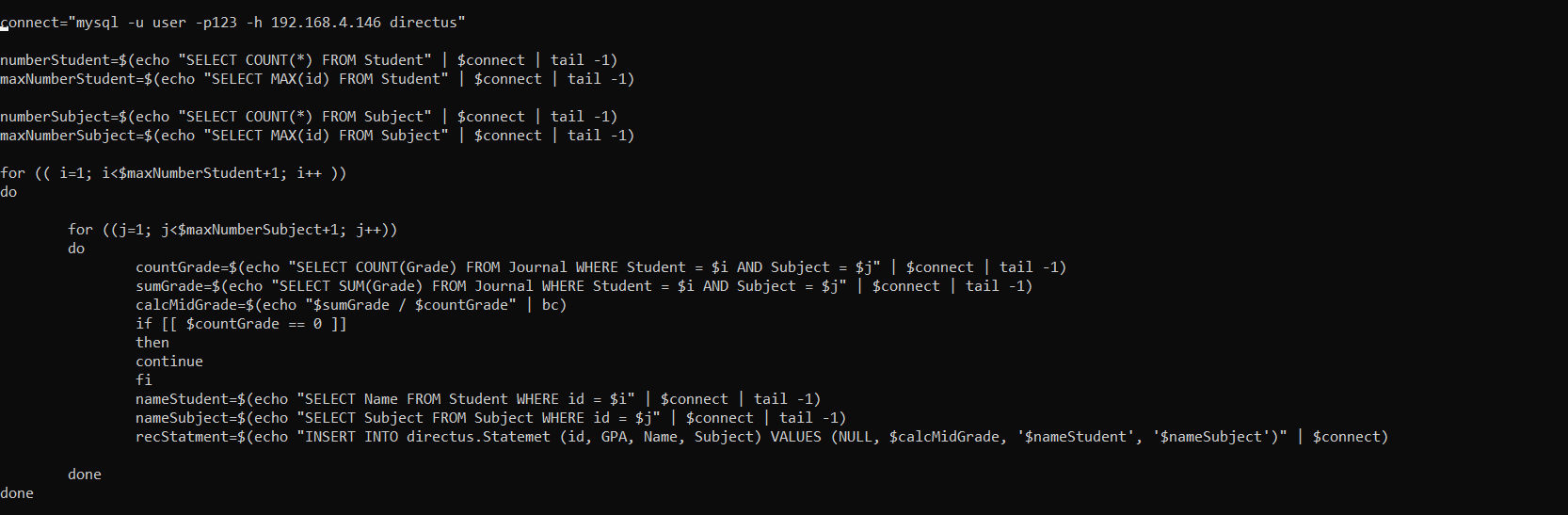


Рисунок 13 - запрос на расчет средней оценки среди учеников

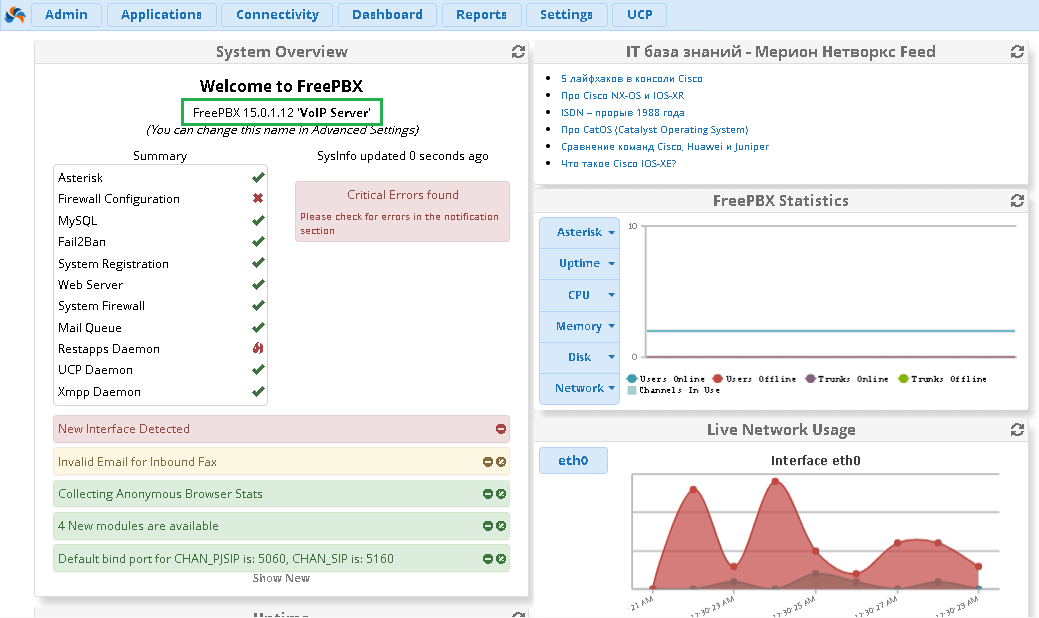


Рисунок 14 – главная страница FreePBX16

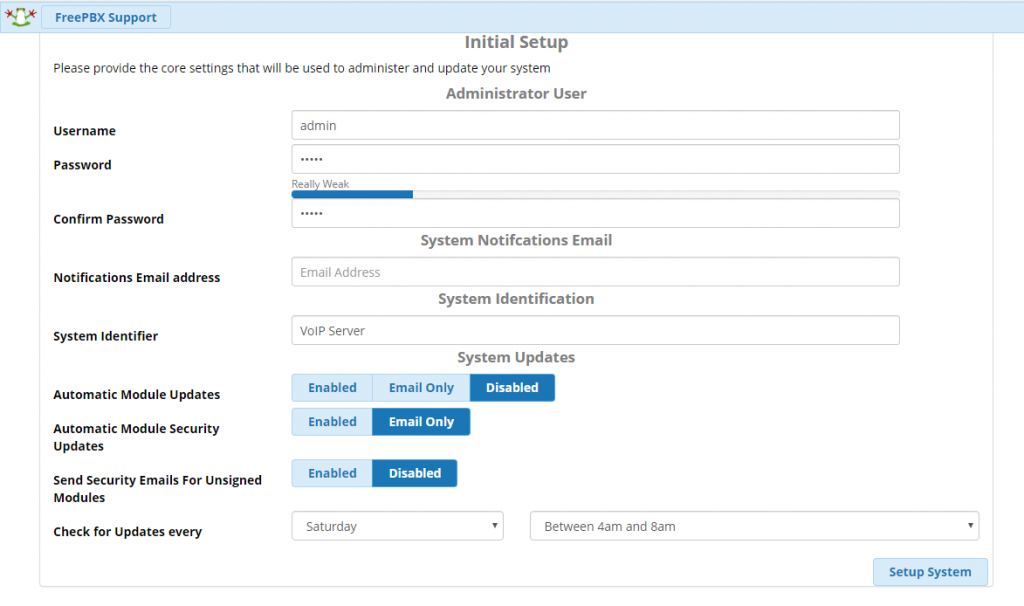


Рисунок 15 – Настройка аккаунта FreePBX16

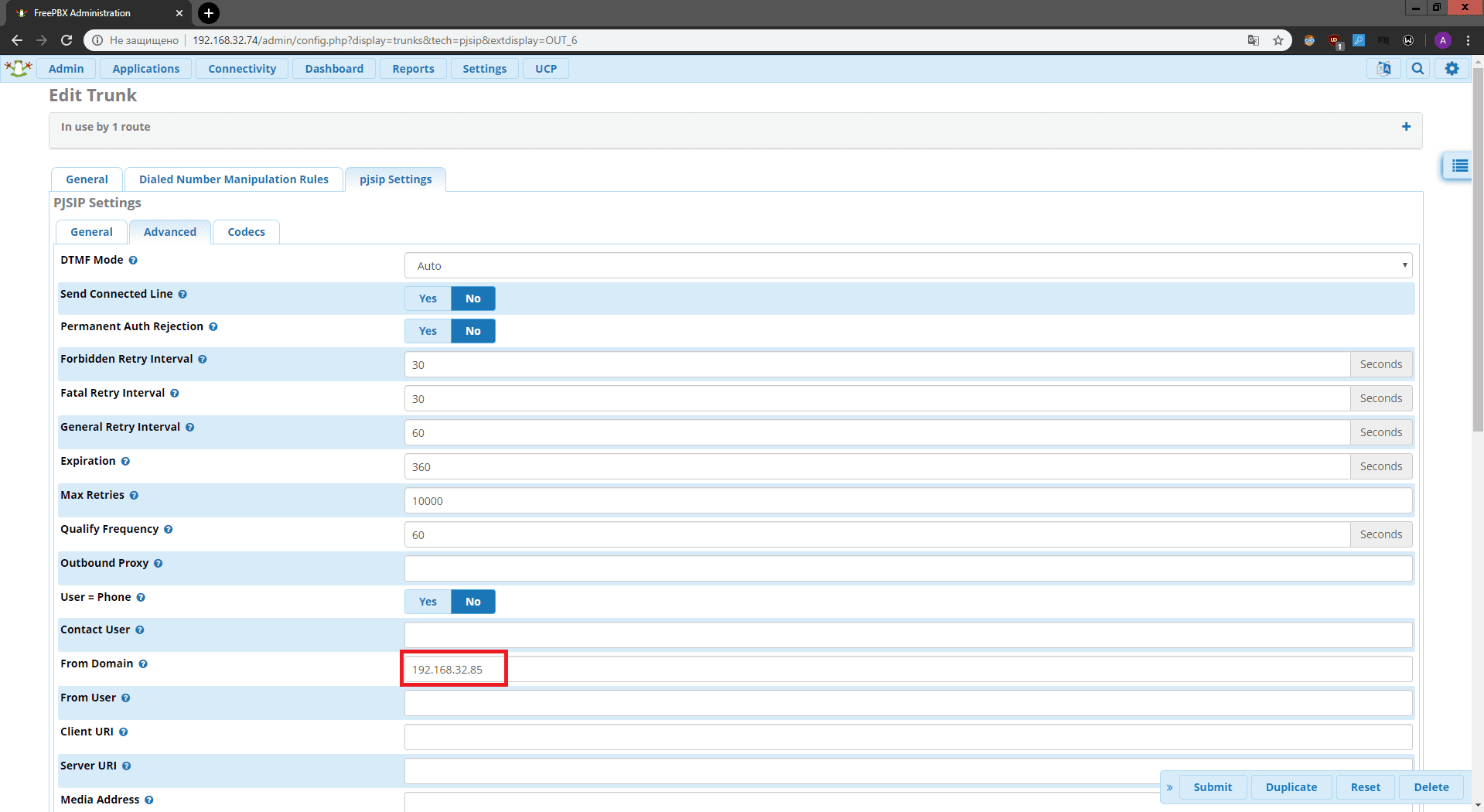


Рисунок 16 – Добавление номера в FreePPX16