**СОДЕРЖАНИЕ**

1 Описание предприятия…………………………….……………………………6

2 Структура и характер деятельности предприятия………………..……………8

3 Правила внутреннего распорядка предприятия ………………………………9

4 Основные положения должностной инструкции специалиста по информационным системам……………………………………………………………………..….10

5 Описание ПО…………………………………………………………………...12

6 Инструкция по технике безопасности при выполнении работ специалиста по обслуживанию телекоммуникаций……………………………………………………22

7 Выполнение индивидуального задания……………………………………...23

8 Фотографии рабочего места…………………………………………………..27

**1 Описание предприятия**

ГК «Решения» — один из крупнейших системных интеграторов Поволжья, который специализируется на решениях в области информационной безопасности, автоматизации бизнес-процессов и управления ИТ-активами. За более 10-ти лет работы на ИТ-рынке мы расширили свой продуктовый портфель до 300+ поставщиков в сфере софта, компьютерного и тепловизионного оборудования, систем противопожарной безопасности, охранной сигнализации и видеонаблюдения, СКУД, СХД и прочего.

В последние два года мы уделяем особое внимание теме импортозамещения. Мы имеем тесные партнерские отношения с такими производителями, как Лаборатория Касперского, Dr.Web, InfoWatch, SerchInform, Группа Астра, Кейсистемс-Безопасность, РАМЭК, KarneevSystems, ContentAi, AKVIS, Роса и многими другими.

На сегодняшний день IT-технологии могут значительно помочь развитию практически любого бизнеса. Однако до сих пор немного компаний, которые могут похвастаться реальными результатами внедрения не одного, а нескольких IT-решений и тем более — комплексным подходом к развитию IT-структуры компании.

Отличительной особенностью является то, что специалисты ГК «Решения» имеют именные сертификаты и умеют грамотно «собирать ИТ-пазлы», причем делать это в сжатые сроки. Мы можем сочетать ПО и оборудование разных разработчиков, как отечественных, так и «дружественных», в пределах одного ТЗ, подбирать «с нуля» или же заменять конкретные позиции под индивидуальный запрос заказчика - будь то дело вкуса или бюджета, или же требования одного из законов РФ.

ГК «Решения» работает с корпоративными заказчиками уровня Enterprise, крупным, средним бизнесом, а также госсектором. Среди них ОЭЗ «Алабуга», ПАО «КАМАЗ», «ПАО «Татнефть», ПАО «Таттелеком», КБЭР «Банк Казани», АО «Татэнерго», ПАО «АК БАРС» Банк, ПАО «УРАЛСИБ» Банк, ФГАОУ ВО К(П)ФУ, КНИТУ КАИ, АО «Морской торговый порт «Ванино» и многие другие.

ГК «Решения» — инновационная, динамично развивающаяся компания на рынке IT-технологий, стремящаяся обеспечить бесперебойную работу всех IT-систем своих партнеров.

Мы поставили себе задачу: сделать сложные вещи простыми. Мы понимаем, что для многих людей компьютер, сервер и база данных — это сложные механизмы, не говоря о таких вещах, как их безопасность, взаимодействие и производительность. Поэтому мы стремимся решать задачи автоматизации бизнеса, предлагая оптимальные решения и внедряя их в жизнь.

**2 Структура и характер деятельности предприятия**

Группа компаний Neosoft представляет собой интегратора ИТ-решений и услуг, предлагающего широкий спектр услуг в различных областях.

Структура компании:

1 Разработка программного обеспечения:

- индивидуальные решения;

- веб и мобильные приложения.

- ERP и CRM системы

2. Консалтинг:

- ИТ-консалтинг;

- аудит бизнес-процессов.

3. Инфраструктурные решения:

- настройка серверов и облачных решений;

- поддержка ИТ-инфраструктуры.

4. Образование и обучение:

- курсы и тренинги;

- вебинары по новым технологиям.

Характер деятельности:

- инновационность: постоянное внедрение современных технологий и методов;

- клиентоориентированность: услуги подбираются с учетом потребностей клиентов;

- качество: высокие стандарты качества внедряемых решений и услуг;

- гибкость: возможность адаптации решений под специфические запросы бизнеса.

**3 Правила внутреннего распорядка предприятия**

1. Общие положения:

- все сотрудники обязаны соблюдать правила внутреннего распорядка;

- правила направлены на создание комфортной и продуктивной рабочей атмосферы.

2. Рабочее место:

- сотрудники обязаны поддерживать порядок на своих рабочем местах;

- использование личных устройств должно осуществляться с соблюдением политики безопасности.

3. Коммуникация:

- взаимодействие между сотрудниками должно быть уважительным и конструктивным;

- запрещено использование ненормативной лексики и дискриминационных высказываний.

4. Время отдыха:

- сотрудники имеют право на перерывы в течении рабочего дня;

- курение разрешено только в специально отведенных местах.

5. Дисциплинарные меры:

- нарушение правил влечет за собой дисциплинарные меры, вплоть до увольнения;

- каждый случай рассматривается индивидуально.

6. Порядок увольнения:

- увольнение по инициативе работника осуществляется при предварительном уведомлении за 14 дней;

- увольнение по инициативе работодателя - согласно трудовому законодательству.

Соблюдение данных правил способствует созданию эффективной и гармоничной рабочей среды в компании.

**4 Основные положения должностной инструкции специалиста по информационным системам**

1. Общие положения

- специалист по информационным системам подчиняется непосредственно руководителю отдела информационных технологий;

- на должность назначается лицо с высшим образованием и опытом работы в области информационных технологий.

2. Цели и задачи

- рассмотрение и анализ потребностей бизнеса в автоматизации процессов;

- консультирование сотрудников по вопросам использования информационных систем;

- участие в проектировании, внедрении и поддержке ит-решений.

3. Функциональные обязанности

- обеспечение бесперебойной работы информационных систем компании;

- проведение обучающих мероприятий для сотрудников по работе с программным обеспечением;

- мониторинг и анализ технических проблем, разработка предложений по их устранению;

- иметь доступ к необходимым ресурсам и системам для выполнения своих обязанностей;

- вносить предложения по улучшению работы информационных систем;

- запрашивать необходимую информацию и помощь от других подразделений.

4. Ответственность

- ответственность за корректную работу информационных систем;

- своевременное выполнение поставленных задач и проектов;

- соблюдение конфиденциальности в отношении данных компании.

5. Взаимодействие

- взаимодействие с другими подразделениями для определения требований и пожеланий к информационным системам;

- сотрудничество с внешними поставщиками и подрядчиками при реализации проектов.

Данная инструкция устанавливает основные функции и требования к специалисту по информационным системам, обеспечивая эффективную работу и развитие информационных технологий в компании.

**5 Описание ПО**

**5.1 Резервное копирование БД. Восстановление БД. Управление доступом к БД.**

Резервное копирование базы данных (БД) - это процесс создания, управления и хранения копий данных на случай их потери или повреждения. Наличие актуальных резервных копий позволяет быстро восстановить работу и минимизировать потери. Также резервные копии БД могут использоваться для переноса информации на другое оборудование, например, в случае миграции сервера.

Дифференциальное резервное копирование сохраняет только изменения, произошедшие с момента последнего полного резервного копирования. Это позволяет сократить время и объем данных, необходимых для резервного копирования, но требует наличия последней полной копии для восстановления;

Инкрементное резервное копирование сохраняет только изменения, произошедшие с момента последнего резервного копирования любого типа (полного, дифференциального или инкрементного). Этот метод позволяет значительно сократить объем данных для резервного копирования, но процесс восстановления может быть более сложным и длительным.

Восстановление базы данных (БД) - процесс, который помогает вернуть потерянные данные из-за сбоев системы, ошибок транзакций, вирусов и других причин.

Некоторые методы восстановления БД:

- Метод отката/отмены. Основан на отмене последствий транзакции, которая не была успешно завершена из-за системного сбоя или ошибки. Для этого используют записи журнала транзакций, которые содержат информацию обо всех операциях в базе данных.

- Метод восстановления фиксации/повтора. Основан на повторном применении изменений, которые были внесены успешно завершённой транзакцией. Для этого также используют записи журнала транзакций.

Управление доступом к базе данных (БД) - один из методов организации защиты БД от различных инцидентов в сфере информационной безопасности.

Некоторые методы управления доступом:

Управление доступом к базе данных (БД) - один из методов организации защиты БД от различных инцидентов в сфере информационной безопасности.

Некоторые методы управления доступом:

- Права доступа на уровне базы данных. Программист или администратор базы данных могут управлять уровнями доступа, чтобы пользователи могли получить доступ только к определённым частям базы данных.

**5.2. Установка и настройка ПО для обеспечения работы пользователей с БД. Установка и настройка ПО для администрирования БД. Мониторинг событий, возникающих в процессе работы БД. Протоколирование событий, возникающих в процессе работы БД.**

Установка и настройка ПО для обеспечения работы пользователей с БД – это процесс, который включает в себя несколько ключевых этапов, направленных на предоставление пользователям доступной и эффективной инфраструктуры для работы с базами данных. Основные аспекты этого процесса:

- Выбор СУБД: Определение, какая система управления базами данных (СУБД) подойдет для решения конкретных задач (например, PostgreSQL, MySQL, Oracle и др.).

- Установка серверного ПО: Процесс инсталляции СУБД на сервер, включая соответствующие настройки для гарантии работоспособности.

- Настройка подключения: Конфигурация файлов и параметров, таких как порты, параметры подключения и IP-адреса, с целью обеспечить корректный доступ к базе данных.

Администрирование баз данных (БД) - это процесс управления и поддержания баз данных для обеспечения их бесперебойной работы, безопасности и производительности. В современном мире данные являются ключевым ресурсом, и эффективное управление ими становится критически важным для успеха любой организации.

Мониторинг событий, возникающих в процессе работы БД - это постоянное отслеживание состояния базы данных: нагрузки на сервер, выполнения запросов, ошибок, блокировок и других критических событий.

Протоколирование событий, возникающих в процессе работы БД - это запись логов (журналов) всех значимых действий и изменений в базе данных: кто и когда подключился, какие запросы выполнял, какие ошибки возникали.

**5.3 Выполнение регламентов техническому сопровождению облачного хранения данных**

Выполнение регламентов техническому сопровождению облачного хранения данных - это набор действий и процедур, направленных на обеспечение бесперебойной работы облачных сервисов хранения данных. Основные аспекты включают:

- мониторинг системы: Регулярное отслеживание состояния облачного хранилища, включая доступность, производительность и использование ресурсов. Использование инструментов аналитики для выявления отклонений от норм;

- управление доступом: Контроль за уровнями доступа пользователей к данным, реализация политик безопасности для защиты конфиденциальной информации.

**5.4 Обеспечение безопасности хранения данных на платформе провайдера**

Безопасность данных в облачных системах является ключевым аспектом, который требует внимания на нескольких уровнях. Рассмотрим основные меры по обеспечению безопасности:

- шифрование данных: Использование технологий шифрования для защиты данных как в покое, так и в процессе передачи. Это помогает предотвратить доступ к данным третьих лиц.

- управление доступом: Внедрение строгих политик контроля доступа. Использование многофакторной аутентификации для повышения защиты учетных записей пользователей.

- регулярные обновления: Обеспечение своевременного обновления программного обеспечения и систем безопасности, чтобы устранить уязвимости и защитить от новых угроз.

**5.5 Организация аудита облачного хранения данных на платформе провайдера**

Организация аудита облачного хранения данных на платформе провайдера включает проведение систематической проверки и анализа процессов управления, безопасности и целостности данных. В рамках аудита осуществляются оценка соответствия текущих практик установленным стандартам и нормативам, а также выявление уязвимых мест и потенциальных рисков. При этом проверяется конфигурация систем, управление доступом, ведение журналов событий и протоколирование операций, что позволяет отслеживать активность пользователей и системных процессов. Важной задачей является оценка эффективности мер по обеспечению безопасности хранения данных и соответствия требованиям защиты информации.

**5.6 Организация резервного копирования информации и облачной инфраструктуры**

Организация резервного копирования информации и облачной инфраструктуры включает разработку и реализацию комплексной политики по созданию копий данных с целью обеспечения их сохранности и возможности восстановления в случае сбоя, аварийных ситуаций или утраты информации. В рамках этого процесса определяются цели и требования к резервному копированию, включая частоту создания копий, объем данных и их хранение на различных носителях или в разных географических регионах. Настраиваются автоматизированные системы для регулярного выполнения резервных копий, а также реализуются процедуры тестирования их целостности и возможности восстановления. Важной составляющей является управление доступом к резервным копиям, обеспечение их защищенности от несанкционированного доступа и повреждения.

**5.7 Обеспечение конфиденциальности персональных данных при облачном хранении данных**

Обеспечение конфиденциальности персональных данных при облачном хранении включает применение комплексных мер по защите информации от несанкционированного доступа, раскрытия и использования. Для этого используют методы шифрования данных как в процессе передачи, так и при хранении, а также реализуют строгие политики управления доступом, ограничивая право просмотра и обработки данных только авторизованным пользователям. Помимо этого, применяются системы аутентификации и многофакторной проверки личности, что обеспечивает дополнительный уровень защиты. Регулярный мониторинг и аудит доступа помогают своевременно обнаруживать попытки нарушения конфиденциальности, а создание резервных копий и их защита предотвращают потерю данных.

**5.8 Участие в предоставлении услуг для мобильных платформ на платформе провайдера**

Участие в предоставлении услуг для мобильных платформ на платформе провайдера включает интеграцию облачных решений, обеспечивающих доступ и функционирование мобильных приложений пользователей. Это предполагает настройку инфраструктуры, а также поддержку мобильных решений в части их работы, безопасности и масштабируемости, чтобы обеспечить пользователям надежный и удобный доступ к данным через мобильные устройства.

Провайдер обеспечивает инфраструктурные решения, включая вычислительные мощности, базы данных и сети доставки контента (CDN) для ускорения доставки данных.

Участие в облачном веб-хостинге подразумевает использование инфраструктуры и технологий облачных провайдеров, таких как Google Cloud для размещения и обслуживания веб-сайтов и приложений. В отличие от традиционного хостинга, облачные решения предлагают большую гибкость и масштабируемость: ресурсы, включая серверы, хранилища и сети, автоматически настраиваются в зависимости от нагрузки, что позволяет сайту оставаться стабильным даже при резком увеличении трафика.

Провайдер отвечает за обслуживание физических серверов, безопасность и резервное копирование, в то время как клиент управляет контентом, доменами и настройками через удобную панель.

**5.9 Участие в предоставлении услуг облачного веб-хостинга.**

Облачный веб-хостинг — это услуга размещения сайтов и приложений на распределенных серверах в облаке. В отличие от традиционного хостинга (где сайт хранится на одном физическом сервере), облачный использует виртуализированные ресурсы.

Для предоставления услуг облачного веб-хостинга необходимо добавить новую информационную базу «База сервера» и создать для неё серверную часть.

5.10 Консультирование пользователей в процессе эксплуатации мобильных платформ облачного хранения данных

Консультирование пользователей в процессе эксплуатации мобильных платформ облачного хранения данных включает предоставление профессиональной поддержки и рекомендаций по использованию возможностей облачных решений на мобильных устройствах.

**5.11 Техническое сопровождение информационной системы облачного хранения данных в процессе эксплуатации.**

Техническое сопровождение информационной системы облачного хранения данных в процессе эксплуатации включает мониторинг её функционирования, обеспечение высокой надежности и безопасности системы. Это также предусматривает проведение профилактических мероприятий, настройку и оптимизацию параметров системы для повышения её эффективности, а также предоставление поддержки пользователям для обеспечения бесперебойной работы и быстрого восстановления данных в случае неполадок.

**5.12 Участие в настройках масштабирования СУБД в облачных вычислениях**

Участие в настройках масштабирования СУБД в облачных вычислениях — это процесс увеличения или уменьшения ресурсов базы данных в зависимости от потребностей приложения. Существует два основных подхода к масштабированию: вертикальное и горизонтальное.

Вертикальное масштабирование включает в себя добавление ресурсов (ЦПУ, оперативной памяти) к существующему серверу. Это обычно проще, так как требует минимальных изменений в архитектуре, но имеет пределы по увеличению производительности.

Горизонтальное масштабирование предполагает добавление новых серверов для распределения нагрузки. Это позволяет лучше справляться с увеличением объема данных и запросов, но требует более сложной архитектуры и механизма репликации данных.

Ключевые аспекты настройки масштабирования:

1. Мониторинг данных и производительности базы данных. Используйте инструменты мониторинга, чтобы отслеживать загрузку системы и своевременно реагировать на изменения.

2. Автоматическое масштабирование. Многие облачные платформы предлагают функции автоматического масштабирования, позволяющие настраивать ресурсы в зависимости от текущих потребностей.

3. Репликация и шардирование. Это техники, позволяющие распределять данные между несколькими серверами для улучшения доступности и производительности.

**5.13 Применение возможностей технологии облачных вычислений в разработке мобильных приложений**

Применение облачных вычислений в разработке мобильных приложений открывает широкий спектр возможностей, существенно упрощая процесс разработки и улучшая функциональность приложений. Вот некоторые ключевые аспекты:

Хранение данных

Облачные решения предоставляют возможность безопасного и масштабируемого хранения данных. Разработчики могут использовать облачные базы данных, что позволяет обеспечить надежное хранение и доступ к данным пользователей, снижая затраты на локальное хранилище.

Обработка данных

Облачные вычисления позволяют выполнять тяжелые вычисления на стороне сервера, уменьшая нагрузку на мобильные устройства. Это особенно важно для приложений, требующих обработки больших объемов данных или сложных вычислительных задач.

Работа с API

Облачные решения часто предлагают мощные API, которые упрощают интеграцию с другими сервисами и платформами. Это может включать взаимодействие с платежными системами, социальными сетями и другими внешними ресурсами.

**5.14 Участие в анализе проблем обеспечения безопасности в облачных сервисах**

Изучение вопросов безопасности облачных платформ предполагает обнаружение и экспертизу слабых мест, способных скомпрометировать информацию и функциональность в облаке.

Эксперты изучают устойчивость управления правами доступа, криптографической защиты и системы отслеживания, выявляют вероятные недостатки в параметрах настройки, к примеру, не закрытые коммуникационные каналы или простые пароли, и также производят оценку угроз, связанных с DDoS-атаками и несанкционированным раскрытием информации.

Специалисты рассматривают журналы регистрации и происшествия, связанные с безопасностью, для обнаружения необычной деятельности, такой как незаконные входы в систему, попытки похищения информации или аномальные обращения к интерфейсу API.

Также проводится проверка соответствия облачной структуры общепринятым нормативам (GDPR, ISO 27001) и внутренним регламентам организации.

По итогам проведенного исследования были рекомендованы следующие действия: усиление криптографической защиты, настройка многофакторной идентификации, пересмотр правил доступа и внедрение SIEM-систем для оперативного реагирования на инциденты.

**5.15 Участие в анализе и составлении сведений об эффективности применения в экономике облачных вычислений**

Участие в анализе и составлении данных об эффективности использования облачных вычислений в экономике подразумевает оценку их воздействия на результативность, затраты и бизнес-процессы организаций или отраслей. Специалисты исследуют, каким образом облачные решения позволяют сократить расходы на IT-инфраструктуру, включая экономию на содержании и серверах, ускорить развертывание новых услуг и повысить адаптивность бизнеса.

Приводятся практические примеры, демонстрирующие, как миграция в облако привела к сокращению периодов простоя, улучшила масштабируемость при росте нагрузок и облегчила удаленную работу персонала. Также принимаются во внимание вторичные выгоды, такие как оперативное тестирование гипотез без существенных вложений и доступ к передовым инструментам аналитики и искусственного интеллекта посредством облачных платформ.

На основе собранных данных подготавливаются отчеты и предложения, помогающие компаниям принимать обоснованные решения о внедрении облачных технологий или оптимизации существующих облачных сервисов. Это позволяет бизнесу не только снижать издержки, но и укреплять свои позиции на рынке за счет использования технологических преимуществ.

**6 Инструкция по технике безопасности при выполнении работ специалиста по обслуживанию телекоммуникаций**

1.1 К самостоятельной работе по обслуживанию линейных сооружений связи и абонентских устройств допускаются лица не моложе 18 лет, прошедшие медицинское освидетельствование, вводный инструктаж, первичный инструктаж, обучение и стажировку на рабочем месте, проверку знаний требований охраны труда, имеющие группу по электробезопасности не ниже III и соответствующую квалификацию согласно тарифно-квалификационного справочника.

1.2 Работник обслуживающий линейные сооружения связи и абонентские устройства обязан:

1.2.1 Выполнять только ту работу, которая определена рабочей инструкцией и инструкцией.

1.2.2 Выполнять правила внутреннего трудового распорядка.

1.2.3 Правильно применять средства индивидуальной и коллективной защиты.

1.2.4 Соблюдать требования охраны труда.

1.2.5 Немедленно извещать своего непосредственного или вышестоящего руководителя о любой ситуации, угрожающей жизни и здоровью людей, о каждом несчастном случае, происшедшем на производстве, или об ухудшении состояния своего здоровья, в том числе о появлении признаков острого профессионального заболевания (отравления).

1.2.6 Проходить обучение безопасным методам и приемам выполнения работ и оказанию первой помощи пострадавшим на производстве, инструктаж по охране труда, проверку знаний требований охраны труда.

1.2.7 Проходить обязательные периодические (в течение трудовой деятельности) медицинские осмотры (обследования), а также проходить внеочередные медицинские осмотры (обследования) по направлению работодателя в случаях, предусмотренных Трудовым кодексом и иными федеральными законами.

1.2.8 Уметь оказывать первую помощь пострадавшим от электрического тока и при других несчастных случаях.

**7 выполнение индивидуального задания**

В рамках выполнения индивидуального задания было разработано мобильное приложение, предназначенное для подсчёта и сохранения результатов, а также визуального взаимодействия с пользователем. Разработка производилась в среде 1С:Предприятие, а тестирование проводилось с использованием эмулятора Android Studio.

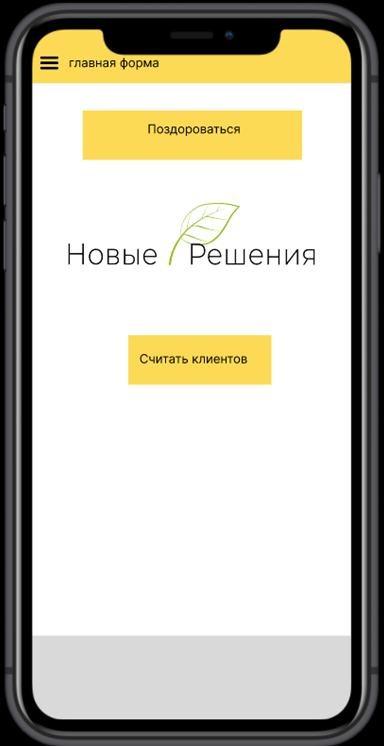


Рисунок 1 – Главный экран

На экране изображено:

- кнопка «Поздороваться», при нажатии на которую отображается приветствие пользователя;

- изображение организации;

- кнопку «Считать клиентов», переходящую ко второму экрану.

Данный экран оформлен в соответствии с требованиями к UX-дизайну и визуальной простоте.

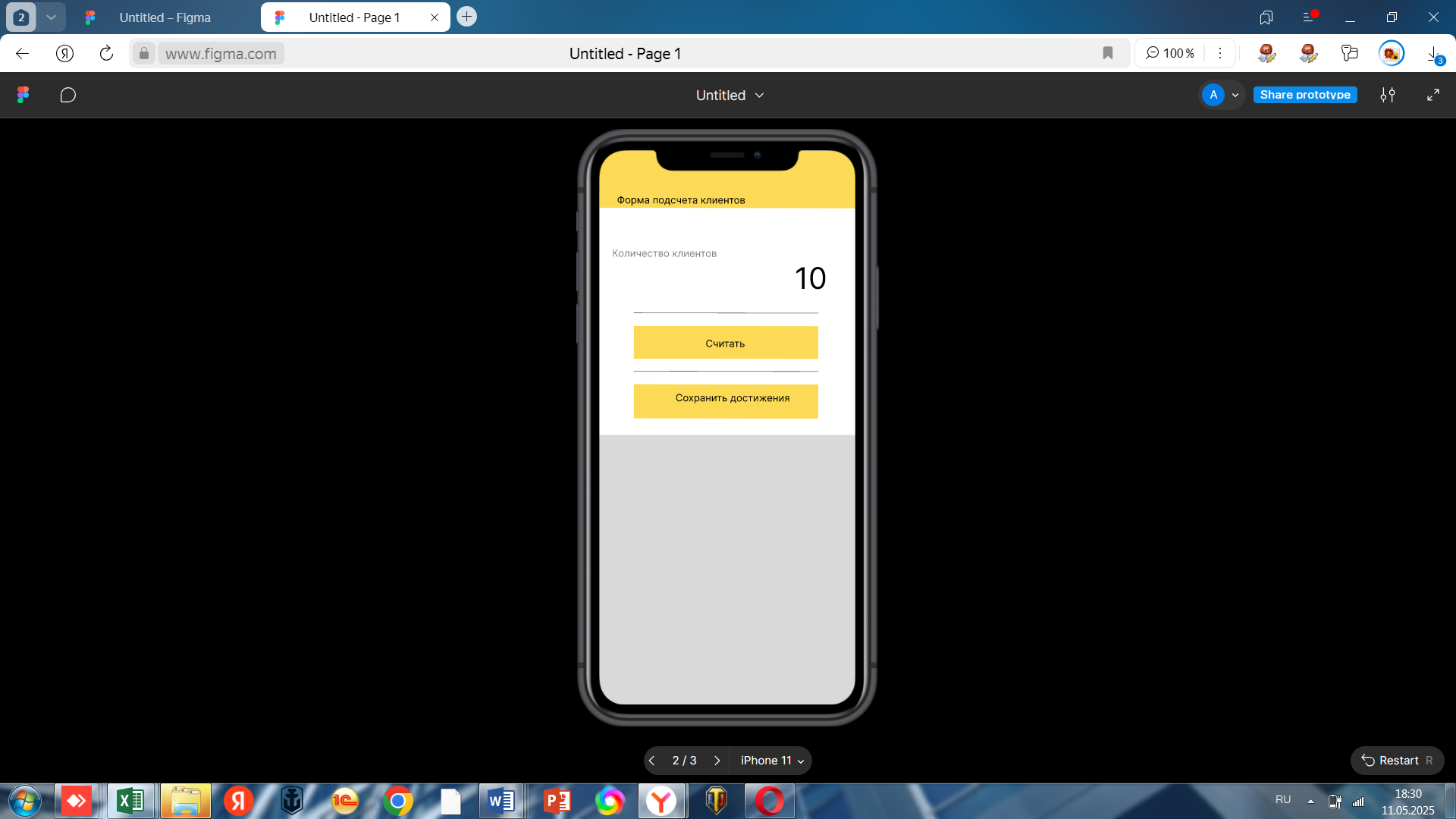


Рисунок 2 - Форма подсчёта

На экране изображено:

- счётчик с текущим значением количества;

- кнопка «Считать» увеличивает значение счётчика;

- кнопка «Сохранить достижения» сохраняет данные, введённые пользователем.

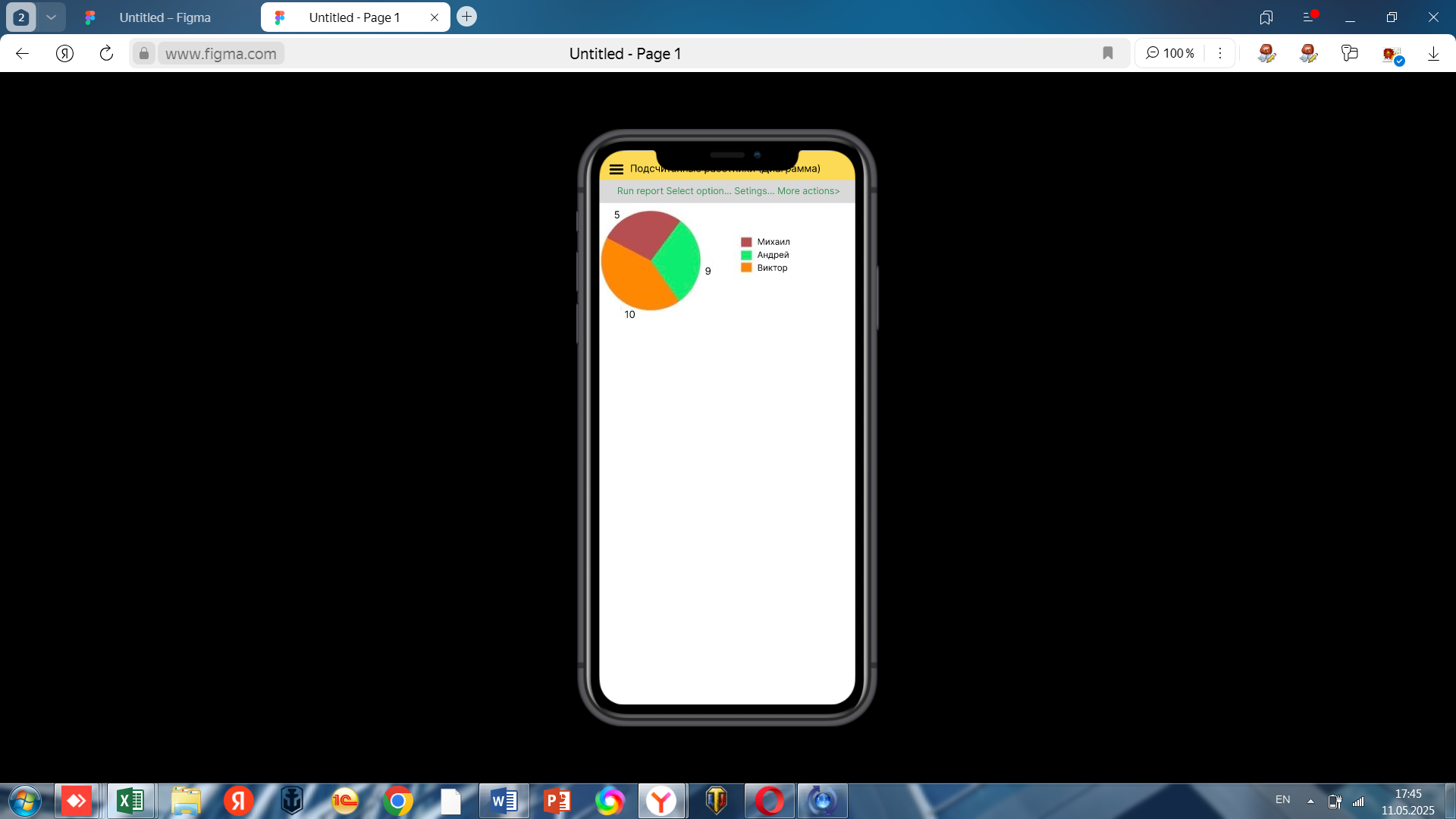


Рисунок 3 – Достижения

На экране «Достижения»:

- круговая диаграмма с результатами счета;

- участники счета;

- количество чисел в счете.

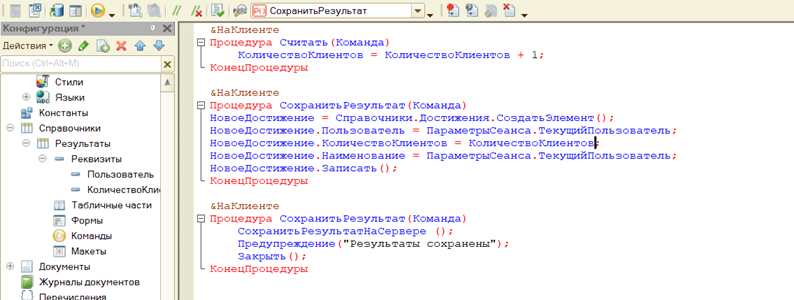


Рисунок 4 – Код счета

Была выполнена проверка работоспособности всех элементов управления. Интерфейс корректно отобразился на эмуляторе Android Studio, ошибки в процессе тестирования не были выявлены.

Ссылка на GitNub:

**8 Фотографии рабочего места**

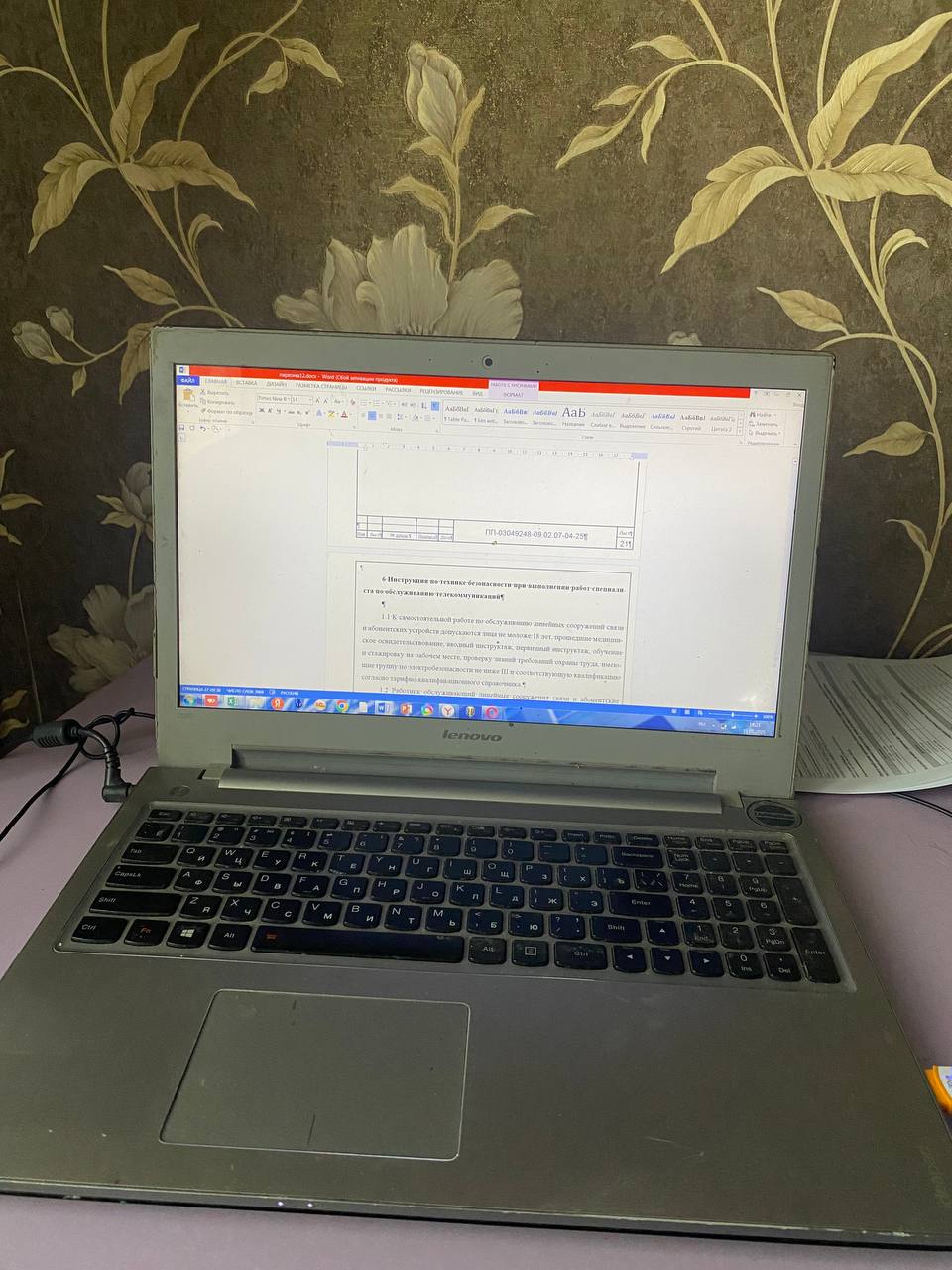


Рисунок 5 - Фото рабочего места

**ОТЧЕТ**

Я, Власова Анастасия Евгеньевна, проходила производственную практику с 16.12.2024 по 23.12.2024 в ГБПОУ РМ «Саранском электромеханическом колледже». За время прохождения практики мною были выполнены следующие задания:

1 Описала предприятие

2 Описала структуру и характер деятельности предприятия

3 Провела внутренний распорядок предприятия

4 Описала основные положения должностной инструкции специалиста по информационным системам

5 Описала инспектирование компонентов ПО на предмет соответствия стандартам кодирования

6 Описала инструкцию по технике безопасности