Содержание

|  |  |
| --- | --- |
| Введение | 2 |
| 1 Краткая характеристика предприятия МКУ «Электронный Краснодар» | 3 |
| 2 Организационная структура предприятия | 8 |
| 3 Должностные обязанности практиканта в должности разработчик прикладного ПО | 9 |
| 4 Индивидуальное задание | 12 |
| 5 Техника безопасности | 14 |
| Заключение | 15 |
| Список источников | 16 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Введение

Производственная практика – это неотъемлемая часть учебного процесса студента, которая позволяет приобрести практические навыки и опыт работы в профессиональной среде. Целью производственной практики является получение практического опыта и знаний в выбранной сфере деятельности, а также расширение профессиональных знаний и умений студента.

Данная практика проводится в организациях, в которых студент может наблюдать и участвовать в процессе производства, приобретать опыт работы в команде и улучшать свои навыки в области своей будущей профессии.

Прохождение производственной практики имеет большое значение в учебном процессе, так как позволяет связать теоретические знания, полученные на учебных занятиях, с практической деятельностью. Это помогает студентам лучше понимать свою будущую профессию, определять свои профессиональные цели и задачи, а также развивать свои личностные качества и навыки.

В процессе прохождения производственной практики студенты сталкиваются с рядом задач, которые необходимо выполнить.

К ним относятся:

1. изучение основных принципов организации работы предприятия;
2. ознакомление с правилами техники безопасности;
3. выполнение задач, связанных с производством продукции;
4. участие в различных проектах и заданиях, выполняемых на предприятии.

Таким образом, производственная практика является важным этапом в профессиональной подготовке студента. Она позволяет студентам приобрести опыт работы в реальной среде, развивать свои профессиональные и личностные качества, а также улучшить свои навыки в выбранной сфере работы.

2 Краткая характеристика предприятия МКУ «Электронный Краснодар»

Основными целями и видами деятельности Казённого учреждения являются:

1. Выполнение работ по повышению эффективности инфор­мационного обеспечения органов местного самоуправления муниципального образования город Краснодар и муниципальных учреждений.
2. Выполнение работ по исполнению скоординированной единой политики информатизации в Администрации и городской Думе Краснодара.
3. Выполнение работ в рамках реализации мероприятий по разви­тию информационного общества на территории муниципального образования город Краснодар.
4. Выполнение работ по развитию, эксплуатации и обслуживанию информа­ционно-коммуникаци­онной инфраструктуры Администрации и городской Думе Краснодара.
5. Выполнение работ по развитию, эксплуатации и обслуживанию муници­пальных информационных систем и ресурсов.
6. Выполнение работ по развитию, эксплуатации и обслуживанию муници­пальных автоматизиро­ванных систем управления, в том числе технологических процессов.
7. Выполнение работ по обеспечению взаимодействия муниципальных ин­формационных систем и ресурсов.
8. Выполнение работ по обеспечению межведомственного электронного взаимодействия Админи­страции с органами государственной власти Россий­ской Федерации и органами государственной власти субъектов Российской Фе­дерации.
9. Выполнение работ по обеспечению доступа к информации, содержащейся в муниципальных информационных системах и ресурсах.
10. Выполнение работ по обеспечению Администрации и городской Думы Краснодара услугами связи и пе­редачи данных (телефо­ния, Интернет, каналы передачи данных, волоконно-оптические линии связи).
11. Выполнение работ по обеспечению Администрации программно-аппарат­ными средствами (про­граммное обеспечение, компьютерная и оргтехника, рас­ходные материалы).
12. Выполнение работ по модернизации, эксплуатации и техническому об­служиванию программно-аппаратных средств Администрации.
13. Выполнение работ по реализации мероприятий в области документальной электросвязи.
14. Выполнение работ по реализации мероприятий в области защиты инфор­мации.
15. Выполнение работ по обеспечению городской Думы Краснодара программным обеспечением.
16. Целью деятельности Казённого учреждения является выполнение работ по развитию, эксплуатации, обслуживанию информационно-телекоммуникационной инфраструктуры Администрации, городской Думы Краснодара и муниципальных учреждений.

Для достижения целей, Казённое учреждение в установленном законодательством порядке осуществляет следующие виды деятельности:

1. Деятельность по выполнению работ по формированию информационно-коммуникационной инфраструктуры муниципального образования город Краснодар и созданию условий для её устойчивого функционирования и комплексного развития.
2. Деятельность по реализации муниципальных целевых программ и механизмов стимулирования в области информатизации и связи.
3. Деятельность по внедрению, развитию, эксплуатации, мониторингу и сопровождению на территории муниципального образования город Краснодар электронной карты жителя Краснодарского края.
4. Деятельность по обеспечению технического сопровождения и поддержки работы Администрации и городской Думы Краснодара, включая муниципальные учреждения, с системами электронных торгов, электронной цифровой подписи и связанных с ними утверждённых процедур.
5. Деятельность по разработке, внедрению, развитию, модернизации, эксплуатации, мониторингу, сопровождению и техническому обслуживанию программного обеспечения Администрации, городской Думы Краснодара и муниципальных учреждений.
6. Деятельность по разработке, внедрению, развитию, модернизации, эксплуатации, мониторингу, сопровождению и техническому обслуживанию ситуационного центра главы муниципального образования город Краснодар.
7. Деятельность по установке, запуску в эксплуатацию, мониторингу, модернизации, эксплуатации, техническому обслуживанию и ремонту вычислительной техники, печатных устройств, копировальной и прочей оргтехники, сетевого оборудования, а также по обеспечению работоспособности любых технических средств, предназначенных для обработки информации муниципальных информационных систем и ресурсов.
8. Деятельность по монтажу, наладке, мониторингу, модернизации, ремонту и техническому обслуживанию структурированных кабельных систем и локальных вычислительных сетей Администрации, городской Думы Краснодара и муниципальных учреждений.
9. Деятельность по обеспечению утилизации вычислительной техники, копировальной техники, печатных устройств, картриджей и аккумуляторных батарей.
10. Информационное обслуживание Администрации, городской Думы Краснодара, включая муниципальные учреждения, в том числе создание и ведение банков данных в области правовой информации, нормотворчества и практики применения законодательства.
11. Деятельность по обеспечению доступа в сеть Интернет, предоставлению каналов передачи данных, телематических услуг связи и передачи данных для Администрации, городской Думы Краснодара, включая муниципальные учреждения.
12. Деятельность по организации и проведению обучения, стажировки и повышения квалификации работников Администрации, городской Думы Краснодара, а также повышения грамотности населения в сфере информационно-коммуникационных технологий и связи, либо в иных сферах на основе применения для организации процесса обучения, стажировки и повышения квалификации информационно-коммуникационных технологий.
13. Деятельность по организации, проведению и техническому сопровождению презентационных выставок, форумов, конференций в сфере информационно-коммуникационных технологий и связи, либо в иных сферах на основе применения для организации выставок, форумов, конференций информационно-коммуникационных технологий.
14. Обеспечение представительства муниципального образования город Краснодар в системе мировых информационных ресурсов.
15. Участие в разработке, приёмке результатов научно-практических разработок, исследований, проектов и программ в сфере информационно-коммуникационных технологий и связи.
16. Разработка, внедрение, развитие, модернизация, эксплуатация, мониторинг, сопровождение, техническое облуживание и информационное наполнение веб-сайтов и порталов Администрации, городской Думы Краснодара включая муниципальные учреждения.

Осуществление мероприятий по мониторингу и защите муниципальных информационных систем и ресурсов:

1. Деятельность по обеспечению технической защиты конфиденциальной информации Администрации, городской Думы Краснодара и муниципальных учреждений.
2. Проведение работ (и обеспечение проведения работ) по защите информации в Администрации, городской Думы Краснодара, включая муниципальные учреждения, выполнение запланированных мероприятий.
3. Организация и проведение периодического контроля эффективности проводимых мероприятий и принимаемых мер по защите информации, учёта и анализа результатов контроля.
4. Организация в установленном порядке расследования причин и условий появления нарушений в области защиты информации, разработка предложений, устранение недостатков и предупреждение подобного рода нарушений.
5. Обеспечение участия муниципального образования город Краснодар в межрегиональной кооперации по вопросам связи и информатизации.
6. Право Казённого учреждения осуществлять деятельность, на которую в соответствии с законодательством Российской Федерации требуется разрешительный документ (лицензия, свидетельство о государственной аккредитации и другое), возникает у Казённого учреждения со дня его получения или в указанный в нём срок и прекращается по истечении срока его действия, если иное не установлено законодательством.

Казённое учреждение принимает участие в реализации федеральных, региональных и муниципальных программ в сфере информационно-коммуникационных технологий и связи, а также планов и программ комплексного социально-экономического развития муниципального образования город Краснодар в области информационно-коммуникационных технологий и связи по поручению управления информационно-коммуникационных технологий и связи администрации муниципального образования город Краснодар.

Казённое учреждение осуществляет функции муниципального заказчика, организует конкурсные процедуры и участвует в проведении конкурсных процедур, заключает в законодательно установленном порядке муниципальные контракты на поставку товаров, оказание услуг для муниципальных нужд в установленной сфере деятельности.

3 Организационная структура предприятия

В организационную структуру предприятия МКУ «Электронный Краснодар» входит:

1. директор;
2. заместитель директора;
3. отдел кадров;
4. бухгалтерия;
5. отдел разработки;
6. главный бухгалтер;
7. ИТ-директор;
8. WEB-разработчик.

Отдел разработки в МКУ «Электронный Краснодар» занимается созданием программного обеспечения, аппаратных компонентов и других технических продуктов. Деятельность по разработке, внедрению, развитию, модернизации, эксплуатации, мониторингу, сопровождению и техническому обслуживанию информационных систем, ресурсов и программных комплексов и по обработке информации в рамках полномочий, в том числе:

на основе геоинформационной системы;

систем электронного документооборота.

Обычно отдел разработки в IT компаниях состоит из разных команд, каждая из которых специализируется на конкретных аспектах разработки, таких как:

1. Команда разработки программного обеспечения, которая отвечает за создание и поддержку программных продуктов;
2. Команда тестирования, которая проверяет работоспособность программного обеспечения и выявляет ошибки и дефекты;
3. Команда проектирования, которая занимается созданием архитектуры;
4. Команда разработки аппаратных компонентов, которая занимается; созданием и разработкой аппаратного обеспечения, такого как компьютеры, мобильные устройства и другие электронные устройства.

В отделе разработки могут также работать менеджеры проектов, которые контролируют процесс разработки и управляют командами разработчиков. Кроме того, отдел разработки может взаимодействовать с другими отделами компании, такими как отдел продаж, маркетинга, поддержки клиентов и т.д. для обеспечения эффективной работы всей компании.

4 Должностные обязанности практиканта в должности разработчик прикладных приложений

Должностные обязанности практиканта в должности разработчика прикладного ПО зависят от конкретных требований и целей компании, в которой он проходит практику. Однако, можно выделить несколько основных обязанностей, которые обычно возлагаются на практиканта в этой должности:

1. Участие в разработке приложений: практикант должен уметь работать с современными инструментами и технологиями, используемыми для создания приложений. Он должен также понимать принципы работы прикладного ПО и понимать, какие технологии используются для управления данными.
2. Тестирование и отладка: практикант должен уметь проводить тестирование создаваемых прикладных приложений и выявлять возможные ошибки и баги. Он должен также уметь использовать различные инструменты для отладки приложений и исправления найденных ошибок;
3. Сотрудничество с командой: практикант должен иметь хорошие коммуникативные навыки и уметь работать в команде, чтобы эффективно взаимодействовать с другими разработчиками, дизайнерами и менеджерами проектов.
4. Отчетность: практикант должен регулярно сообщать о своих достижениях и проблемах, чтобы обеспечить прозрачность процесса разработки приложений.
5. Ведение документации: практикант должен вести документацию и хранить код в системе контроля версий для обеспечения лучшей организации и управления проектом.

Общая задача практиканта в должности разработчика прикладного ПО — это помощь в создании и поддержке качественных прикладных приложений, обладающих хорошей производительностью и пользовательским интерфейсом, который максимально удовлетворит потребности заказчиков.

5 Индивидуальное задание

В качестве индивидуального задания выступает описание информационной системы компании, в данном случае ИС является сайт организации.

В описании ИС должно входить:

1. Описание функционала системы
2. Описание информационного компонента системы
3. Описание подсистемы защиты информации

Сайт предоставляет пользователям удобный интерфейс, позволяющий быстро и просто оставлять заявки на поддержку. Для этого необходимо пройти процедуру регистрации, после чего можно будет оставлять заявки, отслеживать их статус и получать информацию о выполнении заявки.

Основные функции сайта поддержки:

1. Оставление заявок на замену расходных материалов. Пользователи могут оставлять заявки на замену расходных материалов (например, картриджей для принтеров), указывая необходимые детали и количество.
2. Оставление заявок на починку оборудования. Пользователи могут оставлять заявки на починку оборудования, указывая тип оборудования, описание проблемы и другую необходимую информацию.
3. Оставление заявок на программную поддержку. Пользователи могут оставлять заявки на программную поддержку (например, настройку программного обеспечения), указывая необходимую информацию и желаемый результат.
4. Отслеживание статуса заявок. Пользователи могут отслеживать статус своих заявок, узнавать, в работе ли заявка, выполнена ли она или требуется дополнительная информация.
5. Предоставление информации о выполнении заявок. Пользователи могут получать информацию о выполнении заявок, например, когда была заменена запчасти, кто выполнял работу и т.д.
6. Обратная связь. Пользователи могут оставлять отзывы о качестве обслуживания и работе сайта, что позволяет постоянно улучшать сервис.
7. Для реализации данной информационной системы необходимо создать базу данных, которая будет хранить информацию о заявках, пользователях и выполненных работах. Также требуется разработать интерфейс для пользователей, который будет интуитивно понятен и удобен в использовании.

В целом, сайт поддержки является важной частью бизнес-процессов многих компаний и может значительно повысить качество обслуживания и удобства.

Конечная цель информационной системы в данном случае – упрощение и автоматизация процесса поддержки оборудования и программного обеспечения, что в свою очередь позволяет компаниям экономить время и ресурсы.

Для реализации данной информационной системы необходимо учесть следующие аспекты:

1. Разработка базы данных. Для хранения информации о заявках, пользователях и выполненных работах необходимо создать базу данных. База данных должна быть проектирована таким образом, чтобы обеспечивать быстрый доступ к информации и ее безопасность.
2. Разработка интерфейса. Интерфейс сайта поддержки должен быть интуитивно понятным и удобным в использовании. Для этого необходимо учесть потребности пользователей и обеспечить наиболее простой и понятный интерфейс для оставления заявок и получения информации.
3. Разработка системы уведомлений. Чтобы пользователи всегда могли быть в курсе статуса своих заявок, необходимо разработать систему уведомлений. Это может быть, как система автоматических уведомлений, так и возможность получать информацию через электронную почту или мессенджеры.
4. Разработка системы аналитики. Для того чтобы постоянно улучшать качество обслуживания, необходимо собирать и анализировать данные о заявках и работе сайта поддержки. Для этого может быть разработана система аналитики, которая позволит определить проблемные места и принимать меры для их устранения.
5. Разработка системы обратной связи. Обратная связь позволяет узнать мнение пользователей о качестве обслуживания и работе сайта поддержки. Для этого может быть разработана система обратной связи, которая позволит собирать отзывы и предложения от пользователей.
6. Разработка системы управления заявками. Для того чтобы обеспечить эффективную работу поддержки, необходимо разработать систему управления заявками, которая позволит быстро и эффективно распределять заявки между исполнителями и контролировать их выполнение.

Таким образом, информационная система в виде сайта поддержки может значительно упростить и улучшить процесс поддержки оборудования.

Подсистема защиты сайта – это совокупность методов и средств, которые используются для защиты сайта от внешних угроз. Данная подсистема состоит из нескольких компонентов:

1. Антивирусное ПО – это программное обеспечение, которое защищает сайт от вредоносных программ, таких как вирусы, троянские программы, шпионское ПО и т.д. Антивирусное ПО позволяет обнаруживать и блокировать подозрительные файлы и обнаруживать уязвимости в системе.
2. Фаервол – это программное обеспечение, которое контролирует входящий и исходящий трафик на сайте. Оно позволяет блокировать несанкционированный доступ и защищать сайт от DDoS-атак и других типов кибератак.
3. SSL-шифрование – это метод шифрования данных между пользователем и сайтом. Он позволяет защитить данные от перехвата и искажения. Веб-серверы могут использовать SSL-сертификаты для шифрования данных, передаваемых между пользователем и сервером.
4. Контроль доступа – это метод, который позволяет контролировать доступ к сайту. Например, администратор может установить ограничения на доступ к определенным страницам или функциям сайта.
5. Мониторинг – это процесс отслеживания активности на сайте. Мониторинг позволяет обнаруживать несанкционированные попытки доступа и проблемы с безопасностью сайта.
6. Резервное копирование – это метод, который позволяет создавать резервные копии данных сайта. Резервное копирование помогает защитить сайт от потери данных при несчастном случае или атаке.

Кроме перечисленных выше методов, существуют и другие методы защиты сайта, которые зависят от конкретных условий и требований. Однако, подсистема защиты сайта должна быть разработана таким образом, чтобы обеспечивать надежную защиту сайта от внешних угроз

6 Техника безопасности

Техника безопасности в муниципальном казенном учреждении (МКУ) должна включать в себя следующие меры:

1. Контроль доступа: необходимо установить систему контроля доступа для ограничения входа на территорию учреждения и в отдельные зоны внутри учреждения. Для этого можно использовать электронные ключи, карты доступа или биометрические системы.
2. Охрана и видеонаблюдение: важно обеспечить наличие квалифицированных охранников на территории учреждения и установить систему видеонаблюдения, которая позволит контролировать доступ и поведение посетителей и сотрудников.
3. Обучение персонала: Все сотрудники МКУ должны быть обучены основам безопасности и знать процедуры действия в случае возникновения чрезвычайных ситуаций.
4. Пожарная безопасность: необходимо обеспечить наличие средств пожаротушения и установить автоматическую систему оповещения в случае пожара.
5. Защита данных: необходимо обеспечить защиту конфиденциальных данных, используемых в работе учреждения, с помощью установки современных систем защиты информации и контроля доступа к ней.
6. Контроль за рабочими местами: необходимо обеспечить безопасность рабочих мест сотрудников МКУ, включая электрические установки и компьютеры, путем регулярной проверки состояния их технического оборудования и устранения выявленных неполадок.
7. Эвакуационные планы: необходимо разработать план эвакуации в случае возникновения чрезвычайных ситуаций, проводить тренировки сотрудников и убедиться, что все выходы и маршруты эвакуации являются безопасными и доступными.

Заключение

В заключение можно сказать, что информационная система — это сложная и многогранная среда, требующая постоянного внимания и развития. Исследование позволяет выявить проблемные моменты в ее работе и принять меры для их устранения, а также определить направления для дальнейшего развития системы. В целом, информационная система является важным инструментом для достижения успеха в бизнесе, и ее правильное функционирование способствует улучшению качества работы организации в целом.

Список источников

1. <https://krd.ru/administratsiya/administratsii-krasnodara/upravlenie-informatsionno-kommunikatsionnykh-tekhnologiy-i-s/podvedomstvennye-organizatsii/org-19112013-1106/>
2. <https://mcotexpertiza.ru/trebovaniya-k-okhrane-truda-dlya-programmistov>
3. <https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/informatsionnaya-bezopasnost-v-otraslyakh/informatsionnaya-bezopasnost-predpriyatij/pravila-informatsionnoj-bezopasnosti-na-predpriyatii/>