Техническое задание «Модернизация инфраструктуры»

v. 1.1

История изменений.

- 1.1
  - Добавлен раздел «Лабораторная демонстрация инфраструктуры».
  - Раздел «Формат модернизации» дополнен пунктом «Набор инструкций по применению служб и инфраструктуры».
- 1.01
  - Орфография и прочие синтаксические правки.

Введение.

Практически все сферы отечественной экономики переживают этап интенсивной информатизации бизнес-процессов. Информационные технологии предлагают новые решения существующих проблем, цифровая трансформация бизнеса открывает новые перспективы повышения производительности труда, снижения издержек и снижения рисков непрерывности бизнеса. Все это невозможно без квалифицированного труда программистов, непосредственно выполняющих разработку программных комплексов и информационных систем. Столь стремительно развивающаяся отрасль, в сочетании с легкостью вхождения и низкими затратами на ведение бизнеса, породила целый класс небольших компаний, специализирующихся на разработке программного обеспечения как в виде отдельных продуктов, так и в составе более крупных команд.

Компания <COMP_NAME> - региональный игрок рынка аутсорсинга разработки программного обеспечения. Требования рынка, анализ рисков, контрактные обязательства перед заказчиками и контрагентами ставят вопрос о конкурентоспособности существующей модели информационных процессов предприятия. Внутренний аудит продемонстрировал большое количество недостатков существуюей информационной системы, выявил все возрастающие риски информационной безопасности, непосредственно затрагивающие непрерывность бизнеса. С целью ликвидации рисков руководство компании

приняло решение выполнить глубокую перестройку и модернизацию существующей инфраструктуры.

Руководство компании так же считает, что в рамках модернизации имеет смысл реализовать набор решений, направленных на повышение производительности труда — повышение уровня автоматизации работы программистов, тестирования и развертывания разрабатываемых приложений. В рамках данного проекта компания ожидает развертывания технологического стека CI/CD на базе одного из своих проектов для последующей оценки возможностей внедрения данного решения в свои бизнес-процессы.

Основные цели модернизации.

За счет проекта модернизации инфраструктуры компания рассчитывает добиться следующих целей:

- минимизировать риски нарушения непрерывности бизнеса, характерные для используемой бизнес-модели предприятия;
- минимизировать финансовые затраты на содержание и обслуживание инфраструктуры предприятия;
- произвести оценку возможности внедрения актуальных технологических решений в сфере автоматизации ключевых бизнес-процессов.

Основные задачи модернизации.

В рамках модернизации инфраструктуры компания рассчитывает решить перечисленные задачи.

1. Устранить выявленные в ходе аудита недостатки информационной инфраструктуры предприятия.
2. Реализовать процессы CI/CD на примере разрабатываемого приложения.

Основные принципы модернизации.

В рамках модернизации инфраструктуры следует руководствоваться нижеизложенными принципами.

- **Модернизация как улучшение**: реализованное решение должно как минимум не уступать по функциональности существующему и заведомо превосходить по совокупности параметров: простоте обслуживания, надежности, стоимости, производительности, ресурсоемкости.

- **Надежность реализации**: механизм должен быть защищен от отказа насколько это возможно; в случае отказа ответственные лица должны быть уведомлены, должна быть реализована политика восстановления после отказа, утери данных при отказе должны быть минимизированы.
- **Удобство администрирования**: то, что будет администрировать человек, должно быть максимально дружелюбным к человеку. Задача должна решаться за минимальное количество шагов, должна быть реализована защита от некорректного ввода данных и повторного срабатывания.
- **Лицензионная чистота**: используемое ПО должно быть легально доступно на территории РФ, поддерживаться разработчиками и получать актуальные обновления.
- **Снижение затрат**: используемые решения должны по возможности опираться на существующие ресурсы компании, приобретаемые либо арендуемые ресурсы должны быть сопоставимы с решаемой задачей.
- **Масштабирование**: используемые решения должны допускать эффективное масштабирование на случай кратного увеличения численности персонала, проектов компании и т.д.
- **Минимизация зависимости:** компания не может гарантировать выбор конкретного инфраструктурного провайдера, поэтому рассчитывает самостоятельно администрировать инфраструктурные службы информационной системы предприятия.
- **Разумная конфиденциальность**: компания требует соблюдения конфиденциальности своих данных, защиту от несанкционированного доступа третьих лиц, однако не считает уважаемых игроков рынка хостинга и облачных услуг в качестве потенциальной угрозы. Тем не менее, компания не доверяет свои критические данные организациям, предоставляющим услуги в формате SaaS.

Шаги, предпринятые компанией в рамках модернизации.

В ходе начальной подготовки к модернизации инфраструктуры руководство компании приняло следующие решения:

Отказ от аппаратных серверов. Невозможность оперативной замены, зависимость от офисных коммуникаций в сфере подключения к сети «Интернет» и электропитания, зависимость от наличия угроз техногенного характера(затопление, пожар и т.п.) представляются руководству серьезной причиной перехода на внешний хостинг с последующем обеспечением

надежного доступа. Тем не менее, Сервер-2 продолжит использоваться в качестве маршрутизатора и может быть задействован для выполнения локальных задач и задач низкого приоритета

Отказ от решений Microsoft в сфере разработки ПО. Отсутствие дальнейшей технической поддержки, сомнительный лицензионный статус и доминирование решений на базе системы контроля версий Git являются достаточными факторами для принятия подобного решения. Компания уже перевела тестовое приложение в репозиторий на базе Git и в ходе модернизации ожидает его внедрения в бизнес-процессы предприятия.

Формат проекта модернизации.

Проект модернизации должен быть представлен следующем формате:

План-презентация. План должен содержать описание всех основных этапов работы, ключевые технологические решения и ключевые детали реализации. Должны быть описаны способы интеграции, резервного копирования, контроля доступа и прочих решений с перечислением программных средств их реализации.

Набор конфигураций служб и сценариев автоматизации. Набор используется исполнителем в ходе демонстрации проекта модернизации инфраструктуры.

Лабораторная демонстрация проекта. Лабораторная демонстрация выполняется в окружении вложенной виртуализации на базе KVM + QEMU. Характеристики полигона составляют:

- vCPU — 8-12 шт.
- ОЗУ — 16 Гб.
- хранилище — SSD + HDD — 450 Гб.

В случае изменения характеристик полигона исполнитель будет уведомлен дополнительно.

Набор инструкций по применению служб и инфраструктуры. Набор используется представителем заказчика при тестировании лабораторного прототипа.

Основные требования к проекту модернизации.

Проект модернизации должен включать в себя следующие разделы:

Анализ потребления арендуемых ресурсов. Компания будет самостоятельно решать вопросы аренды хостинга и организации среды виртуальных машин, однако компании необходимо точно понимать сколько требует ресурсов проект модернизации. Должно быть исследовано потребление 3 видов ресурсов: vCPU, ОЗУ, объем и тип хранилища данных.

Проект устранения недостатков инфраструктуры, выявленных в ходе аудита. Компания осознает риски и желает получить комплексное инфраструктурное решение, которое будет оптимизировано под реалии существующих бизнес-процессов. Проект должен покрывать все инфраструктурные компоненты реализованного рабочего процесса и соответствовать принципам проекта модернизации.

Проект модернизации процесса разработки программного обеспечения. Компания осознает требования рынка к наличию культуры непрерывной интеграции и доставки и желает оценить реализацию процесса на своем тестовом проекте.

Приложение. Инструкция по применению и администрированию настроенных служб и решений. Должна содержать актуальные ссылки на развернутые службы и пояснения к применению.

Общие сведения о компании.

<COMP_NAME> — молодая, динамично развивающаяся компания, специализирующая на разработке программного обеспечения различного назначения. Компания как обладает собственными программными решениями, адаптируемыми под конкретного заказчика, так и участвует в разработке и сопровождении программных компонент сторонних комплексов на правах привлеченного разработчика. Компания специализируется на веб-решениях, взаимодействующих по стандартам REST или аналогичным протоколам. Хостинг программных продуктов выполняется на платформах заказчиков, однако присутствует и собственный узел хостинга для презентационных и отладочных целей.

Персонал компании может быть разделен на две категории: постоянные и привлекаемые сотрудники. Постоянные сотрудники компании осуществляют поддержку продуктов компании и общее руководство группами разработки. Постоянные сотрудники используют офисные компьютеры в качестве рабочих мест. Привлекаемые сотрудники ведут разработку проектов компании на договорной основе с применением собственной компьютерной техники, подключаемой к инфраструктуре компании на время действия контракта.

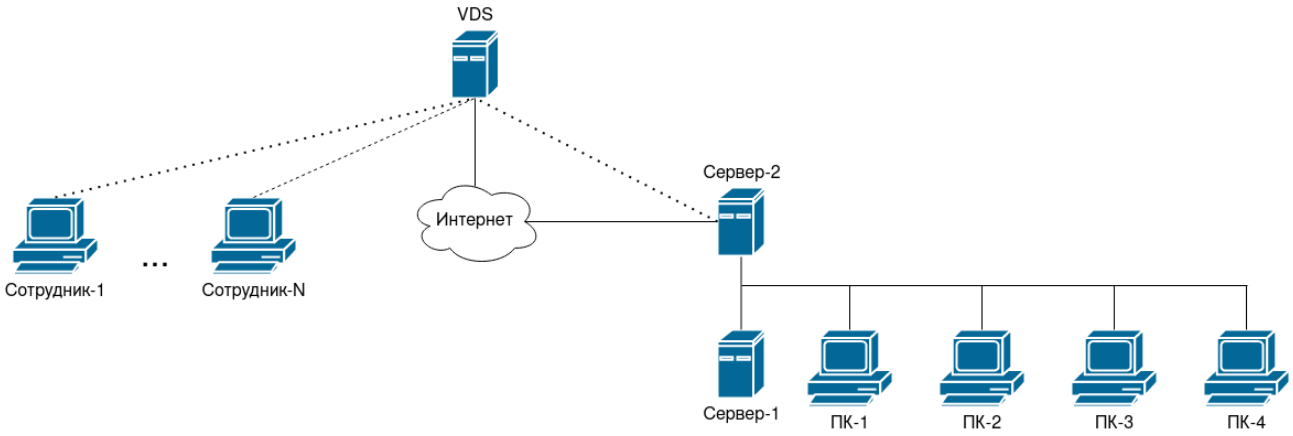
Вспомогательные процессы компании — кадровое администрирование, ведение бухгалтерии, обслуживание офиса и т.п. — выполняется с привлечением аутсорсинга и не является темой данного проекта.

Наиболее ценные активы предприятия.

Наиболее ценными активами предприятия являются программный код разрабатываемых программных комплексов, рабочая документация по проектам компании и различные учетные данные для доступа к информационным системам заказчиков.

Информационная структура предприятия.

Информационная структура предприятия представлена информационной системой офиса компании и внешними арендованными вычислительными ресурсами. Компьютеры привлеченных сотрудников на время действия договора рассматриваются как специфичная часть общей информационной инфраструктуры. Схематично инфраструктура предприятия представлена на рисунке ниже:



Характеристики используемых платформ представлены в таблице ниже:

Хост	ОС	vCPU	ОЗУ	Хранение
Сервер-1	Windows Server 2016	12	32	SSD: 250 Гб HDD: 2 Тб
Сервер-2	CentOS 7	4	4	HDD: 500 Гб
ПК-1	Windows 10	8	16	SSD: 500 Гб
ПК-2	Ubuntu 20.04	8	16	SSD: 500 Гб

ПК-3	Windows 10	8	16	SSD: 500 Гб
ПК-4	Windows 10	8	16	SSD: 500 Гб
VDS	CentOS 8 stream	2	4	SSD: 100 Гб

Резерв аппаратных возможностей представлен 3 персональными компьютерами аналогичного типа и маршрутизатором, предоставляемым провайдером, с функциями DHCP-сервера и DNS-резолвера. Доступно применение публичного IP-адреса.

Основные рабочие процессы предприятия.

Ниже представлены существующие сценарии работы всех сотрудников предприятия в контексте использоваться информационной системы компании и её ресурсов.

Директор. Использует ПК-1, согласно инструкции имеет право доступа ко всем ПК и серверам предприятия. Директор занимается офисной работой с применением ПК-1. Всю ключевую информацию директор хранит в домашнем каталоге своего пользователя. Использует файловые службы Сервер-1 для обмена данными с другими сотрудниками через подключенный в формате сетевого диска файловый ресурс.

Программист (постоянный сотрудник). Используют ПК-2-4, закрепленные за ними. Не имеют доступа к чужим ПК, имеют доступ к серверам компании. Занимаются разработкой с применением персонализированного набора ПО на базе ПК. Осуществляют разработку программного кода, локальное тестирование с применением системы виртуализации VirtualBox. Используют файловые службы Сервер-1 для обмена данными с другими сотрудниками через подключенный в формате сетевого диска файловый ресурс. В качестве системы контроля версий используется Microsoft Team Foundation Server, развернутый на Сервер-1. В качестве тестовой системы используется Сервер-2, веб-сервер NGINX и СУБД Postgresql. Могут применять программу AnyDesk для удаленного доступа к собственному рабочему месту из дома или другой локации.

Программист (привлекаемый сотрудник). Используют собственные ПК в качестве рабочей среды. Не имеют доступа к чужим ПК, могут опционально иметь доступ к серверам. Осуществляют разработку программного кода и локальное тестирование с применением VirtualBox. Используют файловые службы Сервер-1 для обмена данными с другими сотрудниками через подключенный в формате сетевого диска файловый ресурс. В качестве системы контроля версий используется Microsoft Team Foundation Server, развернутый на

Сервер-1. В качестве тестовой системы используется Сервер-2, веб-сервер NGINX и СУБД Postgresql.

Развернутые инфраструктурные службы.

Ниже перечислены основные настроенные инфраструктурные решения предприятия и сценарии их применения.

DHCP-сервер. развернут на Сервер-2, пакет ISC DHCP. Используется для автоматической конфигурации хостов офиса. Раздаются параметры: адрес, адрес локального DNS-сервера, маршрут по умолчанию.

DNS-сервер, развернут на Сервер-2, пакет BIND. Используется для разрешения и кэширования DNS-запросов офиса, обслуживает зону test.company.

Файловый сервер, развернут на Сервер-1, роль «Файловые службы Windows». Испольуется для оперативного обмена файлами, раздается каталог Share на диске D:\. Предоставлен доступ всем ПК из сети офиса, используется пользователь Administrator.

VPN-сервер, развернут на VDS, пакет OpenVPN. Реализует TLS VPN-сервер. ключевая информация генерируется локально. Подключенные клиенты используют типовую конфигурацию и единую клиентскую ключевую информацию. Присвоение адресов происходит автоматически средствами OpenVPN.

Интернет-шлюз, развернут на Сервер-2, пакеты Firewalld и NetworkManager. Осуществляет подключение к сети провайдера с применением протокола PPPoE. Выполняется трансляция исходящего трафика в адрес внешнего интерфейса.

Развернутые службы сопровождения разработки.

Ниже перечислены службы сопровождения бизнес-процессов разработки приложений:

Веб-сервер NGINX. Развернут на Сервер-2, обслуживается тестовые варианты приложений, разрабатываемых в компании. Прослушивает внутренние адреса, осуществляет перенаправление запросов по доменному имени.

СУБД Postgresql. Развернута на Сервер-2, обслуживает тестовые варианты приложений, разрабатываемых в компании. Прослушивает внутренние адреса, предоставляет доступ всем пользователям локальной сети предприятия. Осуществляет обслуживание баз данных тестовых приложений.

Microsoft Team Foundation Server(выводится из эксплуатации). Развернут на Сервер-1. Централизованная система контроля версий и распределения задач, используется программистами для планирования работ и хранения исходников разрабатываемых проектов.

Результаты внутреннего аудита компании.

В результате внутреннего аудита были установлены многочисленные несоответствия реального положения дел современным мировым практикам организации информационной инфраструктуры. Аудитор отметил следующие недостатки эксплуатируемой инфраструктуры:

- отсутствие механизмов централизованного управления аутентификацией и авторизацией пользователей при доступе к ресурсам и службам;
- отсутствие механизмов мониторинга инфраструктуры и оповещения ответственных сотрудников об инцидентах;
- отсутствие механизмов резервного копирования критичной информации;
- отсутствие резервирования критичных компонентов инфраструктуры;
- отсутствие механизмов разделения доступа к ресурсам и службам предприятия;
- отсутствие механизмов эффективного отзыва прав доступа сотрудников по истечении их рабочей деятельности.

Ожидаемые направления модернизации процесса разработки.

Инфраструктура тестового приложения представлена перечисленными ниже хостами.

- **Хост PROD**. Доступный из внешней сети хост, ответственный за обслуживание внешних клиентов.
- **Хост TEST**. Доступный из внутренний сети хост, ответственный за тестирование и отладку.

Компания рассматривает следующие технологические решения в области повышения производительности труда программистов.

Системы собственного тестирования. Каждый проект будет (на уровне разработки и дизайна приложения) оснащен системами тестирования.

Система контейнеризации Docker. Приложения будут распространятся в формате образов Docker для упрощения менеджмента зависимостей и упрощения доставки и интеграции.

Системы управления разработкой. Применение инфраструктурных решений управления процессом разработки на базе технологии Git.

Реализация концепций CI/CD. Автоматизация процессов тестирования, сборки и доставки приложений.

Компания рассматривает внедрение процесса отладки и тестирования программного обеспечения в формате трех этапов:

1. выполнение внутренних тестов;
2. сборка и загрузка образов Docker;
3. развертывание приложения.

Компания ожидает выполнения всех этапов отладки и тестирования на каждое зарегистрированное изменение программного кода.

Компания рассматривает следующие направления развертывания своего продукта:

- **ветка «master»** развертывается на ВМ, ответственной за обслуживание пользователей;
- **прочие ветки** развертываются на ВМ, предназначенной для тестирования.

Предварительное описание тестового приложения.

Тестовый проект предназначен для отработки обновленного процесса разработки с применением современных технологий. Проект представляет из себя перечисленные ниже компоненты.

- **Веб-приложение**. Реализация: язык Python и фреймворк FastAPI. Реализует несложные операции с данными, хранящимися в базе данных.

- **База данных**. Реализация: СУБД Postgresql. Реализует хранение нескольких таблиц.

Проект снабжен комплектом для локального запуска, средствами тестирования. Полноценное использование подразумевается в связке с сервером NGINX.

Прочая информация будет доступна в документации к приложению.

Лабораторная демонстрация инфраструктуры.

Лабораторная демонстрация инфраструктуры выполняется с применением технологий вложенной виртуализации на базе CentOS 8, пользовательское ПО управления виртуализацией — virt-manager. Исполнителю не рекомендуется обращаться к системе виртуализации за пределами обычных пользовательских операций, выполняемых из GUI. Ниже указаны особенности построения прототипа на виртуальной среде.

Загрузка образов ISO, необходимых для построения прототипа, выполняется самостоятельно с применением установленных стандартных средств среды виртуализации — браузер firefox. При необходимости установки дополнительных пакетов выполнить их установку самостоятельно с помощью предоставленного пользователя с правами администратора.

Прототип должен содержать образцы виртуальных машин для тестирования сценариев работы. Для экономии ОЗУ и процессорного времени допускается поочередное включение данных ВМ (в общем случае можно считать, что только одна пользовательская ВМ включена в один момент времени). Требуются следующие образцы ВМ:

- **PC-1**, как ПК директора;
  - При демонстрации ПК должен быть полностью настроен и интегрирован в процессы компании;
- **PC-X**, как ПК постоянного сотрудника;
  - При демонстрации ПК должен быть полностью настроен и интегрирован в процессы компании;
  - Установлено ПО VSCode и средства работы с git;
- **RC-W**, как ПК внешнего сотрудника на базе Windows 10;

- При демонстрации должен быть в базовой конфигурации с установленным ПО VSCode и средствами работы с git.
- В ходе тестирования эксперт

- **RC-U**, как ПК внешнего сотрудника на базе Ubuntu 20.04;
  - При демонстрации должен быть в базовой конфигурации с установленным ПО VSCode и средствами работы с git.

Прототип должен содержать образцы виртуальных машин реализации инфраструктуры предприятия. Должны быть созданы прототипы как локальной («on-prem») инфраструктуры, располагаемой в офисе, так и инфраструктуры, располагаемой на арендованном ресурсе. Для визуального опознавания компонентов инфраструктуры должна быть реализована следующая схема именования виртуальных машин лабораторного стенда:

<**C**|**L**>-<**ИмяВМ**>

где C или L обозначает удаленное («Cloud») или локальное («Local») расположение данного хоста. Имя ВМ должно, по возможности, отражать назначение ВМ. Экземпляры ВМ, ответственные за обслуживание инфраструктуры и процесс разработки должны быть запущены постоянно.

Прототип должен сопровождаться пакетом инструкций, представленном в электронном виде на рабочем столе лабораторного стенда. Документация должна содержать инструкции для следующих пользователей:

- **Директор** — менеджмент инфраструктурного обеспечения основных бизнес-процессов, доступ ко всем ресурсам, полный доступ к инфраструктуре разработки, доступ к средствам централизованного управления и мониторинга;
  - Процессы, характерные для системного администратора, рекомендуется описать в данном пакете инструкций (как минимум, до получения дополнительных указаний).
- **Сотрудник** — использование инфраструктурных служб, использование инфраструктуры разработки.
- **Привлеченный сотрудник** — подключение к инфраструктуре, использование инфраструктурных служб, использование инфраструктуры разработки;