

М. Ю. Благодаренко^{1✉}, Т. Ю. Бугакова¹

Развертывание защищенной инфраструктуры удаленных рабочих мест с системой мониторинга на базе Proxmox VE и Docker контейнеров

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: maxblag04@gmail.com

Аннотация. Статья посвящена проблеме организации удаленного доступа к рабочим местам для сотрудников. Коммерческие решения часто избыточно дороги и не предоставляют достаточной гибкости при настройке системы. Целью исследования является развертывание защищенной инфраструктуры удаленных рабочих мест на программном обеспечении с открытым исходным кодом. Для этого были использованы такие методы, как: виртуализация (Proxmox VE), настройка межсетевого экранирования (pfSense, OpenVPN) и контейнеризация системы мониторинга (Zabbix в Docker). Результатом являются готовые к внедрению виртуальные машины, сетевой оффлайн репозиторий для обновления пакетов на них, шифрованное VPN-туннелирование и централизованный сбор метрик со всех машин. Стресс-тесты и тесты на отказоустойчивость подтвердили стабильность, как отдельных виртуальных машин, так и системы целиком. Подводя итоги, можно сказать, что предложенная архитектура полностью соответствует поставленным задачам и предоставляет надежное решение для практического внедрения инфраструктуры в организацию.

Ключевые слова: защищенная инфраструктура, виртуальная машина, система мониторинга

М. Yu. Blagodarenko^{1✉}, T. Yu. Bugakova¹

Deployment of a secure remote workplace infrastructure with a monitoring system based on Proxmox VE and Docker containers

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: maxblag04@gmail.com

Abstract. The article is devoted to the problem of organizing remote access to workplaces for employees. Commercial solutions are often unnecessarily expensive and do not provide sufficient flexibility when configuring the system. The purpose of the study is to deploy a secure remote workplace infrastructure based on open source software. For this, methods such as virtualization (Proxmox VE), firewall configuration (pfSense, OpenVPN) and containerization of the monitoring system (Zabbix in Docker) were used. The result is ready-to-deploy virtual machines, an offline network repository for updating packages on them, encrypted VPN tunneling, and centralized collection of metrics from all machines. Stress tests and fault tolerance tests have confirmed the stability of both individual virtual machines and the entire system. Summing up, we can say that the proposed architecture is fully consistent with the tasks set and provides a reliable solution for the practical implementation of infrastructure in the organization.

Keywords: secure infrastructure, virtual machine, monitoring system

Введение

Современные организации все больше переходят на удаленный формат работы. Распределенная структура персонала диктует новые требования к ИТ-инфраструктуре, в частности, необходимость создания защищенного периметра для безопасного доступа сотрудников к внутренним ресурсам компании без ущерба для конфиденциальности данных.

Вместе с тем, анализ рынка показывает, что готовые коммерческие решения для организации удаленного доступа часто обладают избыточной стоимостью для малого и среднего бизнеса, либо не предоставляют необходимого уровня гибкости и контроля над инфраструктурой безопасности. В связи с этим, целесообразным представляется использование программного обеспечения с открытым исходным кодом. Применение таких инструментов, как гипервизор Proxmox VE, межсетевой экран pfSense и система мониторинга Zabbix, позволяет построить отказоустойчивую и экономически эффективную среду, адаптированную под конкретные нужды организации.

Целью исследования является построение полностью функционирующей защищенной инфраструктуры удаленных рабочих мест с использованием только программного обеспечения с открытым исходным кодом, а также подтверждение ее работоспособности и отказоустойчивости. Для достижения цели решены следующие задачи: спроектирована архитектура инфраструктуры, межсетевого экрана и системы мониторинга; развернуты виртуальные рабочие станции на базе Astra Linux; организован защищенный VPN-доступ к ним через OpenVPN; реализован централизованный сбор метрик и мониторинг состояния всех узлов.

Практическая значимость исследования заключается в возможности внедрения предложенного решения в организациях для обеспечения безопасной удаленной работы сотрудников. Разработанная инфраструктура была выполнена в рамках реального задания производственного отдела ООО «СИГНАТЕК» и принята в опытную эксплуатацию.

Методы и материалы

В рамках реальных производственных задач ООО «СИГНАТЕК» было разработано и утверждено техническое задание, которое определило совокупность обязательных требований к развертываемой инфраструктуре удаленных рабочих мест. Документ предписывал использование платформы виртуализации Proxmox VE версии 8.0, развертывание десяти виртуальных машин под управлением Astra Linux Common Edition 1.7.6 с заданной минимальной конфигурацией, создание межсетевого экрана pfSense с OpenVPN-сервером, организацию внутреннего АРТ-репозитория на базе Apache, а также выделение отдельного сервера для системы мониторинга Zabbix в среде Docker.

В части обеспечения безопасности техническое задание требовало настроить правила файрвола с открытием UDP-порта 1194 для VPN, запретить прямой доступ к серверу мониторинга из внешней сети, организовать выделенную VPN-сеть в диапазоне 10.0.8.0/24 с фиксированными адресами для узлов, обеспечить

невозможность доступа к любой виртуальной машине без активного VPN-подключения, а также провести тестирование всех защитных механизмов. Выполнению каждого из перечисленных пунктов посвящены соответствующие этапы практической реализации, описанные в разделе «Результаты».

В процессе выполнения исследования применялись следующие методы. Метод анализа предметной области – использовался для обоснования выбора компонентов инфраструктуры и изучения существующих решений [1]. Метод архитектурного моделирования, который позволил спроектировать взаимосвязь между гипервизором, межсетевым экраном, виртуальными машинами и системой мониторинга. Архитектура визуализирована при помощи аппаратно-программной диаграммы взаимосвязей компонентов инфраструктуры на рисунке А.1 (Приложение А). Одним из самых важных являлся метод экспериментального тестирования, этот метод включал в себя проведение стресс-тестов виртуальных машин при помощи специализированного скрипта, а также тестов отказоустойчивости путем имитации отказа работоспособности различных компонентов инфраструктуры. Последним методом является сравнительный анализ, который применялся для оценки эффективности предложенного решения по сравнению с коммерческими аналогами.

В качестве материалов использовалось серверное оборудование Dell PowerEdge с 64 ГБ оперативной памяти. Используемое программное обеспечение включало платформу виртуализации Proxmox VE, межсетевой экран pfSense с OpenVPN, систему мониторинга Zabbix, которая была развернута в Docker контейнерах, а также гостевую операционную систему Astra Linux 1.7.6.

Результаты

Была выполнена полная практическая реализация развертывания защищенной инфраструктуры удаленных рабочих мест в полном соответствии с техническими требованиями ООО «СИГНАТЕК». Первым этапом была выполнена настройка серверного оборудования, конфигурирование отказоустойчивого RAID-массива и установка системы виртуализации Proxmox VE, это обеспечило надежную аппаратную и программную подготовку для выполнения последующих задач. С использованием веб-интерфейса гипервизора созданы десять рабочих станций на базе Astra Linux, узел межсетевого экрана pfSense, и сервер сетевого оффлайн репозитория A-Repo с расширенным дисковым пространством (рис. 1).

PROXMOX Виртуальная среда

Server View

Центр обработки данных

Узел TDA3

Поиск

100 (pfSense)
101 (RM-1)
102 (RM-2)
103 (RM-3)
104 (RM-4)
105 (RM-5)
106 (RM-6)
107 (RM-7)
108 (RM-8)
109 (RM-9)
110 (RM-10)
111 (A-Repo)
локальная сеть (TDA3)
local-btrfs (TDA3)

Краткие сведения
Примечания
Оболочка
Система
Сеть
Сертификаты
DNS
Хозяева
Опции
Время
Системный журнал
Обновления
Репозитории
Брандмауэр
Диски
LVM
LVM-Тонкий
Каталог
ZFS
Циф

Тип	Описание	Использов...	Использов...	Использов...	Время безот...	Использов...	Использов...
qemu	100 (pfSense)	0.0 %	7.7 %	1.4 % от 2 ...	00:00:46	0.7 % от 4 ...	1.0 %
qemu	101 (RM-1)	0.0 %	10.5 %	2.7 % от м...	00:00:45	0.7 % от 4 ...	2.1 %
qemu	102 (RM-2)	0.0 %	10.6 %	2.4 % от м...	00:00:44	0.6 % из 4 ...	2.1 %
qemu	103 (RM-3)	0.0 %	10.9 %	2.4 % от м...	00:00:43	0.6 % из 4 ...	2.1 %
qemu	104 (RM-4)	0.0 %	11.0 %	2.4 % от м...	00:00:41	0.6 % из 4 ...	2.1 %
qemu	105 (RM-5)	0.0 %	10.4 %	2.4 % от м...	00:00:40	0.6 % из 4 ...	2.1 %
qemu	106 (RM-6)	0.0 %	10.8 %	2.4 % от м...	00:00:39	0.6 % из 4 ...	2.1 %
qemu	107 (RM-7)	0.0 %	10.4 %	2.4 % от м...	00:00:38	0.6 % из 4 ...	2.0 %
qemu	108 (RM-8)	0.0 %	10.2 %	2.5 % от м...	00:00:37	0.6 % из 4 ...	2.0 %
qemu	109 (RM-9)	0.0 %	10.2 %	2.4 % от м...	00:00:36	0.6 % из 4 ...	2.0 %
qemu	110 (RM-10)	0.0 %	10.9 %	2.4 % от м...	00:00:35	0.6 % из 4 ...	2.1 %
qemu	111 (A-Repo)	0.0 %	10.4 %	2.5 % от м...	00:00:33	0.6 % из 4 ...	2.1 %
sdn	локальная сеть (TDA3)	-	-	-	-	-	-
Хран...	local-btrfs (TDA3)	6.0 %	-	-	-	-	-

Рис. 1. Веб-интерфейс Proxmox VE

Особое внимание уделено настройке межсетевого экрана на базе pfSense, где организован защищенный сетевой периметр: настроены WAN и LAN интерфейсы, активирован DHCP-сервер, прописаны правила файрвола и реализован NAT для порта UDP 1194. Также одним из самых важных пунктов являлось создание OpenVPN-сервера с шифрованием трафика, для которого сгенерированы клиентские конфигурационные файлы для удаленных сотрудников.

Для обеспечения автономности и повышения безопасности инфраструктуры создан сетевой оффлайн репозиторий, позволяющий устанавливать и обновлять ПО без доступа к внешнему интернету. На отдельном физическом сервере реализована система мониторинга Zabbix в изолированной среде Docker-контейнеров. На всех узлах инфраструктуры установлен Zabbix Agent, и настроен сбор ключевых метрик, добавлены хосты в веб-интерфейс и сформирован дашборд для визуализации состояния ресурсов (рис. 2).

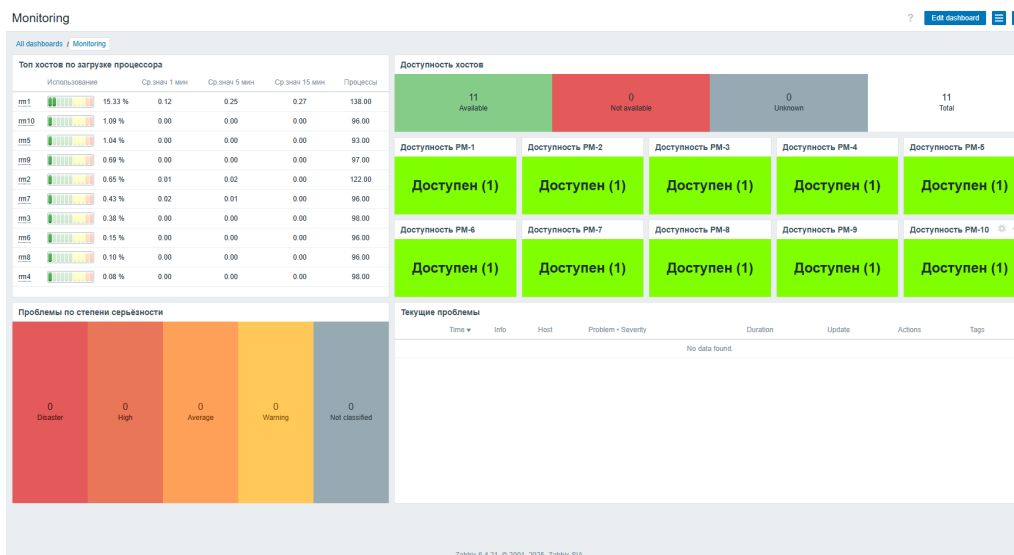


Рис. 2. Дашборд системы мониторинга

Обсуждение

Полученные в ходе исследования результаты подтверждают, что инфраструктура удаленных рабочих мест на базе открытого программного обеспечения способна обеспечить уровень доступности, отказоустойчивости, а главное безопасности, сопоставимый с коммерческими решениями. При этом система не включает в себя ограничений для масштабирования наподобие лицензионных правил.

Сравнение с результатами авторов [2, 3], изучавших контейнеризацию приложений, показывает, что выбранный подход с разделением Zabbix на три Docker контейнера обеспечивает изоляцию сервисов без потери производительности. Также стресс-тестирование позволило наглядно убедиться в том, что виртуальные рабочие станции сохраняют работоспособность при 100 % загрузке процессора в течение 60 секунд, что сопоставимо с результатами, представленными в исследованиях, где аналогичные показатели достигались на физическом оборудовании [4, 5].

Заключение

Основной идеей исследования являлось подтверждение возможности построения полностью функционирующей защищенной инфраструктуры удаленных рабочих мест с использованием только программного обеспечения с открытым исходным кодом. Ключевые результаты – стабильная работа десяти виртуальных рабочих станций с доступностью только через VPN туннелирование и централизованный сбор метрик для системы мониторинга.

Спроектированная и развернутая инфраструктура была передана в опытную эксплуатацию производственному отделу ООО «СИГНАТЕК», что подтверждает ее практическую пригодность и полное соответствие утвержденному техническому заданию. Направления дальнейших исследований включают оценку

максимального порога масштабирования инфраструктуры, а также поиск способов повышения отказоустойчивости сетевого шлюза.

Благодарности

Авторы выражают благодарность производственному отделу ООО «СИГ-НАТЕК» за содействие при выполнении работы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Корпоративная ИТ-инфраструктура: [сайт]. – URL: <https://cyberleninka.ru/article/n/korporativnaya-it-infrastruktura> (дата обращения: 16.04.2026). – Режим доступа: свободный. – Текст: электронный.
2. Системный подход к безопасности пользовательских файлов: от первичной валидации до изоляции в Docker: [сайт]. – URL: <https://cyberleninka.ru/article/n/sistemnyy-podhod-k-bezopasnosti-polzovatelskih-faylov-ot-pervichnoy-validatsii-do-izolyatsii-v-docker> (дата обращения: 16.04.2026). – Режим доступа: свободный. – Текст: электронный.
3. Контейнеризация и автоматизация развертывания веб-приложений: анализ и практическая реализация: [сайт]. – URL: <https://cyberleninka.ru/article/n/konteynerizatsiya-i-avtomatizatsiya-razvertyvaniya-veb-prilozheniy-analiz-i-prakticheskaya-realizatsiya> (дата обращения: 16.04.2026). – Режим доступа: свободный. – Текст: электронный.
4. Повышение надежности ИТ-инфраструктуры при использовании виртуализации: [сайт]. – URL: <https://cyberleninka.ru/article/n/povyshenie-nadezhnosti-it-infrastruktury-pri-ispolzovanii-virtualizatsii> (дата обращения: 16.04.2026). – Режим доступа: свободный. – Текст: электронный.
5. Виртуализация и виртуальные машины в подготовке современных ИТ-специалистов: [сайт]. – URL: <https://cyberleninka.ru/article/n/virtualizatsiya-i-virtualnye-mashiny-v-podgotovke-sovremennyh-it-spetsialistov> (дата обращения: 16.04.2026). – Режим доступа: свободный. – Текст: электронный.

© М. Ю. Благодаренко, Т. Ю. Бугакова, 2026

ПРИЛОЖЕНИЕ А АРХИТЕКТУРА ИНФРАСТРУКТУРЫ

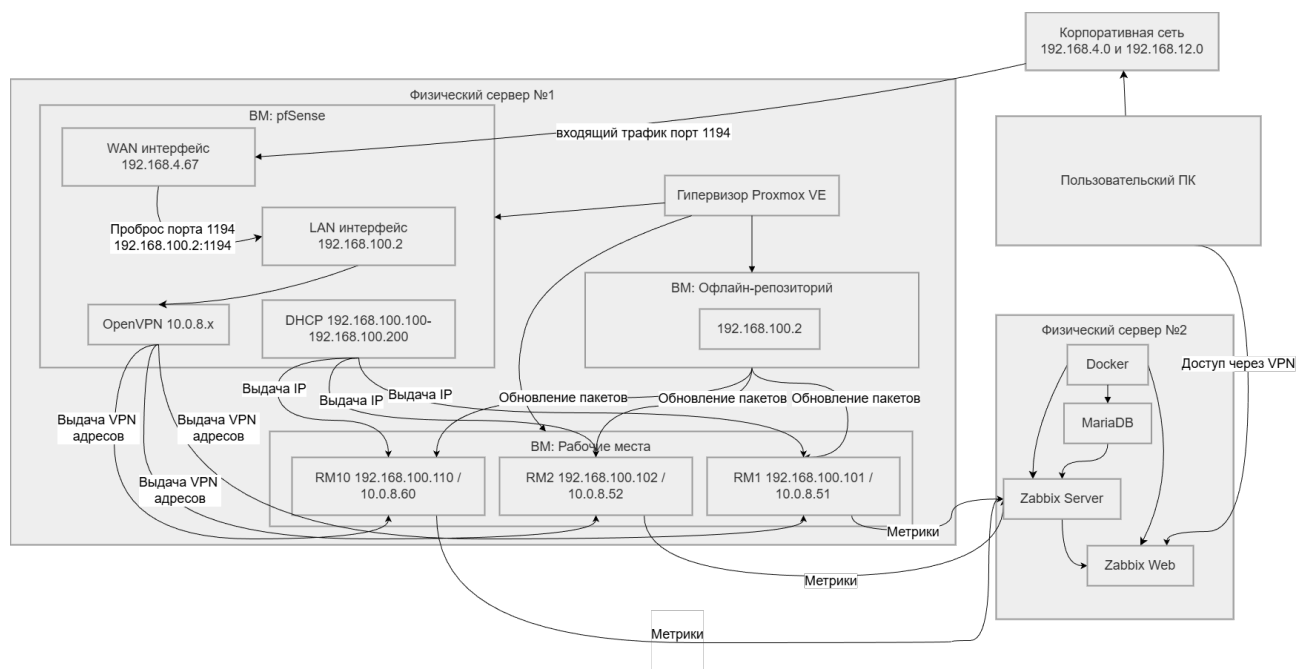


Рис. А.1. Аппаратно-программная архитектура инфраструктуры удаленных рабочих мест с системой мониторинга