**ОРГАНИЗАЦИЯ ЗАЩИТЫ СЕРВЕРНОЙ ИНФРАСТРУКТУРЫ НА БАЗЕ REDOS**

Актуальность проблемы организации защиты серверной инфраструктуры является главной задачей для любого бизнеса или организации. Угрозы безопасности, такие как кибератаки, DDoS-атаки, несанкционированные доступы и утечки данных, представляют собой серьезную проблему, требующий комплексный подход к обеспечению безопасности.

Исследование организации по защите серверной инфраструктуры поможет понять основные принципы безопасности данных, выявить уязвимые места в системах и разработать стратегию по защите цифровых ресурсов. Кроме того, актуальность данной темы подтверждается постоянным развитием технологий и появлением новых угроз для серверных систем.

Цель исследования:разработка стратегии построения многоуровневой системы защиты.

Серверная инфраструктура — это комплекс аппаратных, программных и сетевых ресурсов, обеспечивающих работу ИТ-систем предприятия. Она включает серверы, системы хранения данных, сети, системы виртуализации, резервного копирования, мониторинга и управления. [1]

**Минимизация активных сервисов**

Первый шаг — отключение ненужных служб. Чем меньше сервисов работает, тем меньше поверхность для атаки. Проверить активные соединения можно командой:

* bash
* ss -tulnp

Неиспользуемые демоны (например, FTP или Telnet) следует остановить и удалить.

**Обновление системы**

Уязвимости в ПО — частый вектор атак. REDOS поддерживает обновления через dnf (или apt в некоторых версиях):

* bash
* sudo dnf update --security -y

Рекомендуется настроить автоматические обновления критических пакетов.

**Настройка межсетевого экрана**

Встроенный firewalld или nftables позволяют контролировать трафик. Пример базовых правил:

* bash
* sudo firewall-cmd --permanent --add-service=ssh
* sudo firewall-cmd --permanent --remove-service=http # если не используется
* sudo firewall-cmd --reload

**Защита SSH-доступа**

SSH — основной способ удалённого управления, но без должной настройки он уязвим к брутфорсу.

**Замена паролей на ключи**

Пароли уязвимы к подбору, поэтому лучше использовать аутентификацию по ключам:

* bash
* ssh-keygen -t ed25519
* ssh-copy-id user@server

В файле /etc/ssh/sshd\_config нужно установить:

* PasswordAuthentication no
* PermitRootLogin no

**Ограничение доступа по IP**

Если возможно, стоит разрешить подключение только с доверенных адресов:

* AllowUsers admin@192.168.1.100

**Контроль целостности и мониторинг**

Настройка аудита с помощью auditd

Служба auditd логирует критичные события (изменение файлов, входы пользователей):

* bash
* sudo auditctl -w /etc/passwd -p wa -k passwd\_changes

**Инструменты обнаружения вторжений**

* Fail2Ban — блокирует IP при множественных неудачных попытках входа.
* Rkhunter — проверяет систему на руткиты.

**Резервное копирование**

Даже при надёжной защите возможны инциденты. Важно настроить регулярные бэкапы:

* bash
* tar -czf /backup/server-$(date +%F).tar.gz /etc /var/www

Для автоматизации подойдёт cron или специализированные утилиты (Borg, Rclone).

**Соответствие требованиям ФСТЭК**

* REDOS может использоваться в госсекторе, но требует дополнительной настройки:
* Включение SELinux в режиме enforcing.
* Использование сертифицированных СЗИ (например, КриптоПро для шифрования).
* Настройка журналирования по Приказу № 239.

Защита серверной инфраструктуры требует постоянного мониторинга, обновления стратегий безопасности и внедрения новейших технологий. Только комплексный подход, учитывающий все аспекты — от анализа угроз до технической настройки — способен обеспечить надежную защиту серверного окружения и сохранность конфиденциальной информации.[2]

**Литература:**

1. Аброскин А.С., Гурьянова М.В. НАВЫКИ И ОБЯЗАННОСТИ СИСТЕМНОГО АДМИНИСТРАТОРА // Мировая наука. 2021. №1;
2. Запечников С. В., Милославская Н. Г., Толстой А. И. З-31 Основы построения виртуальных частных сетей. Учебное пособие для вузов. – 2-е изд., стереотип. – М.: Горячая линия–Телеком, 2021. – 248 с;
3. Официальный сайт RED OS. [Электронный ресурс] <https://redos.red-soft.ru/?ysclid=m3nvl57vpa846158518> (дата обращения: 18.12.2024 г.).
4. Документация RED OS. [Электронный ресурс] <https://redos.red-soft.ru/product/docs/> (дата обращения: 04.10.2024 г.).