Практическое руководство: Настройка комплексной безопасности сервера через Webmin

By V B
cze 2, 2026

Данное руководство описывает пошаговый процесс развертывания многоуровневой системы безопасности (ОС $\rightarrow$ OpenCms $\rightarrow$ Apache OFBiz) с использованием исключительно графического интерфейса и модулей панели **Webmin**.

Мы разберем, как защитить систему от четырех ключевых векторов угроз: физического доступа, вторжения из локальной сети (LAN), атак со стороны провайдера/интернета и аппаратных сбоев.

ЭТАП 1: Безопасность на уровне ОС kUbuntu и самой панели Webmin

Защита хост-системы и управляющего интерфейса — это критически важный первый шаг. Все настройки на этом этапе выполняются через стандартные модули Webmin.

1.1. Защита от физического доступа к серверу

Вектор угрозы: злоумышленник имеет физический доступ к корпусу сервера, пытается загрузиться с флешки для сброса паролей или войти в консоль восстановления GRUB.

1. **Создание хэша пароля GRUB (через Webmin):**
    - Перейдите в **Tools (Инструменты)** $\rightarrow$ **Command Shell (Командная строка)**.
    - В поле ввода команды выполните: `grub-mkpasswd-pbkdf2`.
    - Введите ваш будущий сложный пароль GRUB. Скопируйте сгенерированную строку хэша (начинается с `grub.pbkdf2.sha512...`).
2. **Защита загрузчика GRUB паролем (Безопасный метод без блокировки автозапуска):**

    > **КРИТИЧЕСКИЙ РИСК ДЛЯ HEADLESS-СЕРВЕРА:** Если вы просто укажете суперпользователя в GRUB, система по умолчанию заблокирует **все** пункты меню. При любой перезагрузке (например, после отключения электричества) сервер зависнет на этапе загрузки, требуя ввести логин и пароль с физической клавиатуры.
    >
    > **Как сделать правильно:** Нам нужно заблокировать паролем только вход в консоль GRUB (клавиша c) и редактирование параметров ядра (клавиша e), но разрешить системе загружаться в стандартном режиме автоматически и без ввода пароля (`--unrestricted`).

    - В Webmin перейдите в **Tools** $\rightarrow$ **File Manager (Файловый менеджер)**.
    - Вместо редактирования системных скриптов, воспользуйтесь стандартным пользовательским конфигуратором. Перейдите по пути `/etc/grub.d/` и откройте файл

`40_custom` во встроенном редакторе (двойной клик или правая кнопка мыши $\rightarrow$ *Edit*).

- Добавьте в конец файла следующие строки:

```
#   GRUB
set superusers="admin"
#       admin
password_pbkdf2 admin <____grub>
```

- Сохраните файл (кнопка *Save*).
- Теперь проверьте, поддерживает ли ваша ОС автоматический бесконсольный запуск. В Ubuntu/kUbuntu generator меню автоматически добавляет параметр `--unrestricted` к стандартным пунктам меню, если видит настроенных суперпользователей.
- Перейдите в **Command Shell** и примените изменения командой:

```
sudo update-grub
```

- **Проверка безопасности (Обязательно до перезагрузки!):**

  Выполните команду поиска ограничений в сгенерированном файле:

```
grep -E "menuentry|unrestricted" /boot/grub/grub.cfg
```

  What you should see in output: Рядом с вашим дефолтным ядром (первая строка `menuentry 'Ubuntu' ...`) должен обязательно присутствовать флаг `--unrestricted`. Это гарантирует, что обычный запуск пройдет автоматически, а пароль потребуется только при попытке взлома меню загрузки.

3. **План спасения (Если вы всё же заблокировали сервер):**

Если после перезагрузки сервер требует пароль для обычной загрузки, а вы его забыли или ошиблись в хэше:

1. Загрузитесь с любого Live-USB (kUbuntu/Ubuntu).
2. Откройте terminal, смонтируйте системный NVMe-накопитель сервера:

```
sudo mount /dev/nvme0n1p3 /mnt
```

3. Откройте файл `/mnt/etc/grub.d/40_custom` и удалите или закомментируйте строки с `superusers` и `password_pbkdf2`.

4. Примените изменения к GRUB на смонтированном диске. Для этого привяжите виртуальные файловые системы хоста к точке монтирования и выполните обновление внутри среды `chroot`:

```
#    Live-USB
for i in /dev /dev/pts /proc /sys /run; do sudo mount -B $i /mnt$i; done

#    /boot     (, sda1),  :
# sudo mount /dev/sda1 /mnt/boot

#   chroot-     grub
sudo chroot /mnt update-grub

#
sudo umount -R /mnt
```

5. Перезагрузитесь. Сервер снова станет доступен в штатном режиме.

1.2. Защита от вторжения через провайдера (Защита панели Webmin)

Вектор угрозы: Webmin работает на стандартном порту 10000, открытом в интернет, подвергаясь атакам брутфорса и сканированию.

1. **Смена стандартного порта Webmin (Безопасный алгоритм без потери доступа):**

   КРИТИЧЕСКИЙ РИСК БЛОКИРОВКИ И КОНФЛИКТА: Поскольку в системе активен брандмауэр UFW, стандартный графический модуль Webmin "Linux Firewall" (iptables) использовать **запрещено** — они будут перезаписывать правила друг друга.

   Все действия с брандмауэром выполняются через встроенную в Webmin веб-консоль **Command Shell** (Командная строка). Это безопасно, быстро и гарантирует корректность правил UFW.

- **Шаг А: Открываем новый порт в брандмауэре через Webmin.**

   1. В левом меню Webmin перейдите в раздел **Tools (Инструменты)** $\rightarrow$ **Command Shell (Командная строка)**.

   2. В поле ввода команды введите следующую строку для открытия нового скрытого порта (например, `10099`) и перезапуска правил:

      ```
      sudo ufw allow 10099/tcp comment 'Webmin New' && sudo ufw reload
      ```

   3. Нажмите кнопку **Execute command** (Выполнить). Убедитесь, что система вернула ответ об успешном добавлении правила и перезапуске брандмауэра.

- **Шаг Б: Меняем рабочий порт в настройках Webmin.**

    - In the left-hand menu, navigate to **Webmin** $\rightarrow$ **Webmin Configuration (Конфигурация Webmin)** $\rightarrow$ **Ports and Addresses (Порты и адреса)**.
    - В поле **Listen on port (Слушать на порту)** измените стандартное значение `10000` на ваш новый скрытый порт `10099`.
    - Нажмите кнопку **Save (Сохранить)**. Служба Webmin автоматически перезапустится на новом порту.
- **Шаг В: Подключаемся по новому адресу.**
    - Откройте новую вкладку в вашем браузере и введите адрес с новым портом: `https://192.168.0.19:10099/`.
    - Убедитесь, что панель управления успешно загружается, и вы можете войти в систему.
- **Шаг Г: Закрываем старый порт в брандмауэре.**
    - Только после успешного входа по новому порту `10099` вернитесь в Webmin $\rightarrow$ **Tools** $\rightarrow$ **Command Shell**.
    - Введите команду для удаления правила брандмауэра для старого неиспользуемого порта `10000`:

      ```
      sudo ufw delete allow 10000/tcp && sudo ufw reload
      ```

    - Нажмите **Execute command**. Старый порт теперь надежно закрыт для внешней и внутренней сети.

2. **Настройка двухфакторной аутентификации (2FA/TOTP в Webmin 2.x):**

   Что делать, если в системе не установлен необходимый Perl-модуль:

   Webmin скроет или заблокирует метод TOTP защиты, если в самой системе kUbuntu не установлен модуль `Authen::OATH`.

   Чтобы исправить это, перейдите в Webmin $\rightarrow$ **Tools** $\rightarrow$ **Command Shell** и выполните команду:

   ```
   sudo apt update && sudo apt install libauthen-oath-perl -y
   ```

- **Включение 2FA для вашего администратора (Webmin 2.641+):**
    1. Перейдите в раздел **Webmin** $\rightarrow$ **Webmin Users** (Пользователи Webmin).
    2. Кликните по вашему имени пользователя (например, `admin` или `survrus`).
    3. Найдите строку **Two-factor authentication provider** (Провайдер двухфакторной аутентификации).

4. Выберите в выпадающем списке **TOTP Authenticator** (Time-based One-Time Password) и нажмите кнопку **Save** внизу страницы.

5. Webmin отобразит страницу настройки с QR-кодом и текстовым **Secret Key** (например, `AJT6M6D5BZIJXJAX`).

6. **Критически важно:** Скопируйте и надежно сохраните этот текстовый Secret Key в вашем менеджере паролей (Bitwarden/KeePassXC). Он позволит восстановить доступ к Webmin при поломке или утере смартфона.

7. Отсканируйте QR-код мобильным приложением-аутентификатором (Aegis, Google Authenticator, 2FAS) и подтвердите активацию.

3. **Сценарии безопасного доступа к Webmin из интернета (Вместо жесткой блокировки по IP):**

   Если вам жизненно необходим доступ к Webmin из внешней сети (интернета), стандартная блокировка "IP Access Control" (разрешающая только подсеть `192.168.0.0/24`) сделает это невозможным.

   Выберите один из трех сценариев для безопасного удаленного администрирования:

- **Сценарий А: Прямой доступ из интернета (Базовый уровень защиты).**
  - Если у вас нет постоянного VPN-туннеля, вы можете оставить доступ к Webmin открытым для всех внешних IP-адресов.
  - **Как сделать:** В модуле **Webmin Configuration** $\rightarrow$ **IP Access Control** оставьте переключатель в режиме **Allow from all addresses** (Разрешить со всех адресов).
  - **Как защититься в этом случае:**
    1. Ваш скрытый порт `10099` защитит от массовых автоматических сканеров портов.
    2. Включенный **2FA (TOTP)** делает подбор пароля бесполезным (злоумышленник не войдет без одноразового кода на вашем телефоне).
    3. В системе должен обязательно работать **Fail2ban** (уже защищает службу Webmin, блокируя IP-адрес атакующего на 24 часа после 3 неудачных попыток ввода пароля).
- **Сценарий Б: Доступ через собственный защищенный VPN-туннель (Рекомендуемый / Профессиональный уровень).**
  - Самый надежный подход: порты управления сервером (Webmin, SSH) полностью закрыты для интернета на роутере. Для входа на server вы сначала включаете VPN на вашем Mac, Linux или смартфоне, а затем открываете Webmin по его локальному IP: `https://192.168.0.19:10099`.

- **Как сделать:** Настройте службу **WireGuard VPN** (на Сервере 1 или вашем роутере) с виртуальной подсетью (например, `10.8.0.0/24`).

- В настройках Webmin **IP Access Control** выберите **Only allow from listed addresses** и введите:

  ```
  192.168.0.0/24 10.8.0.0/24 127.0.0.1
  ```

- Нажмите **Save**. Доступ открыт только для домашней сети и ваших VPN-клиентов из любой точки мира.

- **Сценарий B: Доступ через Cloudflare Tunnel с авторизацией Zero Trust (Максимальный уровень).**

  - Если сервер находится за NAT провайдера (нет белого IP), настройте **cloudflared** для публикации Webmin.

  - В панели Cloudflare Zero Trust настройте правило авторизации (Access Application): при попытке открыть веб-панель из интернета, Cloudflare сначала потребует ввести одноразовый пин-код, высылаемый на вашу личную почту, и только после этого перенаправит трафик в защищенный туннель до Webmin. IP Access Control на самом сервере при этом может оставаться в локальном режиме.

1.3. Защита от атак из локальной сети (LAN)

Вектор угрозы: компрометация одного из домашних/офисных устройств, сканирование портов SSH и Samba внутри сети.

1. **Ограничение и перевод службы SSH на ключи:**

   - Перейдите в **Servers (Службы)** $\rightarrow$ **SSH Server (SSH-сервер)**.

   - Откройте вкладку **Authentication (Аутентификация)**.

   - Установите параметры:

     - *Allow authentication by password? (Разрешить вход по паролю?)* $\rightarrow$ **No** (Вход будет возможен только по ранее импортированным SSH-ключам).

     - *Permit login by root? (Разрешить вход root?)* $\rightarrow$ **No** (Запрещает прямое подключение суперпользователя).

   - Нажмите **Save**.

   - Перейдите во вкладку **Access Control (Контроль доступа)**. В полях **Port (Порт)** смените стандартный порт 22 на альтернативный (например, 2222). Нажмите **Save**, а затем нажмите **Apply Changes (Применить изменения)** в верхнем правом углу модуля.

2. **Настройка брандмауэра (UFW через Webmin Command Shell — Сценарий A):**

- Перейдите в **Tools (Инструменты)** $\rightarrow$ **Command Shell (Командная строка)**.
- Для реализации **Сценария А (Прямой доступ из интернета с защитой через 2FA и Fail2ban)** выполните последовательно команды для открытия портов управления внешнему миру:

```
#   :  ,
sudo ufw default deny incoming
sudo ufw default allow outgoing

#  - (HTTP/HTTPS)
sudo ufw allow 80/tcp comment 'Apache HTTP'
sudo ufw allow 443/tcp comment 'Apache HTTPS'

#  :        (WAN/LAN)
#    , 2FA  Fail2ban
sudo ufw allow 2222/tcp comment 'SSH WAN/LAN'
sudo ufw allow 10099/tcp comment 'Webmin WAN/LAN'

#    ERP OFBIZ:
#   8443      ERP   IP 89.229.203.98
# ([https://89.229.203.98:8443/catalog/control/FindProduct](https://89.229.2
sudo ufw allow 8443/tcp comment 'OFBiz Temporary Direct HTTPS'

#   (Samba) -      192.168.0.0/24
sudo ufw allow from 192.168.0.0/24 to any port 137 proto udp comment 'Samba
sudo ufw allow from 192.168.0.0/24 to any port 138 proto udp comment 'Samba
sudo ufw allow from 192.168.0.0/24 to any port 139 proto tcp comment 'Samba
sudo ufw allow from 192.168.0.0/24 to any port 445 proto tcp comment 'Samba

#
sudo ufw reload
```

- Нажмите кнопку **Execute command** (Выполнить). Теперь ваш сервер kUbuntu защищен надежным сетевым экраном, настроенным под прямой доступ из интернета.

1.4. Защита от аппаратных сбоев

Вектор угрозы: внезапное отключение электроэнергии (повреждение баз данных), незамеченный износ ячеек памяти системного SSD.

1. **Настройка SMART-мониторинга дисков:**
   - Перейдите в **Hardware (Оборудование)** $\rightarrow$ **SMART Drive Status (Статус дисков SMART)**.
   - Выберите ваш системный SSD и диски внешнего «зоопарка».

- Активируйте регулярные фоновые тесты накопителей. При выявления критических ошибок (деградации ячеек SSD или появлении битых секторов на HDD WD Passport) Webmin отправит вам уведомление на почту.

2. **Интеграция ИБП (UPS) для безопасного выключения:**
    - Подключите ИБП к серверу по USB-кабелю.
    - Перейдите в **System (Система)** $\rightarrow$ **Software Packages (Программные пакеты)**. Установите пакет `apcupsd` или `nut`.
    - Перейдите в **Tools** $\rightarrow$ **File Manager** и откройте конфигурационный файл ИБП `/etc/apcupsd/apcupsd.conf`.
    - Убедитесь, что параметры автовыключения настроены на безопасный предел батареи (например, `BATTERYLEVEL 15`).
    - *Результат:* При долгой аварии по питанию система сама корректно размонтирует MergerFS, завершит процессы СУБД, Tomcat и OFBiz, предотвращая порчу данных.

ЭТАП 2: Безопасность на уровне OpenCms (Tomcat) через Webmin

Наша цель — полностью изолировать процессы Java-приложения от операционной системы и ограничить сетевую видимость Tomcat внутренними интерфейсами.

2.1. Изоляция процессов и лишение прав root

Вектор угрозы: взлом OpenCms через веб-уязвимость (например, загрузку файлов) дает злоумышленнику права root на сервере, если Tomcat запущен некорректно.

1. **Создание изолированной группы и пользователя:**
    - Проще всего это сделать одной быстрой командой в **Tools** $\rightarrow$ **Command Shell**:

      ```
      sudo groupadd tomcat && sudo useradd -s /usr/sbin/nologin -g tomcat -d /opt/
      ```

    - *Примечание:* Использование системного шелла `/usr/sbin/nologin` гарантирует, что злоумышленник не сможет залогиниться под учетной записью `tomcat`.
2. **Смена владельца файлов Tomcat через Webmin:**
    - Перейдите в **Tools** $\rightarrow$ **File Manager**.
    - Найдите папку установки Tomcat (например, `/opt/opencms/tomcat/`).
    - Кликните правой кнопкой мыши по папке и выберите **Info** (или **Properties / Свойства**).

- В полях **Owner (Владелец)** и **Group (Группа)** выберите созданного пользователя `tomcat` и группу `tomcat`.

- Отметьте галочку **Apply to subfolders (Применить к подпапкам / рекурсивно)** и нажмите **Save**.

3. **Привязка службы в Systemd:**

   - В **File Manager** откройте файл службы `/etc/systemd/system/tomcat.service`.

   - Убедитесь, что в секции `[Service]` прописаны строки:

     ```
     User=tomcat
     Group=tomcat
     ```

   - Перейдите в **System** $\rightarrow$ **Bootup and Shutdown (Загрузка и выключение)**. Выделите службу `tomcat` в списке и нажмите **Restart (Перезапустить)**.

2.2. Защита локальных сетевых портов

Вектор угрозы: обращение злоумышленника к Tomcat напрямую по порту 8080 в обход Reverse Proxy Apache и правил SSL.

1. **Биндинг порта 8080 на 127.0.0.1:**

   - В **File Manager** откройте файл `/opt/opencms/tomcat/conf/server.xml`.

   - Найдите XML-тег `<Connector port="8080"` и добавьте внутрь параметр `address="127.0.0.1"`:

     ```
     <Connector port="8080" protocol="HTTP/1.1"
                address="127.0.0.1"
                connectionTimeout="20000"
                redirectPort="8443" />
     ```

   - Сохраните файл. Перезапустите службу Tomcat через модуль **Bootup and Shutdown**.

   - *Результат:* Теперь порт 8080 физически закрыт для внешней сети и доступен только для локального прокси-сервера Apache.

2.3. Безопасность веб-интерфейса и сессий

Вектор угрозы: подбор паролей к стандартной панели управления Tomcat `/manager` или перехват сессионных кук администратора в локальной сети.

1. **Удаление дефолтных приложений через File Manager:**

- Перейдите в папку `/opt/opencms/tomcat/webapps/`.
- Выделите и безвозвратно удалите каталоги: `manager`, `host-manager`, `examples`, `docs`.

2. **Защита Cookies в веб-конфигурации:**
   - В **File Manager** откройте файл `/opt/opencms/tomcat/conf/web.xml`.
   - Найдите блок `<session-config>` и приведите его к следующему защищенному виду:

```
<session-config>
    <session-timeout>30</session-timeout>
    <cookie-config>
        <http-only>true</http-only>
        <secure>true</secure>
    </cookie-config>
</session-config>
```

   - *Результат:* Флаг `http-only` запрещает JavaScript читать ваши куки авторизации (защита от XSS-атак), а `secure` гарантирует передачу куки сессии только внутри зашифрованного HTTPS-соединения.

3. **Перезапуск сервера Tomcat для применения изменений:**
   - Для того чтобы новые параметры безопасности сессионных кук вступили в силу, необходимо перезапустить сервер Tomcat. Выполните это одним из следующих способов:
     - **Способ А: Через Command Shell (Командная строка Webmin):**

```
sudo systemctl restart tomcat
```

     - **Способ Б: Через графический интерфейс Webmin:**

       Перейдите в **System (Система)** $\rightarrow$ **Bootup and Shutdown (Загрузка и выключение)**, найдите в списке службу `tomcat`, установите напротив неё флажок и нажмите кнопку **Restart (Перезапустить)** внизу страницы.

ЭТАП 3: Безопасность на уровне Apache OFBiz и баз СУБД через Webmin

ERP-система OFBiz хранит коммерческие секреты, MRP-планы и расчеты себестоимости. Наша задача — изолировать СУБД и предотвратить перегрузку сервера при сложных расчетах.

3.1. Изоляция и защита встроенной СУБД Apache Derby

Вектор угрозы: несанкционированный локальный доступ к файлам базы данных или некорректные права доступа, позволяющие другим пользователям/службам читать или изменять критические данные.

Поскольку ваш Apache OFBiz работает на встроенной (embedded) СУБД **Apache Derby**, она не запускает отдельный независимый сетевой процесс и по умолчанию не слушает внешние порты (такие как 5432 или 3306). Это обеспечивает великолепную сетевую изоляцию "из коробки". Однако файлы таблиц физически лежат на диске, и их защиту необходимо организовать на уровне операционной системы.

1. **Ограничение прав доступа к файлам Derby через File Manager:**
    - Перейдите в **Tools** $\rightarrow$ **File Manager**.
    - Найдите папку базы данных по пути расположения вашего проекта: `/srv/Ofbiz/IG /runtime/data/derby/`.
    - Кликните правой кнопкой мыши по папке `derby` и выберите **Info** (или **Permissions / Свойства**).
    - В полях **Owner (Владелец)** и **Group (Группа)** убедитесь, что установлена выделенная учетная запись `ofbiz:ofbiz` (см. шаг создания пользователя в `ofbiz.service`).
    - В разделе прав доступа (Permissions) установите маску **`0700`** (`rwx------`) для каталогов и **`0600`** (`rw-------`) для вложенных файлов. Это полностью заблокирует возможность чтения и копирования файлов базы данных для любых других пользователей сервера (включая пользователя `tomcat` от OpenCms).
    - Отметьте галочку **Apply to subfolders (Применить к подпапкам / рекурсивно)** и нажмите **Save**.

3.2. Настройка Apache Webserver для защиты от DoS-атак на ERP

Вектор угрозы: перегрузка ERP-системы большим количеством одновременных тяжелых запросов.

1. **Добавление лимитов в хост erp.in-genium.in:**
    - Перейдите в **Servers** $\rightarrow$ **Apache Webserver**.
    - Найдите в списке виртуальных хостов ваш хост `erp.in-genium.in` на порту **443** (HTTPS) и кликните по нему.
    - Нажмите на кнопку **Edit Directives (Редактировать директивы)**.
    - Вставьте следующие лимиты для защиты от флуда и атак типа Slowloris (требуется установленный модуль `mod_qos`):

      ```
      #       ERP
      QS_LocRequestLimitDefault 30
      #     (    Slowloris)
      QS_SrvMinDataRate 120
      ```

    - Сохраните и нажмите **Apply Changes** в верхнем углу модуля Apache Webserver.

3.3. Аудит встроенной СУБД Derby и ротация демо-пользователей

Поскольку Apache Derby является встроенной базой данных, вы не можете администрировать её таблицы и данные напрямую через стандартные модули СУБД в Webmin (MySQL или PostgreSQL Database Server). Управление учетными записями внутри Derby выполняется через встроенную административную панель самого OFBiz — **Webtools**.

1. **Блокировка демонстрационных аккаунтов через веб-интерфейс:**
    - Перейдите по защищенному адресу вашей ERP в раздел веб-инструментов: `https://erp.in-genium.in/webtools/control/main`.
    - Перейдите во вкладку **Entity Engine** $\rightarrow$ **Entity Data Maintenance** (Обслуживание данных сущностей).
    - Найдите в списке сущностей (таблиц) системную сущность **UserLogin** (используйте поиск на странице).
    - Нажмите кнопку **Find** (Поиск) для вывода списка всех зарегистрированных пользователей.
    - Найдите демонстрационные системные записи (`demouser`, `flexadmin`, `company`, `gregory`).
    - Кликните на каждую запись и измените параметр **Enabled** на значение **`N`** (или заполните поле `disabledDateTime` текущим временем).

        > **Внимание:** Удалять записи демо-пользователей напрямую не рекомендуется, так как на них в демонстрационной базе данных могут ссылаться выполненные проводки и складские документы. Блокировка (`Enabled = N`) — самый безопасный метод.

    - Для учетной записи главного администратора **`admin`** принудительно задайте новый сложный, уникальный пароль.

3.4. Защита от аппаратного исчерпания ресурсов при расчете MRP

Вектор угрозы: запуск сложного расчета планирования производства в OFBiz утилизирует 100% процессора Intel N100, вызывая «зависание» сервера и падение сайта OpenCms. Мы лимитируем ресурсы OFBiz через встроенные cgroups ядра Linux.

1. **Настройка лимитов службы в Systemd через Webmin:**
    - Перейдите в **Tools** $\rightarrow$ **File Manager**.
    - Откройте файл службы `/etc/systemd/system/ofbiz.service`.
    - В секцию `[Service]` добавьте параметры жесткого ограничения приоритета и использования ядер процессора:

```
[Service]
Nice=10
#  ERP-  50%    (2   4)
```

```
CPUQuota=50%
```

- Сохраните файл.
- Перейдите в **Tools** $\rightarrow$ **Command Shell** и выполните команду для перезагрузки демона systemd:

  ```
  sudo systemctl daemon-reload
  ```

- Перейдите в **System** $\rightarrow$ **Bootup and Shutdown**, выберите службу `ofbiz` и нажмите **Restart**.
- *Результат:* Теперь, даже если OFBiz начнет выполнять тяжелейший многочасовой расчет калькуляций, ядро Linux выделит ему только 50% ресурсов процессора Intel N100, оставив остальные 50% ресурсов для моментальной отдачи страниц OpenCms внешним клиентам по адресу `in-genium.in`.