



# Intecso. Руководство пользователя

## Установка Intecso

### 1. Подготовка образа установки:

Скачайте образ Intecso с официального сайта проекта, распакуйте его.

- Используйте программу для распаковки образа (например, 7zip для Windows). Для систем на базе Unix используйте команду **bzip2 -d OPNsense-<filename>.bz2**.
- Запишите образ на USB-накопитель, используя соответствующую вашей операционной системе команду **dd** или программу записи (например, Etcher или Rufus для Windows).

### 2. Создание загрузочного носителя:

Запись образа на USB-накопитель или жесткий диск выполняется различными способами в зависимости от операционной системы:

- **FreeBSD:** Используйте **dd if=OPNsense-##.#.##-[Type]-[Architecture].img of=/dev/daX bs=16k**, где **X** - номер устройства вашего USB-накопителя (проверьте с помощью **dmesg**).
- **OpenBSD:** Используйте **dd if=OPNsense-##.#.##-[Type]-[Architecture].img of=/dev/rsd6c bs=16k**, где устройство должно быть полным (например, 'C' раздел в терминологии Windows/DOS).
- **Linux:** Команда **sudo dd if=OPNsense-##.#.##-[Type]-[Architecture].img of=/dev/sdX bs=16k** позволит записать образ, где **X** - имя IDE устройства вашего USB (проверьте с помощью **hdparm -i /dev/sdX**).
- **macOS:** Используйте **sudo dd if=OPNsense-##.#.##-[Type]-[Architecture].img of=/dev/rdiskX bs=64k**, где **X** - номер дискового устройства вашей карты (проверьте в Disk Utility)<sup>1</sup>.
- **Windows:** Для записи используйте программы **physdiskwrite**, **Etcher** или **Rufus**.

### 3. Подготовка системы к загрузке:



Убедитесь, что можете получить доступ к консоли. Также необходимо знать, как получить доступ к меню загрузки или к BIOS/UEFI, чтобы загрузиться с медиа.

### **Процесс загрузки и установки:**

1. После загрузки с установочного носителя, на экране появится меню установки Intesco.
2. Вам будет предложено войти в систему с использованием предоставленных учетных данных (обычно пользователь root).
3. Выберите "Guided installation" для запуска полуавтоматической установки.
4. Выберите диск, на который будет установлена система.
5. Выберите режим разметки диска: GPT для новых систем с UEFI или MBR для старых систем с BIOS.
6. Подождите, пока система установится на выбранный диск.
7. Задайте пароль для пользователя root.
8. После завершения установки перезагрузите систему и извлеките установочный носитель.

#### *После перезагрузки:*

1. После перезагрузки системы появится меню консоли Intesco.
2. Вы увидите IP-адрес интерфейса LAN, который можно изменить, выбрав соответствующий пункт меню.

### **Использование функции Importer:**

5. Если у вас уже есть установленный Intesco, и конфигурация осталась нетронутой, вы можете использовать функцию Importer для запуска новой версии в памяти с существующей конфигурацией или для миграции конфигурации на новое оборудование.

### **Взаимодействие с Live-средой:**

6. После загрузки с образа Intesco вы окажетесь в Live-среде, где сможете взаимодействовать с системой через локальную консоль, веб-интерфейс (HTTPS) или SSH. Стандартные учетные данные для входа в систему - это пользователь **root** с заданным при установке паролем.

## **Первоначальная настройка Intesco**



## 1. Подключение к Intecso

- Подключите ваш компьютер напрямую к одному из LAN-портов Intecso.
- Убедитесь, что ваш компьютер настроен для автоматического получения IP-адреса через DHCP.

## 2. Доступ к веб-интерфейсу

- Откройте веб-браузер и введите IP-адрес, заданный по умолчанию для LAN интерфейса Intecso (например, 192.168.1.1).
- Введите стандартные учетные данные: обычно это **root** для имени пользователя и **Intecso** для пароля.

## 3. Мастер настройки

- После входа в систему рекомендуется запустить мастер настройки, который пошагово проведет вас через основные настройки системы.

## 4. Настройка интерфейсов

- Настройте WAN и LAN интерфейсы. WAN интерфейс обычно настраивается для получения IP-адреса через DHCP от вашего интернет-провайдера, в то время как для LAN-интерфейса может быть задан статический IP-адрес, который использовался для доступа к веб-интерфейсу.
- Важно также отключить любые опции аппаратной проверки (например, "Disable hardware checksum offload"), если они не поддерживаются вашим оборудованием.

## 5. Настройка общих системных параметров

- Настройте системные параметры, такие как имя хоста, домен, временную зону и DNS-серверы через раздел "System > Settings > General" в веб-интерфейсе.

## 6. Настройка администрирования

- В разделе "System > Settings > Administration" настройте параметры доступа к веб-интерфейсу, такие как протокол (HTTPS), порт (обычно 443) и другие параметры безопасности.

## 7. Настройка VLAN



- Если вам необходимо создать VLAN, это делается через раздел "Interfaces > Other Types > VLAN". Задайте соответствующий тег VLAN и приоритет, если требуется.

## **8. Присвоение интерфейсов**

- После создания VLAN необходимо назначить его определенному интерфейсу в разделе "Interfaces > Assignments". Это позволяет создать отдельные физические или логические сети в Intesco.

## **9. Дополнительные настройки интерфейса**

- Для каждого интерфейса, такого как WAN, LAN и созданные VLAN, может потребоваться настройка дополнительных параметров, таких как IP-адрес, маска подсети и шлюз по умолчанию.

## **10. Настройка безопасности**

- Ознакомьтесь с настройками брандмауэра, чтобы обеспечить защиту вашей сети. Настройте правила, которые будут управлять трафиком через Intesco.

## **11. Обновление ПО**

- Убедитесь, что ваш Intesco обновлен до последней версии ПО. Это можно сделать через раздел "System > Firmware".

## **12. Резервное копирование и восстановление**

- Настройте резервное копирование и восстановление системы через раздел "System > Backup".

## **13. Мониторинг и отчетность**

- Настройте систему мониторинга и отчетности для отслеживания производительности и состояния вашего Intesco.

## **14. Дополнительные службы**

- Исследуйте и настройте дополнительные службы, такие как VPN, DHCP сервер, DNS-резолвер и другие функции в соответствии с вашими потребностями.

## **15. Консольный доступ**



- Для дополнительных настроек или устранения неполадок вы можете использовать консольный доступ. Подключитесь через порт или SSH, используя стандартные учетные данные.

По мере того как вы будете продвигаться через каждый из этих шагов, следуйте подсказкам и рекомендациям, представленным в мастере настройки и справочных материалах веб-интерфейса. Убедитесь, что вы сохраняете изменения на каждом этапе и регулярно проверяйте работоспособность настроенных функций.

## Подробная настройка Intecso

### 1. Определение шлюзов

Шлюзы определяют возможные маршруты, которые могут быть использованы для доступа к другим сетям, таким как интернет. Вы можете управлять всеми путями, доступными для вашего брандмауэра, в разделе System->Intecsos->Single. Эти шлюзы могут быть определены вручную или предоставлены автоматически динамически настроенными интерфейсами, такими как DHCP.

### 2. Автоматические и статические маршруты

Когда шлюз генерируется автоматически (например, **WAN\_DHCP**), у вас все еще есть возможность изменить его настройки. Для маршрутизации определенных сетей можно использовать статические маршруты, которые настраиваются в System->Routes->Configuration. Может быть только один маршрут по умолчанию для каждого IP-протокола (IPv4, IPv6), который используется, когда нет другого подходящего статического маршрута.

### 3. Приоритет и настройки Upstream

У шлюзов есть приоритеты, которые помогают определить, какой из них использовать. Они варьируются от **1** (очень важно) до **255** (наименее важно). Также есть настройка 'upstream', которая отмечает шлюз как кандидата на роль шлюза по умолчанию. Если шлюзы настроены на мониторинг, их статус учитывается при выборе, и вы можете включить 'Переключение шлюза' для динамических изменений шлюза по умолчанию в System->Settings->General.

### 4. Основные настройки шлюза

- **Отключено:** Временно отключить шлюз.



- **Имя:** Присвоить уникальное имя для идентификации.
- **Описание:** Предоставить описание (не обязательно).
- **Интерфейс:** Указать подключенный интерфейс.
- **Семейство адресов:** Выбрать между IPv4 или IPv6.
- **IP-адрес:** Установить IP-адрес шлюза, который может быть динамическим, если он создается автоматически.
- **Upstream Intecso:** Отметить шлюз как кандидата на роль шлюза по умолчанию.
- **Far Intecso:** Разрешить шлюзу находиться за пределами подсети интерфейса.
- **Отключить мониторинг шлюза:** Опция рассматривать шлюз всегда в режиме онлайн.
- **IP-мониторинг:** Установить альтернативный адрес для мониторинга, удостоверившись, что он доступен через интерфейс.
- **Отметить шлюз как неработающий:** Определить шлюз как неработающий, исключив его из выбора по умолчанию.
- **Приоритет:** Установить приоритет для определения важности шлюза.

## 5. VLAN и правила брандмауэра

При работе с VLAN рекомендуется пятиэтапный процесс: подготовка сетевой среды, создание VLAN, настройка интерфейсов VLAN, настройка правил брандмауэра для VLAN и тестирование конфигурации. Это обеспечивает правильное управление трафиком и сегментацию в соответствии с вашими сетевыми потребностями.

## 6. Настройка DHCP и DNS

Настройте шлюз как DHCP и сервер имен, перейдя в Services > Unbound DNS > General. Здесь вы можете управлять настройками DNSSEC, статическими привязками DHCP и перенаправлением DNS-запросов. Обязательно настройте дополнительные опции для исходящих сетей по мере необходимости.

## 7. Настройка отказоустойчивости и многоканального подключения



ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "ИНСАЙТТЕХСОЛЮШНС"

Для сред с многоканальным подключением настройка отказоустойчивости включает добавление IP-адресов для мониторинга к шлюзам, создание групп шлюзов, настройку DNS для каждого шлюза и реализацию маршрутизации на основе политик для использования группы шлюзов. Должны быть добавлены соответствующие правила брандмауэра, особенно для DNS-трафика, предназначенного для самого брандмауэра.