

ПРАВИЛА КОРИСТУВАННЯ VPS

STHost.pro

Дата останнього оновлення: 23 серпня 2025р

Дата набрання чинності: 25 серпня 2025р

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Ці Правила користування VPS (Virtual Private Server) (далі - "Правила") регулюють використання послуг віртуальних приватних серверів Фізичної особи-підприємця Діхтярь Ірини Олександрівни (далі - "Провайдер", "STHost.pro").

1.2. VPS (Virtual Private Server) - це віртуалізована серверна среда з гарантованими ресурсами, root-доступом та повним контролем над операційною системою.

1.3. Використання послуг VPS означає повну згоду з цими Правилами, Загальними умовами обслуговування та всіма супутніми документами STHost.pro.

1.4. Ці Правила доповнюють загальні правила використання хостингу та містять специфічні вимоги для VPS послуг.

2. ВІДОМОСТІ ПРО ПРОВАЙДЕРА

ФОП Діхтярь Ірина Олександрівна

- РНОКПП: 3009915262
- Адреса: 49047, м. Дніпро, вул. Холодноярська, 10, кв. 9
- Телефон: +38(097)-714-19-80
- Email: pllanoiv@gmail.com
- Веб-сайт: <https://sthost.pro>
- Дата реєстрації: 18.08.2025

3. ВИЗНАЧЕННЯ ТА ТЕРМІНОЛОГІЯ

3.1. **VPS (Virtual Private Server)** - віртуальний приватний сервер з ізольованими ресурсами.

3.2. **Hypervisor** - програмне забезпечення для створення та управління віртуальними машинами.

3.3. **Root-доступ** - повні адміністративні права в операційній системі.

3.4. **SSH** - протокол для безпечного віддаленого доступу до сервера.

3.5. **Snapshot** - миттєвий знімок стану VPS.

3.6. **Backup** - резервна копія даних VPS.

3.7. **ISO** - образ операційної системи для встановлення.

3.8. **KVM/OpenVZ/Xen** - технології віртуалізації.

3.9. **Bandwidth** - пропускна здатність мережі.

3.10. **IOPS** - кількість операцій введення-виведення в секунду.

4. ТИПИ VPS ПОСЛУГ

4.1. LINUX VPS

4.1.1. Підтримувані операційні системи:

- Ubuntu (18.04, 20.04, 22.04, 24.04 LTS)
- CentOS (7, 8, 9)
- Debian (10, 11, 12)
- AlmaLinux (8, 9)
- Rocky Linux (8, 9)
- openSUSE
- Arch Linux

4.1.2. Панелі управління:

- Стандартний SSH доступ
- Веб-панелі: ispmanager

4.2. WINDOWS VPS

4.2.1. Підтримувані версії:

- Windows Server 2019
- Windows Server 2022
- Windows 10/11 (для розробки)

4.2.2. Ліцензування:

- Ліцензії Windows Server включені в тариф
- Додаткові CAL ліцензії за окрему плату
- MSDN підписки за домовленістю

4.3. MANAGED VPS

4.3.1. Управління системою:

- Встановлення та налаштування ОС
- Регулярне оновлення системи
- Моніторинг стану сервера
- Базове адміністрування

4.3.2. Технічна підтримка:

- Розширена підтримка 24/7
- Допомога з налаштуванням ПЗ
- Усунення проблем з продуктивністю
- Консультації з оптимізації

5. ТЕХНІЧНІ ХАРАКТЕРИСТИКИ ТА РЕСУРСИ

5.1. ГАРАНТОВАНІ РЕСУРСИ

5.1.1. Процесорні ресурси:

- Гарантовані CPU ядра згідно з тарифом
- Можливість burst до додаткових ядер
- Пріоритетний доступ до CPU ресурсів
- Без обмежень на тип процесів

5.1.2. Оперативна пам'ять:

- Гарантована RAM згідно з тарифним планом
- Повний контроль над використанням
- Можливість swap файлів
- ECC пам'ять на Enterprise тарифах

5.1.3. Дисковий простір:

- SSD диски високої швидкості
- Гарантований IOPS згідно з тарифом
- Можливість додаткових дисків
- RAID захист даних

5.1.4. Мережеві ресурси:

- Гарантована пропускна здатність
- Виділена IP адреса
- Можливість додаткових IP
- DDoS захист базового рівня

5.2. ТЕХНІЧНІ ОБМЕЖЕННЯ

5.2.1. Загальні обмеження:

- Максимальна кількість одночасних з'єднань: 10,000
- Максимальний розмір одного файлу: без обмежень
- Кількість процесів: без жорстких лімітів
- Кількість відкритих файлів: згідно з системними налаштуваннями

5.2.2. Мережеві обмеження:

- Швидкість мережі згідно з тарифом (100 Mbps - 1 Gbps)
- Місячний трафік згідно з планом
- Додатковий трафік: за встановленими тарифами
- Заборона на порушення мережевих протоколів

6. УСТАНОВКА ТА НАЛАШТУВАННЯ

6.1. ПОЧАТКОВЕ РОЗГОРТАННЯ

6.1.1. Процес активації:

- Час розгортання: до 30 хвилин після оплати
- Автоматична установка обраної ОС
- Надсилання root/Administrator паролів на email
- Доступ до панелі управління VPS

6.1.2. Початкові налаштування:

- Зміна стандартних паролів (обов'язково)
- Налаштування SSH ключів
- Конфігурація мережевих параметрів
- Установка базового ПЗ безпеки

6.2. ПЕРЕУСТАНОВКА СИСТЕМИ

6.2.1. Умови переустановки:

- Безкоштовна переустановка: 1 раз на місяць
- Додаткові переустановки: 100 грн за процедуру
- Повне видалення всіх даних
- Час переустановки: до 60 хвилин

6.2.2. Резервування даних:

- Клієнт самостійно відповідає за backup перед переустановкою
- Провайдер не несе відповідальності за втрачені дані
- Рекомендується створення snapshot перед переустановкою

6.3. КАСТОМНА КОНФІГУРАЦІЯ

6.3.1. Власні ISO образи:

- Можливість використання власних ISO
- Перевірка образів на безпеку
- Підтримка стандартних форматів
- Додаткова плата: 200 грн за установку

6.3.2. Спеціальні налаштування:

- Налаштування мережевої конфігурації
- Встановлення додаткового ПЗ
- Конфігурація безпеки
- Консультації по телефону/email

7. ПРАВА ТА ОБМЕЖЕННЯ ROOT ДОСТУПУ

7.1. ДОЗВОЛЕНІ ДІЇ

7.1.1. Системне адміністрування:

- Повний контроль над операційною системою
- Встановлення будь-якого сумісного ПЗ
- Налаштування мережевих сервісів
- Створення користувачів та управління правами

7.1.2. Серверне програмне забезпечення:

- Веб-сервери (Apache, Nginx, IIS)
- Бази даних (MySQL, PostgreSQL, MongoDB)
- Мови програмування та середовища виконання
- Системи моніторингу та логування

7.1.3. Мережеві сервіси:

- VPN сервери (за умови дотримання законів)
- Email сервери з антиспам захистом
- DNS сервери
- Проксі сервери (для власних потреб)

7.2. ЗАБОРОНЕНІ ДІЇ

7.2.1. Незаконна діяльність:

- Хакерські атаки на інші системи
- Розповсюдження шкідливого ПЗ
- Фішинг та соціальна інженерія
- Порушення авторських прав

7.2.2. Мережеві зловживання:

- DDoS атаки будь-якого типу
- Масове сканування портів
- Спам розсилки без згоди отримувачів
- Відкриті relay сервери

7.2.3. Ресурсні зловживання:

- Майнінг криптовалют (без спеціального дозволу)
- Процеси, що монополізують ресурси
- Порушення роботи hypervisor
- Спроби доступу до інших VPS

7.3. БЕЗПЕКА СИСТЕМИ

7.3.1. Обов'язкові заходи безпеки:

- Регулярне оновлення операційної системи
- Використання сильних паролів

- Налаштування файрволу
- Відключення непотрібних сервісів

7.3.2. Рекомендовані заходи:

- Використання SSH ключів замість паролів
- Встановлення систем виявлення вторгнень
- Регулярне створення backup
- Моніторинг логів системи

8. МЕРЕЖЕВІ НАЛАШТУВАННЯ ТА IP АДРЕСИ

8.1. IP АДРЕСАЦІЯ

8.1.1. Базова IP адреса:

- Одна виділена IPv4 адреса включена в тариф
- Статична IP адреса
- Повний контроль над конфігурацією
- Можливість зміни hostname та PTR запису

8.1.2. Додаткові IP адреси:

- Додаткові IPv4: 100 грн/місяць за адресу
- IPv6 підмережі: безкоштовно
- Максимум 8 додаткових IPv4 на VPS
- Обґрунтування необхідності додаткових IP

8.1.3. Географічне розташування:

- IP адреси українського сегменту
- Можливість IP з інших регіонів за домовленістю
- Інформація про геолокацію IP
- Підтримка anycast для DNS серверів

8.2. МЕРЕЖЕВА КОНФІГУРАЦІЯ

8.2.1. Мережеві інтерфейси:

- Ethernet інтерфейси з повним контролем
- Можливість створення VLAN
- Bonding інтерфейсів на Enterprise планах
- Налаштування QoS правил

8.2.2. DNS налаштування:

- Власні DNS сервери
- Управління зонними файлами
- Можливість делегування субдоменів
- Підтримка DNSSEC

8.3. ЗАХИСТ ТА БЕЗПЕКА МЕРЕЖІ

8.3.1. DDoS захист:

- Базовий DDoS захист включений
- Захист до 1 Gbps атак
- Розширений захист: за додатковою платою
- Автоматична фільтрація шкідливого трафіку

8.3.2. Мережевий файрвол:

- Програмний файрвол в ОС
- Можливість налаштування iptables/firewalld
- Мережевий файрвол на рівні провайдера
- Гнучкі правила фільтрації трафіку

9. РЕЗЕРВНЕ КОПІЮВАННЯ ТА ВІДНОВЛЕННЯ

9.1. АВТОМАТИЧНІ BACKUP

9.1.1. Системні backup:

- Щоденні автоматичні backup
- Зберігання протягом 7 днів
- Інкрементальні backup для економії місця
- Можливість відключення автоматичного backup

9.1.2. Розширені backup послуги:

- Преміум backup: зберігання до 30 днів
- Географічно розподілені backup
- Шифрування backup файлів
- Автоматична перевірка цілісності

9.2. SNAPSHOT ФУНКЦІОНАЛЬНІСТЬ

9.2.1. Створення snapshot:

- Миттєві знімки стану VPS
- До 5 snapshot одночасно
- Snapshot включають всю файлову систему
- Можливість планування automatic snapshot

9.2.2. Відновлення з snapshot:

- Повне відновлення VPS
- Часткове відновлення файлів
- Створення нового VPS з snapshot
- Час відновлення: 10-30 хвилин

9.3. КОРИСТУВАЦЬКІ BACKUP

9.3.1. Власні рішення backup:

- Встановлення backup ПЗ за вибором
- rsync, tar, duplicity та інші
- Зберігання backup на зовнішніх сервісах
- FTP/SFTP доступ для backup

9.3.2. Backup на додаткові диски:

- Підключення додаткових дисків для backup
- Можливість віддаленого зберігання
- Автоматизація через cron завдання
- Моніторинг успішності backup

10. МОНІТОРИНГ ТА СТАТИСТИКА

10.1. СИСТЕМНИЙ МОНІТОРИНГ

10.1.1. Базовий моніторинг:

- Доступність VPS (ping, SSH)
- Завантаження CPU та RAM
- Використання дискового простору
- Мережевий трафік

10.1.2. Розширений моніторинг:

- Детальна статистика ресурсів
- Моніторинг сервісів та процесів
- Аналіз продуктивності дисків
- Мережева аналітика

10.1.3. Алерти та сповіщення:

- Email/SMS сповіщення про проблеми
- Налаштовувані пороги спрацьовування
- Ескалація критичних проблем
- Інтеграція з зовнішніми системами

10.2. ГРАФІКИ ТА ЗВІТИ

10.2.1. Віртуальна панель моніторингу:

- Real-time графіки ресурсів
- Історичні дані за місяць/рік
- Експорт статистики в різних форматах
- Порівняння з попередніми періодами

10.2.2. Користувацький моніторинг:

- Встановлення власних систем моніторингу
- Zabbix, Nagios, Prometheus підтримка
- SNMP доступ до системної статистики
- API для отримання метрик

11. МАСШТАБУВАННЯ ТА АПГРЕЙД

11.1. ВЕРТИКАЛЬНЕ МАСШТАБУВАННЯ

11.1.1. Збільшення ресурсів:

- CPU: додаткові ядра за 200 грн/місяць
- RAM: додаткова пам'ять за 50 грн/GB/місяць
- Диск: додатковий простір за 10 грн/GB/місяць
- Мережа: збільшення швидкості за 100 грн/100Mbps

11.1.2. Процедура апгрейду:

- Онлайн збільшення ресурсів (без перезавантаження)
- Миттєва активація після оплати
- Пропорційна доплата за поточний період
- Можливість планового апгрейду

11.2. ЗМЕНШЕННЯ РЕСУРСІВ

11.2.1. Downgrade ресурсів:

- Можливе з наступного розрахункового періоду
- Попередження за 7 днів
- Перевірка сумісності з поточним навантаженням
- Збереження даних при можливості

11.3. МІГРАЦІЯ МІЖ ПЛАНАМИ

11.3.1. Зміна типу VPS:

- Міграція між Linux/Windows
- Переход з Managed на Unmanaged
- Міграція між дата-центрами
- Індивідуальний план міграції

12. ДОЗВОЛЕНІ ДОДАТКИ ТА СЕРВІСИ

12.1. ВЕБ-ДОДАТКИ

12.1.1. Веб-сервери та CMS:

- Apache, Nginx, LiteSpeed, IIS
- WordPress, Joomla, Drupal
- Інтернет-магазини: Magento, PrestaShop, OpenCart
- Custom веб-додатки на будь-яких мовах

12.1.2. Бази даних:

- MySQL, MariaDB, PostgreSQL
- MongoDB, Redis, Memcached
- Microsoft SQL Server
- Спеціалізовані бази даних

12.2. ДОДАТКИ РОЗРОБКИ

12.2.1. Середовища розробки:

- IDE та редактори коду
- Git сервери (GitLab, Gitea)
- CI/CD системи (Jenkins, GitLab CI)
- Системи контролю якості коду

12.2.2. Мови програмування:

- PHP, Python, Node.js, Ruby
- Java, .NET Framework/.NET Core
- Go, Rust, C++
- Контейнери Docker/Podman

12.3. БІЗНЕС-ДОДАТКИ

12.3.1. ERP та CRM системи:

- odoo, SugarCRM, SuiteCRM
- Custom бізнес-додатки
- Системи документообігу
- Бухгалтерські системи

12.3.2. Комунікаційні сервіси:

- Email сервери (Postfix, Exim)
- Chat сервери (Rocket.Chat, Mattermost)
- VoIP системи (Asterisk, FreePBX)
- Відеоконференції (Jitsi Meet)

13. ЗАБОРОНЕНІ ДОДАТКИ ТА ДІЯЛЬНІСТЬ

13.1. КАТЕГОРИЧНО ЗАБОРОНЕНО

13.1.1. Незаконна діяльність:

- Розповсюдження піратського контенту
- Хакерські інструменти та експлойти
- Фішинг та соціальна інженерія
- Торгівля наркотиками, зброєю

13.1.2. Шкідливе програмне забезпечення:

- Віруси, троянські програми
- Botnets та C&C сервери
- Keyloggers та spyware
- Ransomware та шифрувальники

13.1.3. Мережеві атаки:

- DDoS атаки та стрес-тестування
- Брутфорс атаки на віддалені сервери
- Експлуатація уразливостей
- Неавторизоване проникнення в системи

13.2. ОБМЕЖЕНО ДОЗВОЛЕНО

13.2.1. За попередньою згодою:

- Майнінг криптовалют (спеціальні умови)
- Відкриті проксі для загального доступу
- Анонімні мережі (Tor релеї)
- P2P файлообмін великих обсягів

13.2.2. З обмеженнями:

- Масові розсилки email (до 1000/день)
- Ресурсномісткі обчислення
- Високочастотний трейдинг
- Стримінг медіа-контенту

13.3. САНКЦІЇ ЗА ПОРУШЕННЯ

13.3.1. Автоматичні санкції:

- Негайне блокування підозрілих процесів
- Ізоляція VPS при виявленні атак
- Тимчасове обмеження мережевого доступу
- Сповіщення служб безпеки при необхідності

13.3.2. Адміністративні санкції:

- Попередження з вимогою усунути порушення
- Призупинення VPS на 24-72 години
- Повне припинення послуг
- Передача інформації правоохоронним органам

14. ТЕХНІЧНА ПІДТРИМКА VPS

14.1. РІВНІ ПІДТРИМКИ

14.1.1. Unmanaged VPS (базова підтримка):

- Підтримка роботи hypervisor та мережі
- Допомога з панеллю управління VPS

- Консультації з базових питань
- Відновлення з backup при збоях обладнання

14.1.2. Managed VPS (розширена підтримка):

- Встановлення та налаштування ОС
- Допомога з налаштуванням веб-серверів
- Усунення проблем з продуктивністю
- Регулярне оновлення системи

14.1.3. Premium Support:

- Персональний технічний менеджер
- Пріоритетна обробка звернень (до 30 хвилин)
- Телефонні консультації
- Віддалене налаштування систем

14.2. КАНАЛИ ПІДТРИМКИ

14.2.1. Основні канали:

- Email підтримка: pllanoviy@gmail.com
- Телефон: +38(097)-714-19-80
- Система тікетів в панелі управління
- Online chat на сайті (якщо доступний)

14.2.2. Термінові звернення:

- Критичні проблеми: телефон 24/7
- Системні збої: автоматичні сповіщення
- Мережеві проблеми: моніторинг в реальному часі
- Безпекові інциденти: негайна ескалація

14.3. SLA ГАРАНТІЇ

14.3.1. Час відгуку:

- Критичні проблеми: до 1 години
- Важливі питання: до 4 годин
- Загальні питання: до 24 годин
- Planned maintenance: повідомлення за 48 годин

14.3.2. Час вирішення:

- Мережеві збої: до 2 годин
- Проблеми hypervisor: до 4 годин
- Відновлення з backup: до 6 годин
- Складні налаштування: до 2 робочих днів

15. БЕЗПЕКА VPS

15.1. СИСТЕМНА БЕЗПЕКА

15.1.1. Ізоляція віртуальних машин:

- Повна ізоляція між VPS
- Захист від overflow атак
- Контроль ресурсів на рівні hypervisor
- Моніторинг аномальної активності

15.1.2. Фізична безпека:

- Захищені дата-центри з контролем доступу
- Резервне електроживлення
- Системи пожежогасіння
- Біометричний контроль доступу

15.2. МЕРЕЖЕВА БЕЗПЕКА

15.2.1. Захист мережі:

- Розподілені DDoS фільтри
- Геоблокінг шкідливих IP
- Аналіз трафіку в реальному часі
- Автоматична блокування атак

15.2.2. Безпека з'єднань:

- Шифровані VPN тунелі
- Захищені SSH з'єднання
- SSL/TLS сертифікати
- Двофакторна автентифікація

15.3. АНТИВІРУСНИЙ ЗАХИСТ

15.3.1. Сканування на рівні hypervisor:

- Регулярне сканування файлової системи
- Перевірка мережевого трафіку
- Виявлення підозрілих процесів
- Карантин заражених файлів

15.3.2. Клієнтські антивіруси:

- Рекомендації щодо вибору антивірусу
- Налаштування системних антивірусів
- Інтеграція з централізованими системами
- Моніторинг статусу антивірусного захисту

16. ПАНЕЛЬ УПРАВЛІННЯ VPS

16.1. ОСНОВНА ПАНЕЛЬ УПРАВЛІННЯ

16.1.1. Функції панелі:

- Запуск, зупинка, перезавантаження VPS
- Встановлення та переустановка ОС
- Управління snapshot та backup
- Моніторинг ресурсів та статистика

16.1.2. Мережеві налаштування:

- Управління IP адресами
- Налаштування DNS записів
- Конфігурація файрволу
- VPN налаштування

16.2. КОНСОЛЬ ТА ВІДДАЛЕНИЙ ДОСТУП

16.2.1. VNC консоль:

- Графічна консоль через браузер
- Доступ навіть при проблемах з мережею
- Повний контроль на рівні BIOS
- Віртуальна клавіатура та миша

16.2.2. SSH доступ:

- Стандартний SSH на порту 22
- Можливість зміни порту
- Підтримка SSH ключів
- Журналування всіх підключень

16.3. API ІНТЕРФЕЙС

16.3.1. RESTful API:

- Управління VPS через API
- Автоматизація рутинних завдань
- Інтеграція з зовнішніми системами
- Документація API з прикладами

16.3.2. SDK та бібліотеки:

- Python, PHP, Node.js SDK
- Готові скрипти для автоматизації
- Webhooks для сповіщень
- GraphQL підтримка

17. БІЛЛІНГ ТА ОПЛАТА

17.1. МОДЕЛІ ОПЛАТИ

17.1.1. Фіксована оплата:

- Місячні, квартальні, річні плани
- Знижки за довготривалу передоплату
- Фіксовані ресурси відповідно до плану
- Передбачувані витрати

17.1.2. Pay-as-you-use:

- Погодинна оплата за використання
- Автоматичне масштабування ресурсів
- Оплата лише за фактичне споживання
- Детальна статистика витрат

17.2. ДОДАТКОВІ ПОСЛУГИ

17.2.1. Платні опції:

- Додаткові IP адреси: 100 грн/місяць
- Розширений backup: 250 грн/місяць
- Управління системою: 750 грн/місяць
- Premium підтримка: 2000 грн/місяць

17.2.2. Одноразові послуги:

- Переустановка ОС: 100 грн
- Налаштування сервера: 300 грн/година
- Міграція з іншого провайдера: від 500 грн
- Відновлення даних: 200 грн/година

17.3. МЕТОДИ ОПЛАТИ

17.3.1. Банківські перекази:

- Переказ на розрахунковий рахунок ФОП
- Онлайн банкінг через інтернет
- Термінали самообслуговування
- Відділення банків України

17.3.2. Електронні платежі:

- Банківські карти Visa/MasterCard
- Електронні гаманці (WebMoney, Perfect Money)
- Мобільні платежі
- Криптовалютні платежі (за наявності)

17.3.3. Автоматична оплата:

- Прив'язка банківської карти
- Автоматичне списання перед закінченням періоду

- Email повідомлення про платежі
- Можливість відключення автоплатежу

18. СЛУЖБА LEVEL AGREEMENT (SLA)

18.1. ГАРАНТІЇ ДОСТУПНОСТІ

18.1.1. Uptime гарантії:

- **Basic VPS:** 99.5% uptime на місяць
- **Business VPS:** 99.9% uptime на місяць
- **Enterprise VPS:** 99.95% uptime на місяць
- Виключення планових технічних робіт (до 4 годин/місяць)

18.1.2. Компенсації за SLA порушення:

- 99.0-99.49%: 5% від місячної оплати
- 98.0-98.99%: 10% від місячної оплати
- 97.0-97.99%: 25% від місячної оплати
- Менше 97%: 50% від місячної оплати

18.2. ГАРАНТІЇ ПРОДУКТИВНОСТІ

18.2.1. Ресурсні гарантії:

- Гарантований доступ до заявлених CPU ресурсів
- Виділена RAM без overbooking
- Гарантований IOPS для дискової підсистеми
- Мінімальна пропускна здатність мережі

18.2.2. Мережеві гарантії:

- Максимальна затримка (latency): 50ms в межах України
- Втрата пакетів (packet loss): не більше 0.1%
- Джиттер: не більше 10ms
- Час відновлення мережі після збоїв: до 15 хвилин

18.3. ПРОЦЕДУРА РОЗРАХУНКУ SLA

18.3.1. Моніторинг uptime:

- Автоматичний моніторинг кожні 5 хвилин
- Перевірка доступності з декількох точок
- Виключення запланованих робіт
- Детальні логи доступності

18.3.2. Звітність SLA:

- Щомісячні звіти по email
- Online dashboard з real-time статистикою
- Історичні дані за весь період
- Автоматичні компенсації при порушеннях

19. МІГРАЦІЯ ТА ПЕРЕНОС ДАНИХ

19.1. МІГРАЦІЯ З ІНШИХ ПРОВАЙДЕРІВ

19.1.1. Безкоштовна міграція:

- Перенос з будь-якого провайдера
- До 100GB даних безкоштовно
- Міграція баз даних та конфігурацій
- Тестування після міграції

19.1.2. Типи міграції:

- **P2V (Physical to Virtual)**: з фізичного сервера
- **V2V (Virtual to Virtual)**: з іншого VPS
- **Cloud to VPS**: з хмарних платформ
- **Shared to VPS**: з віртуального хостингу

19.1.3. Процес міграції:

- Аналіз поточної інфраструктури
- Планування міграції з мінімальним downtime
- Поетапний перенос сервісів
- Тестування та оптимізація після міграції

19.2. МІГРАЦІЯ МІЖ ДАТА-ЦЕНТРАМИ

19.2.1. Географічна міграція:

- Перенос між різними локаціями
- Збереження всіх даних та налаштувань
- Координація зміни DNS записів
- Мінімізація downtime (до 30 хвилин)

19.2.2. Причини міграції:

- Покращення latency для користувачів
- Юридичні вимоги щодо локації даних
- Оптимізація мережевих маршрутів
- Розширення географічного покриття

19.3. ЕКСПОРТ ТА ПОРТАБЕЛЬНІСТЬ ДАНИХ

19.3.1. Формати експорту:

- Повні образи дисків (RAW, VMDK, VHD)
- Архіви файлових систем (tar, zip)
- Експорт баз даних (SQL dump)
- Snapshot у форматах різних гіпервізорів

19.3.2. Право на портабельність:

- Безкоштовний експорт даних при припиненні послуг
- Допомога з переносом до інших провайдерів
- Збереження доступу до даних протягом 30 днів
- Консультації щодо міграції

20. COMPLIANCE ТА СТАНДАРТИ

20.1. ДОТРИМАННЯ СТАНДАРТІВ

20.1.1. Міжнародні стандарти:

- ISO 27001 (Інформаційна безпека)
- ISO 9001 (Система менеджменту якості)
- SOC 2 Type II (Security, Availability, Confidentiality)
- PCI DSS Level 1 (для платіжних систем)

20.1.2. Регіональні стандарти:

- Відповідність GDPR для європейських клієнтів
- Законодавство України про персональні дані
- Стандарти НБУ для фінансових установ
- Галузеві стандарти безпеки

20.2. АУДИТ ТА СЕРТИФІКАЦІЯ

20.2.1. Зовнішні аудити:

- Щорічні аудити безпеки незалежними компаніями
- Penetration testing інфраструктури
- Перевірка відповідності стандартам
- Публікація звітів про безпеку

20.2.2. Внутрішній контроль:

- Регулярні внутрішні аудити процесів
- Моніторинг дотримання політик безпеки
- Навчання персоналу з безпеки
- Постійне покращення процедур

20.3. ЮРИДИЧНЕ ДОТРИМАННЯ

20.3.1. Законодавство України:

- Закон "Про телекомунікації"
- Закон "Про електронні довірчі послуги"
- Закон "Про захист персональних даних"
- Податковий кодекс України

20.3.2. Міжнародне право:

- Конвенція про кіберзлочинність
- Угоди про взаємну правову допомогу

- Міжнародні санкційні списки
- Export control regulations

21. СПЕЦІАЛЬНІ СЦЕНАРІЇ ВИКОРИСТАННЯ

21.1. РОЗРОБКА ТА ТЕСТУВАННЯ

21.1.1. Development VPS:

- Знижені тарифи для розробників
- Швидке клонування середовищ
- Інтеграція з CI/CD системами
- Тимчасові VPS для тестів

21.1.2. Staging середовища:

- Ідентичні продакшн конфігурації
- Синхронізація з production даними
- Automated deployment pipeline
- Rollback можливості

21.2. БІЗНЕС КРИТИЧНІ СИСТЕМИ

21.2.1. High Availability конфігурації:

- Кластери VPS з автоматичним failover
- Load balancing між інстансами
- Географічне розподілення для DR
- 24/7 моніторинг критичних систем

21.2.2. Enterprise рішення:

- Виділені фізичні ресурси
- Priority support з гарантованим SLA
- Індивідуальні договори обслуговування
- Консультації архітекторів рішень

21.3. СПЕЦІАЛІЗОВАНІ ЗАСТОСУНКИ

21.3.1. Ігрові сервери:

- Низька затримка мережі
- Оптимізовані CPU для ігрових додатків
- DDoS захист для ігрових серверів
- Підтримка популярних ігрових платформ

21.3.2. Media streaming:

- Висока пропускна здатність
- CDN інтеграція для контенту
- Транскодинг відео на сервері
- Live streaming підтримка

22. ЕКОЛОГІЧНА ВІДПОВІДАЛЬНІСТЬ

22.1. ЗЕЛЕНІ ТЕХНОЛОГІЇ

22.1.1. Енергоефективність:

- Використання енергоефективних серверів
- Optimized cooling systems в дата-центрах
- Віртуалізація для максимального використання ресурсів
- Моніторинг та оптимізація енергоспоживання

22.1.2. Відновлювана енергія:

- Перехід на використання відновлюваних джерел енергії
- Компенсація вуглецевого сліду
- Інвестиції в зелені технології
- Сертифікація Green IT

22.2. ВІДПОВІДАЛЬНЕ ВИКОРИСТАННЯ

22.2.1. Освіта клієнтів:

- Рекомендації з оптимізації енергоспоживання
- Best practices для ефективного використання ресурсів
- Інструменти моніторингу споживання
- Заохочення екологічно свідомого використання

23. ІННОВАЦІЇ ТА МАЙБУТНІЙ РОЗВИТОК

23.1. НОВІ ТЕХНОЛОГІЇ

23.1.1. Containerization підтримка:

- Нативна підтримка Docker
- Kubernetes orchestration
- Serverless functions
- Microservices архітектури

23.1.2. Edge Computing:

- VPS в edge локаціях
- Low-latency обчислення
- IoT додатки підтримка
- Real-time data processing

23.2. ШТУЧНИЙ ІНТЕЛЕКТ

23.2.1. AI-powered оптимізація:

- Автоматична оптимізація ресурсів
- Прогнозування навантажень

- Intelligent scaling
- Predictive maintenance

24. НАВЧАННЯ ТА РЕСУРСИ

24.1. ДОКУМЕНТАЦІЯ

24.1.1. Технічна документація:

- Детальні гайди налаштування
- Best practices для різних сценаріїв
- Troubleshooting guides
- API документація з прикладами

24.1.2. Навчальні матеріали:

- Відеоуроки для початківців
- Webinars з експертами
- Case studies успішних проектів
- Certification programs

24.2. СПІЛЬНОТА

24.2.1. Community форум:

- Обмін досвідом між користувачами
- Питання та відповіді від експертів
- Анонси нових функцій
- User-generated контент

24.2.2. Заходи та конференції:

- Регулярні meetups для клієнтів
- Участь в IT конференціях
- Воркшопи з новітніх технологій
- Нетворкінг заходи

25. ПРОЦЕДУРИ ОСКАРЖЕННЯ ТА СКАРГИ

25.1. ПОДАННЯ СКАРГ

25.1.1. Канали для скарг:

- Email: support-vps@sthost.pro
- Система тікетів з пріоритетом "Complaint"
- Письмова скарга поштою
- Телефон для термінових питань

25.1.2. Інформація в скарзі:

- Детальний опис проблеми

- Хронологія подій
- Документальні підтвердження
- Очікуваний результат

25.2. РОЗГЛЯД СКАРГ

25.2.1. Процедура розгляду:

- Підтвердження отримання протягом 24 годин
- Initial response протягом 3 робочих днів
- Детальне розслідування до 14 днів
- Остаточна відповідь протягом 30 днів

25.2.2. Ескалація:

- Перший рівень: технічна підтримка
- Другий рівень: керівник технічного відділу
- Третій рівень: керівництво компанії
- Зовнішня медіація за необхідності

25.3. КОМПЕНСАЦІЇ ТА ВІДШКОДУВАННЯ

25.3.1. Види компенсацій:

- Відшкодування невикористаного часу
- Безкоштовні додаткові послуги
- Знижки на майбутні платежі
- Прямі грошові компенсації

25.3.2. Критерії компенсацій:

- Ступінь порушення SLA
- Фінансові втрати клієнта
- Тривалість проблеми
- Вплив на бізнес клієнта

26. ПРИПИНЕННЯ ПОСЛУГ

26.1. ДОБРОВІЛЬНЕ ПРИПИНЕННЯ

26.1.1. З ініціативи клієнта:

- Повідомлення за 7 днів до припинення
- Можливість експорту всіх даних
- Повернення невикористаних коштів (pro-rata)
- Збереження backup протягом 30 днів

26.1.2. Процедура закриття:

- Backup всіх критичних даних
- Видалення sensitive інформації
- Підтвердження завершення міграції

- Остаточне видалення VPS

26.2. ПРИПИНЕННЯ ЗА ПОРУШЕННЯ

26.2.1. Процедура припинення:

- Письмове попередження з вказівкою порушення
- Термін для усунення (24-72 години)
- Призупинення при неусуненні
- Остаточне припинення через 7 днів

26.2.2. Екстрені припинення:

- При критичних порушеннях безпеки
- DDoS атаки з VPS
- Розповсюдження malware
- Незаконна діяльність

26.3. ТЕХНІЧНЕ ПРИПИНЕННЯ

26.3.1. З технічних причин:

- Критичні збої обладнання
- Припинення діяльності провайдера
- Force majeure обставини
- Зміни в законодавстві

26.3.2. Компенсації:

- Повне відшкодування оплаченого періоду
- Безкоштовна допомога з міграцією
- Додатковий час на експорт даних
- Пріоритетна підтримка при міграції

27. КОНТАКТИ ТА ПІДТРИМКА

27.1. ОСНОВНІ КОНТАКТИ

27.1.1. Контактна інформація:

- **Адреса:** 49047, м. Дніпро, вул. Холодноярська, 10, кв. 9
- **Телефон:** +38(097)-714-19-80
- **Email:** pllanoviy@gmail.com
- **Веб-сайт:** <https://sthost.pro>

27.1.2. Спеціалізовані контакти:

- **VPS підтримка:** support-vps@sthost.pro
- **Sales:** sales-vps@sthost.pro

27.2. ГРАФІК РОБОТИ

27.2.1. Технічна підтримка:

- **Email та тікети:** 24/7/365
- **Телефон:** Пн-Пт 9:00-18:00, Сб-Нд 10:00-16:00 (UTC+2)
- **Екстрені випадки:** 24/7 +38(093)-025-39-41
- **Планові роботи:** 02:00-06:00 (UTC+2)

27.3. РЕКВІЗИТИ ПРОВАЙДЕРА

ФОП Діхтярь Ірина Олександрівна

- **РНОКПП:** 3009915262
- **IBAN:** UA273348510000026000010598
- **Банк:** АТ "ПУМБ"
- **МФО:** 334851
- **Адреса:** 49047, м. Дніпро, вул. Холодноярська, 10, кв. 9

28. ЗАКЛЮЧНІ ПОЛОЖЕННЯ

28.1. ПРАВОВА СИЛА

28.1.1. Ці Правила користування VPS є обов'язковими для всіх користувачів VPS послуг STHost.pro.

28.1.2. Правила доповнюють Загальні умови обслуговування та інші договірні документи.

28.1.3. У разі суперечностей між документами, пріоритет мають ці спеціальні Правила VPS.

28.2. ЗМІНИ ТА ОНОВЛЕННЯ

28.2.1. Провайдер має право вносити зміни до цих Правил з повідомленням користувачів за 30 днів.

28.2.2. Критичні зміни безпеки можуть впроваджуватися негайно.

28.2.3. Продовження використання VPS після змін означає згоду з новими правилами.

28.3. ЮРИСДИКЦІЯ

28.3.1. Ці Правила регулюються законодавством України.

28.3.2. Всі спори вирішуються в судах за місцезнаходженням Провайдера.

28.3.3. Для міжнародних клієнтів можливе застосування медіації.