ПОЛІТИКА БЕЗПЕКИ СЕРВЕРІВ VPS

STHost.pro

Дата останнього оновлення: 23 серпня 2025р
Дата набрання чинності: 25 серпня 2025р

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Ця Політика безпеки серверів VPS (далі - "Політика") визначає комплексні заходи забезпечення інформаційної безпеки віртуальних приватних серверів Фізичної особи-підприємця Діхтярь Ірини Олександрівни (далі - "Провайдер", "STHost.pro").

1.2. Політика розроблена відповідно до міжнародних стандартів кібербезпеки та вимог українського законодавства у сфері захисту інформації.

1.3. Дотримання цієї Політики є обов'язковим для всіх користувачів VPS послуг та співробітників Провайдера.

1.4. Ця Політика доповнює Правила користування VPS та інші договірні документи STHost.pro.

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: pllanoviy@gmail.com
- Веб-сайт: https://sthost.pro
- Дата реєстрації: 18.08.2025

3. ПРИНЦИПИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1. ФУНДАМЕНТАЛЬНІ ПРИНЦИПИ

3.1.1. Конфіденційність (Confidentiality):

- Захист інформації від несанкціонованого доступу
- Шифрування даних у спокої та при передачі
- Контроль доступу за принципом найменших привілеїв
- Класифікація інформації за рівнями конфіденційності

3.1.2. Цілісність (Integrity):

- Забезпечення точності та повноти інформації
- Захист від несанкціонованих змін

- Контроль версій та аудиторські сліди
- Перевірка цілісності даних та системних файлів

3.1.3. Доступність (Availability):

- Гарантування доступу до ресурсів авторизованим користувачам
- Мінімізація часу простоїв
- Резервування критичних систем
- Планування відновлення після аварій

3.2. ДОДАТКОВІ ПРИНЦИПИ

3.2.1. Автентичність (Authentication):

- Достовірна ідентифікація користувачів та систем
- Багатофакторна автентифікація для критичних операцій
- Цифрові підписи та сертифікати
- Перевірка джерел інформації

3.2.2. Невідрекнення (Non-repudiation):

- Неможливість заперечити виконані дії
- Детальне логування всіх операцій
- Цифрові сліди та часові мітки
- Юридична значущість доказів

3.2.3. Підзвітність (Accountability):

- Особиста відповідальність за безпеку
- Аудит дій користувачів та систем
- Звітність про інциденти безпеки
- Моніторинг дотримання політик

4. АРХІТЕКТУРА БЕЗПЕКИ VPS ІНФРАСТРУКТУРИ

4.1. МОДЕЛЬ БЕЗПЕКИ

4.1.1. Defense in Depth (Багатошарова оборона):

```
[Користувач]
    ↓ [Authentication & Authorization]
[Internet]
    ↓ [External Firewall & DDoS Protection]
[DMZ]
    ↓ [Load Balancer & Proxy]
[Management Network]
    ↓ [Internal Firewall]
[Hypervisor Layer]
    ↓ [VPS Isolation & Access Control]
[Hardware Layer]
    ↓ [Physical Security]
[Data Storage]
```

4.1.2. Зони безпеки:

- **Public Zone:** інтернет-з'єднання та публічні сервіси
- **DMZ Zone:** демілітаризована зона з проксі-серверами
- **Management Zone:** системи управління та моніторингу
- **Private Zone:** внутрішня мережа та сховище даних
- **Isolated Zone:** критичні системи та backup

4.2. СЕГМЕНТАЦІЯ МЕРЕЖІ

4.2.1. VLAN сегментація:

- **Management VLAN (10):** системи управління
- **Customer VLAN (100-999):** клієнтські VPS
- **Storage VLAN (1000):** системи зберігання
- **Backup VLAN (1001):** backup інфраструктура
- **Monitoring VLAN (1002):** системи моніторингу

4.2.2. Micro-segmentation:

- Ізоляція кожного VPS на мережевому рівні
- Контроль трафіку між VPS одного клієнта
- Обмеження lateral movement при компрометації
- Динамічна фільтрація за поведінковими ознаками

5. ФІЗИЧНА БЕЗПЕКА ІНФРАСТРУКТУРИ

5.1. ЗАХИСТ ДАТА-ЦЕНТРУ

5.1.1. Периметр безпеки:

- **Фізичне обмеження:** огорожі, бар'єри, контрольовані входи
- **Системи виявлення:** датчики руху, розбиття скла, вібрації
- **Освітлення периметру:** автоматичне включення при детекції

5.2. СЕРВЕРНІ ПРИМІЩЕННЯ

5.2.1. Екологічна безпека:

- **Пожежогасіння:** газова система
- **Датчики диму:** аспіраційна система раннього виявлення
- **Контроль температури:** підтримка 15-30°C
- **Контроль вологості:** 20-80% відносної вологості
- **Витік води:** датчики під підлогою та на стелі

5.2.2. Електробезпека:

- **UPS системи:** N+1 резервування, 3 години автономності
- **Заземлення:** технічне та захисне заземлення
- **Захист від перенапруги:** SPD на всіх рівнях

5.3. ЗАХИСТ ОБЛАДНАННЯ

5.3.1. Серверні стійки:

- **Замкові системи:** електронні замки з аудитом
- **Датчики відкриття:** сповіщення про несанкціонований доступ
- **Кріплення обладнання:** антикрадіжні кріплення
- **Inventory tags:** RFID мітки для відстеження

5.3.2. Мережеве обладнання:

- **Захищені порти:** автоматичне відключення невикористаних
- **MAC filtering:** контроль на рівні MAC адрес
- **Console security:** захищені консольні порти
- **Cable management:** організоване кабельне господарство

6. МЕРЕЖЕВА БЕЗПЕКА

6.1. ПЕРИМЕТРОВА БЕЗПЕКА

6.1.1. Firewall архітектура:

- **External firewall:** d-link+cisco
- **Internal firewall:** розподілені точки контролю
- **Application firewall:** захист веб-додатків (WAF)
- **Database firewall:** захист баз даних від SQL-ін'єкцій

6.1.2. Правила firewall:

```
Default Policy: DENY ALL
Allow Rules:
- HTTP/HTTPS (80,443) → Web Servers
- SSH (22,224) → Management Network (restricted IPs)
- DNS (53) → Public DNS Servers
- NTP (123) → Time Servers
- Custom Ports → As per customer requirements

Deny Rules:
- Any → Private Subnets (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)
- Suspicious IPs → Any (Dynamic blacklist)
- Tor Exit Nodes → Any
- Known malware C&C → Any
```

6.2. DDoS ЗАХИСТ

6.2.1. Багатошарова архітектура захисту:

```
Layer 1: ISP Level Protection (100+ Gbps capacity)
    ↓ [Rate limiting, Blackholing]
Layer 2: Edge Router Protection (10 Gbps)
    ↓ [BGP routing, GRE tunnels]
Layer 3: DDoS Appliance (5 Gbps)
    ↓ [Pattern detection, Challenge-response]
Layer 4: Application Level (1 Gbps)
    ↓ [Web Application Firewall]
Layer 5: VPS Level Protection
    ↓ [Host-based filtering]
```

6.2.2. Типи захисту:

- **Volumetric attacks:** bandwidth overwhelming
- **Protocol attacks:** TCP SYN flood, UDP flood, ICMP flood
- **Application attacks:** HTTP flood, Slowloris, RUDY
- **Reflection attacks:** DNS, NTP, SNMP amplification

6.3. СИСТМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ

6.3.1. Network IDS/IPS:

- **Suricata IDS:** моніторинг мережевого трафіку
- **Snort rules:** бази правил виявлення загроз
- **Behavioral analysis:** виявлення аномальної поведінки
- **Threat intelligence:** інтеграція з CTI feeds

6.3.2. Host-based IDS:

- **OSSEC HIDS:** моніторинг змін файлової системи
- **Auditd:** аудит системних викликів
- **Process monitoring:** контроль запущених процесів
- **Network connections:** моніторинг з'єднань

6.3.3. SIEM система:

- **Log aggregation:** централізований збір логів
- **Correlation rules:** виявлення складних атак
- **Alerting:** сповіщення про інциденти
- **Forensics:** розслідування інцидентів

7. БЕЗПЕКА ВІРТУАЛІЗАЦІЇ

7.1. HYPERVISOR БЕЗПЕКА

7.1.1. KVM захист:

- **SELinux/AppArmor:** mandatory access control
- **Kernel hardening:** відключення непотрібних модулів
- **ASLR/DEP/SMEP:** захист від buffer overflow
- **Control groups (cgroups):** ізоляція ресурсів

7.1.2. QEMU безпека:

- **Sandboxing:** seccomp фільтри системних викликів
- **Privilege dropping:** мінімальні привілеї процесів
- **Memory protection:** захист пам'яті гіпервізора
- **Input validation:** перевірка всіх вхідних даних

7.2. VPS ІЗОЛЯЦІЯ

7.2.1. Мережева ізоляція:

- **Private networks:** ізольовані L2 домени
- **VLAN tagging:** 802.1Q мітки для кожного VPS

- **Anti-spoofing:** захист від підміни IP/MAC адрес
- **Bandwidth limiting:** QoS для справедливого розподілу

7.2.2. Дискова ізоляція:

- **Encrypted storage:** шифрування дисків AES-256
- **Copy-on-write:** захист від модифікації базових образів
- **Quota enforcement:** жорстке обмеження дискового простору
- **Secure delete:** криптографічне видалення даних

7.2.3. Процесорна ізоляція:

- **CPU pinning:** прив'язка до конкретних ядер
- **Cache partitioning:** розділення кешу процесора
- **Side-channel protection:** захист від Spectre/Meltdown
- **Performance isolation:** гарантовані ресурси CPU

7.3. УПРАВЛІННЯ ОБРАЗАМИ

7.3.1. Базові образи:

- **Hardened templates:** захищені шаблони ОС
- **Regular updates:** щомісячне оновлення образів
- **Vulnerability scanning:** сканування перед публікацією
- **Digital signatures:** підписи цілісності образів

7.3.2. Користувацькі образи:

- **Malware scanning:** антивірусна перевірка
- **Compliance checking:** відповідність політикам безпеки
- **Encryption at rest:** шифрування snapshot'ів
- **Access logging:** аудит використання образів

8. АВТЕНТИФІКАЦІЯ ТА АВТОРИЗАЦІЯ

8.1. УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ

8.1.1. Система аутентифікації:

- **Multi-factor authentication (MFA):** обов'язково для admin
- **LDAP integration:** централізоване управління користувачами
- **SSO capabilities:** single sign-on для управління
- **Risk-based authentication:** адаптивна аутентифікація

8.1.2. Політики паролів:

- **Мінімальна довжина:** 12 символів
- **Складність:** великі/малі літери, цифри, спецсимволи
- **Термін дії:** 90 днів для привілейованих акаунтів
- **Заборона повторного використання:** останні 12 паролів
- **Блокування після невдалих спроб:** 5 невдалих спроб

8.2. КОНТРОЛЬ ДОСТУПУ

8.2.1. Role-Based Access Control (RBAC):

```
Roles:
├── SuperAdmin (повний доступ до всіх систем)
├── SystemAdmin (управління інфраструктурою)
├── NetworkAdmin (мережеві налаштування)
├── SecurityAdmin (системи безпеки)
├── SupportTier1 (базова підтримка клієнтів)
├── SupportTier2 (розширена технічна підтримка)
└── Customer (доступ лише до власних ресурсів)
```

8.2.2. Принцип найменших привілеїв:

- **Just-in-time access:** тимчасове підвищення привілеїв
- **Privileged access management:** управління admin доступом
- **Session recording:** запис сесій привілейованих користувачів
- **Break-glass procedures:** екстрені процедури доступу

8.3. SSH БЕЗПЕКА

8.3.1. SSH конфігурація:

```
# /etc/ssh/sshd_config security hardening
Protocol 2
PermitRootLogin no
PubkeyAuthentication yes
PasswordAuthentication no
ChallengeResponseAuthentication no
UsePAM yes
X11Forwarding no
MaxAuthTries 3
ClientAliveInterval 600
ClientAliveCountMax 0
LoginGraceTime 120
MaxSessions 2
AllowUsers support admin
DenyUsers root guest
```

8.3.2. SSH ключі:

- **Мінімальна довжина RSA:** 2048 біт (рекомендовано 4096)
- **Підтримка ECDSA:** P-256, P-384, P-521 curves
- **Ed25519 підтримка:** найбільш безпечний алгоритм
- **Certificate authorities:** централізоване управління ключами

9. ШИФРУВАННЯ ТА КРИПТОГРАФІЧНИЙ ЗАХИСТ

9.1. ШИФРУВАННЯ ДАНИХ У СПОКОЇ

9.1.1. Дискове шифрування:

- **Full disk encryption:** LUKS з AES-256-XTS
- **Key management:** централізоване управління ключами
- **Hardware security modules:** апаратні модулі безпеки

- **Key rotation:** ротація ключів кожні 12 місяців

9.1.2. Database шифрування:

- **Transparent data encryption:** прозоре шифрування БД
- **Column-level encryption:** шифрування окремих полів
- **Backup encryption:** зашифровані резервні копії
- **Key segregation:** розділення ключів між системами

9.2. ШИФРУВАННЯ ДАНИХ ПРИ ПЕРЕДАЧІ

9.2.1. Network encryption:

- **TLS 1.3:** найновіша версія протоколу
- **Perfect forward secrecy:** відмова від сталих ключів
- **Certificate pinning:** прив'язка до конкретних сертифікатів
- **HSTS enforcement:** обов'язкове використання HTTPS

9.2.2. VPN з'єднання:

- **IPSec tunnels:** для site-to-site підключень
- **WireGuard:** сучасний VPN протокол
- **Certificate-based authentication:** автентифікація сертифікатами
- **Perfect forward secrecy:** регулярна зміна ключів сесії

9.3. УПРАВЛІННЯ КЛЮЧАМИ

9.3.1. Key lifecycle management:

- **Key generation:** використання апаратних ГСЧ
- **Key distribution:** захищене розповсюдження
- **Key storage:** захищені сховища ключів
- **Key rotation:** автоматична ротація ключів
- **Key escrow:** резервування ключів
- **Key destruction:** безпечне знищення ключів

9.3.2. Certificate management:

- **Internal CA:** власний центр сертифікації
- **Certificate lifecycle:** автоматичне продовження
- **Revocation lists:** списки відкликаних сертифікатів
- **OCSP stapling:** онлайн перевірка статусу

10. МОНІТОРИНГ ТА АУДИТ БЕЗПЕКИ

10.1. БЕЗПЕРЕРВНИЙ МОНІТОРИНГ

10.1.1. Security Operations Center (SOC):

- **24/7 monitoring:** цілодобове спостереження
- **Tier 1 analysts:** перша лінія реагування
- **Tier 2 specialists:** глибокий аналіз інцидентів

- **Threat hunters:** проактивне полювання на загрози

10.1.2. Automated monitoring:

- **SIEM platform:** Security Information and Event Management
- **User behavior analytics:** аналіз поведінки користувачів
- **Network traffic analysis:** аналіз мережевого трафіку
- **Endpoint detection:** моніторинг кінцевих точок

10.2. ЛОГУВАННЯ ТА АУДИТ

10.2.1. Централізований логування:

```
Log Sources:
├── Firewalls → Security events, denied connections
├── Hypervisors → VM lifecycle, resource usage
├── Network devices → Traffic flows, configuration changes
├── Operating systems → Login attempts, privilege escalations
├── Applications → Business logic, data access
├── Security tools → Alerts, detections, responses
└── Physical security → Access logs, environmental
```

10.2.2. Log management:

- **Retention policy:** 3 роки для security logs
- **Log integrity:** цифрові підписи та хеші
- **Real-time analysis:** миттєвий аналіз критичних подій
- **Long-term storage:** архівування для compliance

10.3. СИСТЕМИ АНАЛІЗУ

10.3.1. Threat intelligence:

- **Commercial feeds:** комерційні джерела загроз
- **Open source intelligence:** відкриті джерела
- **Government sources:** урядові бюлетені безпеки
- **Industry sharing:** обмін інформацією з колегами

10.3.2. Machine learning:

- **Anomaly detection:** виявлення аномалій в поведінці
- **Predictive analytics:** прогнозування загроз
- **Automated response:** автоматичне реагування
- **False positive reduction:** зменшення хибних спрацьовувань

11. УПРАВЛІННЯ ІНЦИДЕНТАМИ БЕЗПЕКИ

11.1. ПРОЦЕДУРИ РЕАГУВАННЯ

11.1.1. Incident Response Team (IRT):

```
Склад команди:
├── Incident Manager (координація реагування)
├── Security Analyst (технічний аналіз)
```

```
├── Network Engineer (мережеві проблеми)
├── System Administrator (системне відновлення)
├── Legal Counsel (правові аспекти)
├── Communications (зв'язки з громадськістю)
└── External Consultants (за потреби)
```

11.1.2. Фази реагування:

1. **Detection & Analysis:** виявлення та аналіз (1-4 години)
2. **Containment:** локалізація інциденту (4-8 годин)
3. **Eradication:** усунення причин (8-24 години)
4. **Recovery:** відновлення сервісів (24-72 години)
5. **Post-incident:** аналіз після інциденту (1 тиждень)

11.2. КЛАСИФІКАЦІЯ ІНЦИДЕНТІВ

11.2.1. Рівні критичності:

- **Critical (P1):** масштабна компрометація, простій сервісів >4 год
- **High (P2):** компрометація окремих систем, простій <4 год
- **Medium (P3):** потенційні загрози, мінімальний вплив
- **Low (P4):** підозрілі події, профілактичні заходи

11.2.2. Типи інцидентів:

- **Malware infections:** віруси, троянські програми
- **Unauthorized access:** несанкціонований доступ
- **Data breaches:** витік конфіденційних даних
- **Service disruption:** порушення роботи сервісів
- **Physical security:** порушення фізичної безпеки
- **Social engineering:** атаки соціальної інженерії

11.3. ПРОЦЕДУРИ ЕСКАЛАЦІЇ

11.3.1. Внутрішня ескалація:

- **L1 → L2:** через 30 хвилин без прогресу
- **L2 → L3:** через 2 години для складних інцидентів
- **L3 → Management:** критичні інциденти негайно
- **Management → External:** залучення зовнішніх експертів

11.3.2. Зовнішні повідомлення:

- **CERT-UA:** кіберінциденти національного значення
- **Правоохоронні органи:** кримінальні кіберзлочини
- **Клієнти:** інциденти, що вплинули на їх дані
- **Партнери:** події, що впливають на співпрацю

12. УПРАВЛІННЯ УРАЗЛИВОСТЯМИ

12.1. VULNERABILITY MANAGEMENT

12.1.1. Процес управління уразливостями:

```
1. Discovery (Виявлення)
   ├── Network scanning (Nessus, OpenVAS)
   ├── Application scanning (OWASP ZAP, Burp)
   ├── Configuration assessment
   └── Threat intelligence feeds

2. Assessment (Оцінка)
   ├── CVSS scoring
   ├── Business impact analysis
   ├── Exploitability assessment
   └── False positive validation

3. Prioritization (Пріоритизація)
   ├── Critical: patch within 24-48 hours
   ├── High: patch within 7 days
   ├── Medium: patch within 30 days
   └── Low: patch during maintenance windows

4. Remediation (Усунення)
   ├── Patch management
   ├── Configuration changes
   ├── Compensating controls
   └── Risk acceptance

5. Verification (Перевірка)
   ├── Re-scanning
   ├── Penetration testing
   ├── Configuration validation
   └── Monitoring
```

12.2. PATCH MANAGEMENT

12.2.1. Patch lifecycle:

- **Testing environment:** тестування всіх патчів
- **Staging deployment:** поетапне розгортання
- **Production rollout:** контрольоване впровадження
- **Rollback procedures:** процедури відкату змін

12.2.2. Emergency patching:

- **Zero-day vulnerabilities:** критичні уразливості
- **Active exploitation:** експлойти в дикій природі
- **High CVSS scores:** оцінка вище 8.0
- **Customer impact:** безпосередній вплив на клієнтів

12.3. PENETRATION TESTING

12.3.1. Регулярне тестування:

- **Quarterly internal tests:** щоквартальне внутрішнє тестування
- **Annual external tests:** річне зовнішнє тестування
- **Post-change testing:** після значних змін
- **Red team exercises:** повноцінні навчання

12.3.2. Scope coverage:

- **Network infrastructure:** мережева інфраструктура
- **Web applications:** веб-додатки
- **Wireless networks:** бездротові мережі
- **Social engineering:** соціальна інженерія
- **Physical security:** фізична безпека

13. БЕЗПЕКА ДОДАТКІВ ТА ВЕБ-СЕРВІСІВ

13.1. WEB APPLICATION FIREWALL (WAF)

13.1.1. WAF конфігурація:

- **OWASP Top 10 protection:** захист від основних загроз
- **Custom rule sets:** специфічні правила для додатків
- **Rate limiting:** обмеження частоти запитів
- **Geo-blocking:** блокування за географією
- **Bot detection:** виявлення автоматизованого трафіку

13.1.2. Protected vulnerabilities:

- **SQL Injection:** ін'єкції SQL коду
- **Cross-Site Scripting (XSS):** міжсайтовий скриптинг
- **Cross-Site Request Forgery (CSRF):** підроблення запитів
- **Remote Code Execution:** віддалене виконання коду
- **File Upload attacks:** атаки через завантаження файлів

13.2. API БЕЗПЕКА

13.2.1. API Gateway:

- **Authentication:** OAuth 2.0, JWT tokens
- **Rate limiting:** контроль частоти запитів
- **Input validation:** перевірка вхідних даних
- **Output filtering:** фільтрація відповідей
- **Audit logging:** логування всіх API викликів

13.2.2. API Security controls:

- **TLS encryption:** шифрування всіх з'єднань
- **Certificate pinning:** прив'язка до сертифікатів
- **Request signing:** підпис критичних запитів
- **Replay protection:** захист від повторних атак

13.3. CONTENT SECURITY

13.3.1. Content filtering:

- **Malware scanning:** сканування завантажуваного контенту
- **Virus detection:** виявлення вірусів
- **Suspicious files:** підозрілі файли та архіви
- **Executable blocking:** блокування виконуваних файлів

13.3.2. Data Loss Prevention (DLP):

- **Sensitive data detection:** виявлення чутливої інформації
- **Content classification:** класифікація контенту
- **Policy enforcement:** забезпечення дотримання політик
- **Incident alerting:** сповіщення про порушення

14. BACKUP TA DISASTER RECOVERY

14.1. СТРАТЕГІЯ РЕЗЕРВНОГО КОПІЮВАННЯ

14.1.1. Backup архітектура:

```
3-2-1 Backup Strategy:
├── 3 копії даних (1 оригінал + 2 копії)
├── 2 різних типи носіїв (диск + стрічка/хмара)
└── 1 копія офсайт (географічно віддалена)

Backup Tiers:
├── Tier 1: Real-time replication (RTO <1h, RPO <15min)
├── Tier 2: Daily incrementals (RTO <4h, RPO <1day)
├── Tier 3: Weekly fulls (RTO <24h, RPO <1week)
└── Tier 4: Monthly archives (RTO <72h, RPO <1month)
```

14.1.2. Backup types:

- **Full backups:** повні копії кожної неділі
- **Incremental backups:** щоденні зміни
- **Differential backups:** зміни з моменту останнього full
- **Snapshot backups:** миттєві знімки стану VPS

14.1.3. Retention policy:

- **Daily backups:** 30 днів зберігання
- **Weekly backups:** 12 тижнів зберігання
- **Monthly backups:** 12 місяців зберігання
- **Yearly backups:** 7 років зберігання (compliance)

14.2. БЕЗПЕКА BACKUP

14.2.1. Encryption в backup:

- **AES-256 encryption:** шифрування всіх backup файлів
- **Unique encryption keys:** унікальні ключі для кожного клієнта
- **Key management:** захищене управління ключами
- **End-to-end encryption:** шифрування від джерела до призначення

14.2.2. Integrity verification:

- **Checksums:** контрольні суми для всіх файлів
- **Digital signatures:** підписи цілісності backup
- **Test restores:** регулярна перевірка відновлення
- **Corruption detection:** виявлення пошкоджених файлів

14.2.3. Access control:

- **Role-based access:** доступ за ролями
- **Audit trails:** логування всіх операцій
- **Immutable backups:** незмінювані backup файли
- **Air-gapped storage:** фізично ізольовані копії

14.3. DISASTER RECOVERY

14.3.1. Business continuity planning:

- **Recovery Time Objective (RTO):** 4 години для критичних систем
- **Recovery Point Objective (RPO):** 15 хвилин втрати даних максимум
- **Maximum Tolerable Downtime (MTD):** 24 години загального простою
- **Work Recovery Time (WRT):** 1 година для відновлення роботи

14.3.2. DR scenarios:

- **Component failure:** відмова окремих компонентів
- **Site disaster:** повна недоступність дата-центру
- **Regional disaster:** природні катастрофи
- **Cyber attack:** масштабні кібератаки

14.3.3. Recovery procedures:

1. **Assessment phase:** оцінка масштабу катастрофи (30 хв)
2. **Activation phase:** активація DR планів (1 година)
3. **Recovery phase:** відновлення критичних систем (4 години)
4. **Restoration phase:** повне відновлення (24-72 години)

15. COMPLIANCE ТА СТАНДАРТИ БЕЗПЕКИ

15.1. МІЖНАРОДНІ СТАНДАРТИ

15.1.1. ISO/IEC 27001:2013:

- **ISMS (Information Security Management System)**
- **Risk management:** управління ризиками
- **Security controls:** 114 контролів безпеки
- **Continuous improvement:** постійне покращення
- **Annual recertification:** щорічна ресертифікація

15.1.2. SOC 2 Type II:

- **Security:** захист від несанкціонованого доступу
- **Availability:** доступність систем та операцій
- **Processing integrity:** цілісність обробки
- **Confidentiality:** захист конфіденційної інформації
- **Privacy:** захист персональних даних

15.1.3. PCI DSS Level 1:

- **Build secure networks:** побудова захищених мереж
- **Protect cardholder data:** захист даних власників карток
- **Vulnerability management:** управління уразливостями
- **Access control:** контроль доступу
- **Monitor networks:** моніторинг мереж
- **Information security policy:** політики інформаційної безпеки

15.2. НАЦІОНАЛЬНІ ВИМОГИ

15.2.1. Законодавство України:

- **Закон "Про основні засади забезпечення кібербезпеки"**
- **Закон "Про захист персональних даних"**
- **Закон "Про телекомунікації"**
- **Технічний регламент щодо електромагнітної сумісності**

15.2.2. Відомчі вимоги:

- **НКЦК України:** вимоги кібербезпеки
- **НКРЗІ:** ліцензування телекомунікацій
- **НБУ:** вимоги для банківського сектору
- **ДССЦ:** криптографічний захист

15.3. ГАЛУЗЕВІ СТАНДАРТИ

15.3.1. NIST Cybersecurity Framework:

- **Identify:** ідентифікація ризиків та активів
- **Protect:** захист критичної інфраструктури
- **Detect:** виявлення кіберзагроз
- **Respond:** реагування на інциденти
- **Recover:** відновлення після інцидентів

15.3.2. CIS Controls:

- **Basic controls (1-6):** базові заходи безпеки
- **Foundational controls (7-16):** фундаментальні контролі
- **Organizational controls (17-20):** організаційні процеси

16. НАВЧАННЯ ТА ПІДВИЩЕННЯ ОБІЗНАНОСТІ

16.1. ПРОГРАМИ НАВЧАННЯ ПЕРСОНАЛУ

16.1.1. Security awareness training:

- **Onboarding security:** навчання нових співробітників
- **Annual refresher:** щорічне оновлення знань
- **Role-specific training:** спеціалізоване навчання за ролями
- **Compliance training:** навчання вимогам регулювання

16.1.2. Technical training:

- **Security tools:** навчання роботи з інструментами безпеки
- **Incident response:** тренінги реагування на інциденти
- **Penetration testing:** навчання тестування на проникнення
- **Forensics:** комп'ютерно-криміналістичні навички

16.2. ПРОГРАМИ ДЛЯ КЛІЄНТІВ

16.2.1. Security education:

- **Best practices guides:** керівництва з кращих практик
- **Webinars:** регулярні вебінари з безпеки
- **Security alerts:** сповіщення про нові загрози
- **Knowledge base:** база знань з безпеки

16.2.2. Technical assistance:

- **Hardening guides:** керівництва з захищення систем
- **Security consulting:** консультації з безпеки
- **Incident support:** допомога при інцидентах
- **Vulnerability assessments:** оцінки уразливостей

16.3. БЕЗПЕРЕРВНИЙ РОЗВИТОК

16.3.1. Professional development:

- **Certifications:** професіональні сертифікації (CISSP, CISM, CEH)
- **Conference attendance:** участь у конференціях
- **Industry training:** галузеві тренінги
- **Peer collaboration:** співпраця з колегами

16.3.2. Knowledge sharing:

- **Internal presentations:** внутрішні презентації
- **Case studies:** аналіз реальних кейсів
- **Lessons learned:** висновки з інцидентів
- **Best practice documentation:** документування кращих практик

17. БЕЗПЕКА КЛІЄНТСЬКИХ VPS

17.1. БАЗОВІ ВИМОГИ БЕЗПЕКИ

17.1.1. Обов'язкові заходи для клієнтів:

- **Зміна стандартних паролів:** негайно після отримання доступу
- **Встановлення оновлень ОС:** регулярні патчі безпеки
- **Налаштування файрволу:** обмеження непотрібних портів
- **Відключення непотрібних сервісів:** мінімізація поверхні атак

17.1.2. Рекомендовані заходи:

- **SSH key authentication:** використання ключів замість паролів
- **Fail2ban configuration:** автоматичне блокування атак

- **Log monitoring:** моніторинг системних логів
- **Regular backups:** регулярне створення backup

17.2. ДОПОМОГА З БЕЗПЕКИ

17.2.1. Automated security:

- **ClamAV antivirus:** безкоштовний антивірус для Linux
- **rkhunter/chkrootkit:** сканери rootkit'ів
- **AIDE/Tripwire:** моніторинг цілісності файлів
- **Logwatch:** автоматичний аналіз логів

17.2.2. Security services:

- **Managed security:** управління безпекою VPS (+500 грн/міс)
- **Vulnerability scanning:** щомісячне сканування (+200 грн/міс)
- **Security hardening:** початкове налаштування (+1000 грн)
- **Incident response:** допомога при інцидентах (+300 грн/година)

17.3. ЗАБОРОНЕНА ДІЯЛЬНІСТЬ

17.3.1. Категорично заборонено:

- **Hacking tools:** інструменти для злому інших систем
- **Botnets:** участь у зомбі-мережах
- **Cryptocurrency mining:** майнінг без дозволу
- **Proxy abuse:** зловмисне використання проксі
- **Spam operations:** масові розсилки спаму

17.3.2. Санкції за порушення:

- **Попередження:** письмове попередження (1-й раз)
- **Тимчасова блокировка:** 24-72 години (2-й раз)
- **Припинення сервісу:** остаточне блокування (3-й раз)
- **Правові дії:** звернення до правоохоронців (кримінальні дії)

18. УПРАВЛІННЯ РИЗИКАМИ

18.1. ІДЕНТИФІКАЦІЯ РИЗИКІВ

18.1.1. Категорії ризиків:

- **Technical risks:** технічні ризики обладнання
- **Operational risks:** операційні ризики процесів
- **Security risks:** ризики інформаційної безпеки
- **Compliance risks:** ризики недотримання вимог
- **Business risks:** бізнес-ризики репутації
- **Environmental risks:** ризики навколишнього середовища

18.3. BUSINESS CONTINUITY

18.3.1. Continuity planning:

- **Business Impact Analysis (BIA):** аналіз впливу на бізнес
- **Critical process identification:** ідентифікація критичних процесів
- **Recovery strategies:** стратегії відновлення
- **Testing and maintenance:** тестування та підтримка

18.3.2. Crisis management:

- **Crisis response team:** команда антикризового реагування
- **Communication plans:** плани комунікацій
- **Media relations:** відносини зі ЗМІ
- **Stakeholder management:** управління зацікавленими сторонами

19. ЗВІТНІСТЬ ТА МЕТРИКИ БЕЗПЕКИ

19.1. KEY PERFORMANCE INDICATORS (KPIs)

19.1.1. Security metrics:

- **Mean Time to Detection (MTTD):** середній час виявлення інцидентів
- **Mean Time to Response (MTTR):** середній час реагування
- **Security incident frequency:** частота інцидентів безпеки
- **Vulnerability patch time:** час усунення уразливостей
- **Security awareness training completion:** відсоток пройденого навчання

19.1.2. Operational metrics:

- **System availability:** доступність систем
- **Backup success rate:** успішність резервного копіювання
- **Recovery time objective achievement:** досягнення цілей відновлення
- **Compliance audit results:** результати аудитів відповідності

19.2. РЕГУЛЯРНА ЗВІТНІСТЬ

19.2.1. Internal reporting:

- **Daily security briefings:** щоденні брифінги безпеки
- **Weekly incident summaries:** тижневі зведення інцидентів
- **Monthly security scorecards:** місячні звітні карти
- **Quarterly risk assessments:** квартальні оцінки ризиків
- **Annual security reviews:** річні огляди безпеки

19.2.2. External reporting:

- **Regulatory compliance reports:** звіти про відповідність регулюванню
- **Customer security updates:** оновлення безпеки для клієнтів
- **Vendor security assessments:** оцінки безпеки постачальників
- **Insurance reporting:** звітність для страхових компаній

19.3. AUDIT TA ASSESSMENT

19.3.1. Internal audits:

- **Monthly security audits:** щомісячні аудити безпеки
- **Quarterly compliance checks:** квартальні перевірки відповідності
- **Annual comprehensive review:** річний всебічний огляд
- **Ad-hoc investigations:** спеціальні розслідування

19.3.2. External audits:

- **ISO 27001 certification audit:** сертифікаційний аудит
- **SOC 2 examination:** перевірка SOC 2
- **Penetration testing:** зовнішнє тестування на проникнення
- **Regulatory inspections:** регулятивні перевірки