NIST SP 800-53
НД ТЗІ 2.3-025-24

Security Board	**Служба Захисту Інформації (СЗІ)**
Security Framework	**Система Технічного Захисту Інформації (СТЗІ)**
Security Profiles	**Комплексна Система Захисту Інформації (КСЗІ)**
Autority to Operate	**Авторизація Системи Захисту (АСЗ)**

https://erp.uno/ca/ — ERP/1: Сертифікати Системи Захисту (ССЗ)

https://ca.n2o.dev/priv/nist.pdf — Загальна інформація про структуру системи технічного захисту інформації (СТЗІ)

https://ca.n2o.dev/priv/security-policy.pdf — Політика і модель комплексної системи захисту інформації (КСЗІ)

https://ca.n2o.dev/priv/security-architecture.pdf — Технічне завдання на побудову авторизації системи захисту (АСЗ)

Theory

SF/NIST

- NIST.PDF
- SECURITY-POLICY.PDF
- L1_BASE_409_126.PDF
- L1_BASE_419_155.PDF
- L2_INDUSTRY_PROFILE_190.PDF

SP/ATO

- SECURITY-ARCHITECTURE.PDF
- ДСА ORDERS (2 ORDERS)
- ICC ORDERS (6 ORDERS)
- L3_TARGET_PROFILE_DC_320.PDF
- L3_TARGET_PROFILE_COURT_350.PDF

Practice

SF/CMDB/SP

- cmdb_profiles.ex
- profile_data.ex
- spe.ex
- tex.ex
- family.ex
- npa.ex
- param.ex
- l1_*.ex
- l2_*.ex
- l3_*.ex
- sys.ex
- hw.ex
- proc.ex
- net.ex
- risk.ex
- abac.ex

SP/SB/ATO

- iss_order_admin_appointment.pdf
- iss_order_at_ir_ma_ps_pe.pdf
- iss_order_kszi_development.pdf
- iss_order_physical_access.pdf
- iss_order_szi_establishment.pdf
- dsa_order_audit_plan.pdf

Legal Documents

Система Технічного Захисту Інформації (СТЗІ) НД ТЗІ 2.3-025-24

НД ТЗІ 1.1-002-99.txt
НД ТЗІ 1.1-003-99.txt
НД ТЗІ 1.4-001-00.txt
НД ТЗІ 1.4-002-08.txt
НД ТЗІ 1.5-001-00.txt
НД ТЗІ 1.5-002-12.txt
НД ТЗІ 1.6-005-13.txt
НД ТЗІ 2.3-001-01.txt
НД ТЗІ 2.3-002-01.txt
НД ТЗІ 2.3-003-01.txt
НД ТЗІ 2.3-004-01.txt
НД ТЗІ 2.3-005-01.txt
НД ТЗІ 2.3-006-01.txt

НД ТЗІ 2.3-025-24-T1.txt
НД ТЗІ 2.3-025-24-T2.txt
НД ТЗІ 2.3-025-24-T3.txt
НД ТЗІ 3.6-006-24.txt

НД ТЗІ 2.5-004-99.txt
НД ТЗІ 2.5-005-99.txt
НД ТЗІ 2.5-006-99.txt
НД ТЗІ 2.5-008-02.txt
НД ТЗІ 2.5-010-03.txt
НД ТЗІ 2.6-001-11.txt
НД ТЗІ 2.7-002-99.txt
НД ТЗІ 2.7-009-09.txt
НД ТЗІ 2.7-010-09.txt
НД ТЗІ 2.7-011-12.txt
НД ТЗІ 3.6-001-00.txt
НД ТЗІ 3.7-001-99.txt
НД ТЗІ 3.7-003-23.txt
НД ТЗІ 4.7-001-01.txt

НАД №409 від 30.06.2025.txt
НАД №419 від 02.07.2025.txt

Security Board

Служба Захисту Інформації (СЗІ)

Administrators

Domain Controller Admin (DCA)
Database Admin (DBA)
Security Admin (SA)
Network Admin (NA)
Application Admin (AA)

Directors

Security Team Directory (STD)
Development Team Director (DTD)
System Analysis Team Director (SAD) Architect
Infrastructure Team Director (DTD)

CDTO

Державна Судова Адміністрація (ДСА)
Державне Підприємство (ДП)
Вища Рада Правосуддя (ВРП)
Вища Кваліфікаційна Комісія Суддів (ВККС)

Security System

Система Технічного Захисту Інформації (СТЗІ) НД ТЗІ 2.3-025-24

Organizational

Awareness and Training (AT)
Incident Response (IR)
Maintenance (MA)
Personnel Security (PS)
Physical and Environmental Protection (PE)

Metainformational

Planning (PL)
Program Management (PM)
Risk Assessment (RA)
System and Services Acquisition (SA)
Privacy (PT)
Security Evaluation Framework (CMDB)

Technical

Access Control (AC)
Audit and Accountability (AU)
Assessment, Authorization, and Monitoring (CA)
Configuration Management (CM)
Contingency Planning (CP)
Identification and Authentication (IA)
Media Protection (MP)
System and Communications Protection (SC)
System and Information Integrity (SI)
Supply Chain Risk Management (SR)

Awareness and Training (AT)

Система Технічного Захисту Інформації (СТЗІ) НД ТЗІ 2.3-025-24

AT-1 — Policy for Literacy Training and Awareness
AT-2 — Literacy Training and Awareness
AT-2(1) — Practical Lessons
AT-2(2) — Phishing Simulations
AT-2(3) — Social Engineering
AT-2(4) — Anomaly Behavior Analysis
AT-3 — Role-Based Training
AT-4 — Educational System with Exams
AT-6 — Feedback Analysis

Risk Assessment (RA)

Система Технічного Захисту Інформації (СТЗІ) НД ТЗІ 2.3-025-24

RA-2 — Security Categorization
RA-3 — Risk Assessment
RA-5 — Vulnerability Monitoring and Scanning

System and Services Acquisition (SA)

Система Технічного Захисту Інформації (СТЗІ) НД ТЗІ 2.3-025-24

SA-5 — System Documentation
SA-9 — External System Services
SA-11 — Developer Testing and Evaluation

Access Control (AC)

Система Технічного Захисту Інформації (СТЗІ) НД ТЗІ 2.3-025-24

AC-1 — Automated System Account Management Policy
AC-2(1) — Automated System Account Management
AC-2(2) — Removal of Temporary and Emergency Accounts
AC-2(3) — Disable Inactive Accounts
AC-2(4) — Automated Audit Actions
AC-2(5) — Inactivity Logout
AC-2(6) — Dynamic Privilege Management
AC-2(7) — Role-Based Schemes
AC-2(8) — Dynamic Account Management.
AC-2(9) — Restrictions on Use of Shared and Group Accounts.
AC-2(10) — Shared and Group Account Credential Change
AC-2(11) — Usage Conditions
AC-2(12) — Account Monitoring for Atypical Usage
AC-2(13) — Disable Accounts of High-Risk Individuals
AC-7(2) — Purge or Wipe Mobile Device

AC-3(3) — Mandatory Access Control
AC-3(4) — Discretionary Access Control
AC-3(7) — Role-Based Access Control
AC-3(10) — Audited Override of Access Control Mechanisms
AC-3(11) — Restrict Access to Specific Information Types
AC-3(12) — Assert and Enforce Application Access
AC-3(13) — Attribute-Based Access Control
AC-3(15) — Discretionary and Mandatory Access Control
AC-5 — Separation of Duties
AC-6 — Least Privilege
AC-6(1) — Authorize Access to Security Functions
AC-6(2) — Non-Privileged Access for Non-Security Functions
AC-6(3) — Network Access to Privileged Commands
AC-6(4) — Separate Processing Domains
AC-6(5) — Privileged Accounts
AC-6(7) — Review of User Privileges
AC-6(9) — Log Use of Privileged Functions
AC-6(10) — Prohibit Non-Privileged Users from Executing Privileged Functions

Access Control (AC-4) BPMN/ABAC

Система Технічного Захисту Інформації (СТЗІ) НД ТЗІ 2.3-025-24

AC-4 (Base Control)
AC-4(1) — Object Security and Privacy Attributes
AC-4(2) — Data Processing Domains
AC-4(3) — Dynamic Information Flow Control
AC-4(4) — Flow Control of Encrypted Information
AC-4(5) — Embedding Data Types
AC-4(6) — Metadata
AC-4(7) — One-Way Flow Mechanisms
AC-4(8) — Security Policy Filters
AC-4(9) — Personnel-Conducted Reviews
AC-4(10) — Filters (De)Activation
AC-4(11) — Security Policy Filter Configuration
AC-4(12) — Data Type Identifiers
AC-4(13) — Decomposition
AC-4(14) — Security Policy Filter Constraints
AC-4(15) — Detection of Unauthorized Info
AC-4(17) — Domain Authentication
AC-4(19) — Metadata Verification
AC-4(20) — Approved Decisions
AC-4(21) — Physical and Logical Flows
AC-4(22) — Single Access Point
AC-4(24) — Normal Form
AC-4(25) — Data Sanitization
AC-4(26) — Audit Filter Actions
AC-4(28) — Linear Filtering
AC-4(29) — Orchestration Mechanism Filter
AC-4(30) — Multi-Process Filtering Mechanisms
AC-4(31) — Prevention of Transfer of Unfiltered Content
AC-4(32) — Information Transfer Process Requirements

Privacy (PT)

Система Технічного Захисту Інформації (СТЗІ) НД ТЗІ 2.3-025-24

PT-2 — Authority to Process Personally Identifiable Information
PT-4 — Consent Management
PT-6 — Disassociation

Assessment, Authorization, and Monitoring (CA)

Система Технічного Захисту Інформації (СТЗІ) НД ТЗІ 2.3-025-24

CA-2 — Control Assessments
CA-6 — Authorization
CA-7 — Continuous Monitoring
CA-8 — Penetration Testing
CA-9 — Internal System Connections

Configuration Management (CM)

Система Технічного Захисту Інформації (СТЗІ) НД ТЗІ 2.3-025-24

CM-2, CM-3 — Baseline Configuration and Configuration Change Control
CM-6 — Configuration Settings
CM-7 — Least Functionality
CM-8 — System Component Inventory
CM-9 — Configuration Management Plan

Contingency Planning (CP)

Система Технічного Захисту Інформації (СТЗІ) НД ТЗІ 2.3-025-24

CP-2 — Contingency Plan
CP-7 — Alternate Processing Site
CP-9 — Information System Backup
CP-10 — Information System Recovery and Reconstitution

Identification and Authentication (IA)

Система Технічного Захисту Інформації (СТЗІ) НД ТЗІ 2.3-025-24

IA-2 — Identification and Authentication (Organizational Users)
IA-2(1) — MFA for Privileged Accounts (Network Access)
IA-2(2) — MFA for Non-Privileged Accounts
IA-5 — Authenticator Management
IA-5(1) — Password-Based Authentication
IA-8 — Identification and Authentication (Non-Organizational Users)

Media Protection (MP)

Система Технічного Захисту Інформації (СТЗІ) НД ТЗІ 2.3-025-24

MP-2, MP-4 — Media Access and Storage
MP-5 — Media Transport
MP-6 — Media Sanitization
MP-7 — Media Use

System and Communications Protection (SC)

Система Технічного Захисту Інформації (СТЗІ) НД ТЗІ 2.3-025-24

SC-7 — Boundary Protection
SC-7(3) — Access Points
SC-8 — Transmission Confidentiality and Integrity
SC-12 — Cryptographic Key Establishment and Management
SC-28 — Protection of Information at Rest

System and Information Integrity (SI)

Система Технічного Захисту Інформації (СТЗІ) НД ТЗІ 2.3-025-24

SI-3 — Malicious Code Protection
SI-4 — System Monitoring
SI-7 — Software, Firmware, and Information Integrity
SI-10 — Information Input Validation

Supply Chain Risk Management (SR)

Система Технічного Захисту Інформації (СТЗІ) НД ТЗІ 2.3-025-24

SR-3 — Supply Chain Controls and Processes
SR-4 — Provenance
SR-11 — Component Authenticity

Security Profiles

Комплексна Система Захисту Інформації (КСЗІ)

Base Profiles

Public and Confidential (126) НАД №409
Official (155) НАД №419

Industry Profiles

Public and Confidential (190)
Official (200)

Target Profiles

Державна Судова Адміністрація (ДСА)
Державне Підприємство (ДП)
Вища Рада Правосуддя (ВРП)
Вища Кваліфікаційна Комісія Суддів (ВККС)

Risk Assessment (CA.PRO.risk)

```
iex> CA.PRO.risk("ERP")
[
{"RISK-OS-01", "Вразливості Active Directory (Kerberoasting, Pass-the-Hash, Golden Ticket)", ["AC", "IA", "SC"]},
{"RISK-OS-02", "Зловживання WMI та PowerShell (Fileless-методи)", ["SI", "SC", "CM"]},
{"RISK-OS-03", "Вразливості на рівні ядра (BYOVD, Ring 0)", ["SI", "CM"]},
{"RISK-OS-04", "Маніпуляція маркерами доступу (Token Stealing)", ["AC", "AU"]},
{"RISK-OS-05", "Некоректні дозволи NTFS / Share (Orphaned SIDs)", ["AC", "CM"]},
{"RISK-OS-06", "Підвищення привілеїв Linux (Kernel, SUID, Dirty COW)", ["AC", "SI"]},
{"RISK-OS-07", "Втеча з контейнерів Docker/Kubernetes", ["SC", "CM"]},
{"RISK-OS-08", "Зловживання eBPF (прихований моніторинг)", ["AU", "SI"]},
{"RISK-OS-09", "Ін’єкції динамічних бібліотек (LD_PRELOAD)", ["SI", "CM"]},
{"RISK-OS-10", "Вразливості PAM (обхід автентифікації)", ["IA", "AC"]},
{"RISK-OS-11", "Обхід XProtect / Gatekeeper / SIP (macOS)", ["CM", "SI"]},
{"RISK-OS-13", "TCC Bypass & Spyware (macOS)", ["SI", "PE"]},
{"RISK-OS-14", "Dyld Hijacking (macOS)", ["SI"]},
{"RISK-OS-15", "Обхід Pointer Authentication PAC (Apple Silicon)", ["SI", "SA"]},
{"RISK-CRY-01", "Пост-квантові загрози SNDL (Store Now, Decrypt Later)", ["SC", "RA", "SA"]},
{"RISK-CRY-02", "Атаки сторонніми каналами (DPA, таймінг, EM)", ["SC", "PE", "SA"]},
{"RISK-CRY-03", "Fault Injection (Glitching, Voltage Drop)", ["PE", "SI", "SC"]},
{"RISK-CRY-07", "Вразливості криптобібліотек \foreignlanguage{ukrainian}{ДСТУ} (Калина, Купина, Padding Oracle)", ["SA", "SI"]}
{"RISK-CRY-08", "Недостатня ентропія генератора псевдовипадкових чисел (PRNG)", ["SC"]},
{"RISK-CRY-09", "Втрата або перехоплення PIN-кодів HSM (кейлогери)", ["IA", "AT", "PE"]},
{"RISK-CRY-10", "Фізична деструкція носіїв «Автор» (CryptoCard)", ["PE", "MP"]},
{"RISK-CRY-11", "Вразливості CCID драйверів токенів (ескалація привілеїв)", ["SI", "CM"]},
{"RISK-CRY-12", "Підміна сесій PKCS#11 (MitM між ПЗ ЦСК та HSM)", ["SC", "SI"]},
{"RISK-NET-01", "BGP Hijacking & Route Leaks (підміна анонсів AS)", ["SC", "SI"]},
{"RISK-NET-02", "Атаки L2 (VLAN Hopping, ARP Spoofing, STP атаки)", ["SC", "AC"]},
{"RISK-NET-03", "Вразливості IPSec / VPN (IKE downgrade, PSK витік)", ["SC", "IA"]},
{"RISK-NET-04", "DDoS (Slowloris, SYN Flood, ампліфікація DNS/NTP)", ["SC", "IR"]},
ї
```

Network Architecture (CA.PRO.net)

```
iex> CA.PRO.net("ERP")
[
{"NET-DMZ-01", "OCSP / CRL публічний ендпоінт", "публічна підмережа"},
{"NET-DMZ-02", "Веб-портал ЦСК", "публічна підмережа"},
{"NET-INT-01", "Сегмент серверів БД", "внутрішня підмережа БД"},
{"NET-INT-02", "Сегмент робочих станцій операторів", "внутрішня підмережа АРМ"},
{"NET-MGT-01", "VLAN IPMI / iLO адміністрування", "management VLAN"},
{"NET-AIR-01", "Кореневий ЦСК (офлайн вузол)", "N/A"}
]
```

Role-Based Access Control (CA.PRO.roles)

```
iex> CA.PRO.roles("ERP")
[
{"ROLE-ADM-01", "Адміністратор безпеки", ["security_admin"]},
{"ROLE-AUD-01", "Аудитор", ["auditor"]},
{"ROLE-OPR-01", "Оператор реєстрації", ["reg_operator"]},
{"ROLE-SYS-01", "Системний процес (Machine-to-Machine)", ["ocsp_service", "crl_generator"]},
{"ROLE-SADM-01", "Глобальний суперадміністратор (root/administrator)", ["global_root_admin", "infra_super_user"]}
]
```

System Software Components (CA.PRO.sys)

```
iex> CA.PRO.sys("ERP")
[
{"SYS-OS-01-WIN", "Windows Server 2025 Datacenter (NATO STIG + DISA hardened) (2025 Datacenter)", []},
{"SYS-OS-01-ESX", "VMware ESXi 8.0 Update 3 (vSphere Foundation) (8.0 U3)", []},
{"SYS-OS-02-W11", "Windows 11 Pro 24H2 (24H2 (Build 26100))", []},
{"SYS-APP-01-IIT", "IIT Користувач ЦСК-1 (бібліотека «IIT Gryada-301») (3.0.1)", []},
{"SYS-APP-01-CIP", "Сайфер HSM Middleware (PKCS#11 + CMS + TSP клієнт) (2.8)", []},
{"SYS-APP-01-SIGN", "Автор E-Підпис Сервер (batch signing, LTV, XAdES-BES) (5.2)", []},
{"SYS-APP-02-WZ", "Wazuh 4.9 SIEM/XDR (OSSEC-based, FIM, compliance CIS/NIST) (4.9)", []},
{"SYS-APP-02-ZBX", "Zabbix 7.2 (active agents, encrypted PSK transport, alerting) (7.2 LTS)", []},
{"SYS-DB-01-PG", "PostgreSQL 17.2 (TDE + pgAudit + pg_partman) (17.2)", []},
{"SYS-DB-01-ORA", "Oracle Database 23ai (Advanced Security Option, TDE, Vault) (23ai (23.5))", []},
{"SYS-DB-02-RDS", "Redis 7.4 (TLS 1.3, ACL, persistence RDB+AOF) (7.4)", []},
{"SYS-INF-01-VBR", "Veeam Backup & Replication 12.3 (immutable backups, SureBackup) (12.3)", []},
{"SYS-INF-01-BCL", "Bacula Community 15.0 (offline tape + air-gapped archive) (15.0)", []},
{"SYS-MW-01-NGX", "Nginx 1.27 (TLS 1.3 only, OCSP Stapling, CT Logs, HSTS) (1.27)", []},
{"SYS-MW-01-HAP", "HAProxy 3.0 (HA pair, health checks, rate limiting) (3.0 LTS)", []},
{"SYS-MW-02-IPA", "FreeIPA 4.12 (Kerberos V, OTP, CA sub-ідентифікатор) (4.12)", []}
]
```

Hardware Inventory (CA.PRO.inventory)

```
iex> CA.PRO.inventory("ERP")
[
{"ERP-STG-01", "ERP-STG-2025-001", "5HT Technology AllFlash NVMe Array (Sapphire Rapids Storage Controller)"},
{"ERP-STG-02", "ERP-STG-2025-002", "5HT Technology AllFlash NVMe Array"},
{"ERP-TAPE-01", "ERP-STG-2025-003", "HPE StoreEver MSL3040 Tape Library"},
{"ERP-WS-01", "ERP-WS-2025-001", "5HT Technology Workstation Compact (Sapphire Rapids)"},
{"ERP-WS-02", "ERP-WS-2025-002", "5HT Technology Workstation Compact (Sapphire Rapids)"},
{"ERP-KZI-01", "ERP-KZI-2025-001", "IIT Gryada-301 PCIe HSM"},
{"ERP-KZI-02", "ERP-KZI-2025-002", "IIT Gryada-301 PCIe HSM"},
{"ERP-KZI-03", "ERP-KZI-2025-003", "Автор CryptoCard Smart-01 (е-Токен, Смарт-карта)"},
{"ERP-NET-01", "ERP-NET-2025-001", "Cisco Catalyst 9500-48Y4C"},
{"ERP-NET-02", "ERP-NET-2025-002", "Cisco Catalyst 9500-48Y4C"},
{"ERP-NET-03", "ERP-NET-2025-003", "Cisco ASR 1002-HX Router"},
{"ERP-FW-01", "ERP-NET-2025-004", "Cisco Firepower 4145 NGFW (FTD 7.6)"},
{"ERP-FW-02", "ERP-NET-2025-005", "Cisco Firepower 4145 NGFW (FTD 7.6)"},
{"ERP-SRV-01", "ERP-2025-001", "5HT Technology Tristellar 3U"},
{"ERP-SRV-02", "ERP-2025-002", "5HT Technology Tristellar 3U"},
{"ERP-SRV-03", "ERP-2025-003", "5HT Technology Quadstellar 4U"},
{"ERP-SRV-04", "ERP-2025-004", "5HT Technology Quadstellar 4U"},
]
```

Base Profile

Базовий профіль безпеки

Public and Confidential (126) НАД №409

ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України
___ _____ 2025 року № ___

Базовий профіль
безпеки системи, де обробляється відкрита або конфіденційна інформація

№	Назва дії з безпеки інформації	Зміст дії	Заходи захисту відповідно до НД ТЗІ 3.6-006-24	Мінімальні необхідні параметри налаштування заходів захисту відповідно до НД ТЗІ 3.6-006-24
1	2	3	4	5
Управління доступом				
1.	Управління обліковими записами	1) визначити дозволені та заборонені типи облікових записів у системі; 2) створювати, активувати, змінювати, деактивувати та видаляти облікові записи із	AC-2	h.1. 24 години h.2. 24 години h.3. 24 години j. мінімум щоквартально

UB
Адміністрація Держспецзв'язку
№04/04/02-15567/2025/ВН від 30.06.2025
КЕП: Головенко А. В. 30.06.2025 15:06
3FAA9288358EC003040000068D93A009159DF00
Сертифікат дійсний з 30.01.2025 00:00 до 29.01.2027 23:59

https://ca.n2o.dev/priv/base-profile-409.pdf

Official (155) НАД №419

ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України
___ _____ 2025 року № ___

Базовий профіль
безпеки системи, де обробляється службова інформація

№	Назва дії з безпеки інформації	Зміст дії	Заходи захисту відповідно до НД ТЗІ 3.6-006-24	Мінімальні необхідні параметри налаштування заходів захисту відповідно до НД ТЗІ 3.6-006-24
1	2	3	4	5
Управління доступом				
1.	Управління обліковими записами	1) визначити дозволені та заборонені типи облікових записів у системі; 2) створювати, активувати, змінювати, деактивувати та видаляти облікові записи із системи відповідно до політики, процедур, передумов і критеріїв організації;	AC-2	h.1. 24 години h.2. 24 години h.3. 24 години j. мінімум щоквартально
			AC-2(3)	1-ий параметр: не більше 72 годин d. 90 днів
			AC-2(5)	кінець робочого дня користувача

UB
Адміністрація Держспецзв'язку
№04/04/02-15743/2025/ВН від 01.07.2025
КЕП: Головенко А. В. 01.07.2025 17:43
3FAA9288358EC003040000068D93A009159DF00
Сертифікат дійсний з 30.01.2025 00:00 до 29.01.2027 23:59

https://ca.n2o.dev/priv/base-profile-419.pdf

Industry Profile

Галузевий профіль безпеки

Більше 35 контрольних елементів до Базового

IA-2(1), IA-2(2), IA-5(2), IA-5(11), IA-5(12), IA-5(15), IA-5(17), IA-7, IA-2(12), AC-4(1), AC-4(2), AC-4(3), AC-4(19), AC-4(22), AC-4(29), AC-7(2), AC-15, AC-16, AC-19(1), AC-19(2), AC-19(4), MP-6, MP-8(4), PE-22, SC-8(1), SC-12, SC-17, SC-28(1), SC-28(2), SC-44, SC-49, SC-51, AU-10, AU-10(5), SI-7

iex(494)> length CA.L2.Court.controls
190

Приклади відкритих галузевих профілів

Міністерство культури
Міністерство цифрової трансформації (Трембіта)
Судова система

ЗАТВЕРДЖЕНО
Наказ Державна Судова Адміністрація України
_____ 2026 року №____

Галузевий профіль безпеки судової системи, що використовуються для надання хмарних послуг та/або послуг центру обробки даних публічним користувачам та/або критично важливим об'єктам інфраструктури

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
ПОЛІТИКИ ТА ПРОЦЕДУРИ				
1	Політики та процедури з безпеки	а. Розробити, задокументувати та поширити [Призначення: серед визначеного організацією персоналу або ролей]: 1. 2. [Вибір (один або декілька): Рівень організації; Рівень місії/бізнес-процесу; рівень системи] політики контролю доступу, яка: (а) містить мету, сферу застосування, ролі, відповідальність, зобов'язання керівництва, координацію між організаційними підрозділами та систему контролю відповідності (compliances);	AC-1	

https://ca.n2o.dev/priv/legal_l2_court_profile.pdf

Target Profile

Цільовий профіль безпеки

Профіль безпеки ЦОД

Містить окремі налаштування словників
— Inventory
— Roles
— Sys
— Data
— Risk
— Proc

```
iex(1)> length CA.TeX.unfold CA.L3.Cod.controls
316
```

Профіль безпеки судів

Містить окремі налаштування словників
— Inventory
— Roles
— Sys
— Data
— Risk
— Proc

```
iex(2)> length CA.TeX.unfold CA.L3.Court.controls
350
```

1.2.804.3.1.2.1 — Базовий профіль безпеки (L1)
1.2.804.3.1.2.2 — Галузевий профіль безпеки (L2)
1.2.804.3.1.2.3 — Цільовий профіль безпеки вищих судів (L3)
1.2.804.3.1.2.3.1 — Велика Палата Верховного Суду
1.2.804.3.1.2.3.2 — Касаційний адміністративний суд
1.2.804.3.1.2.3.3 — Касаційний господарський суд
1.2.804.3.1.2.3.4 — Касаційний кримінальний суд
1.2.804.3.1.2.3.5 — Касаційний цивільний суд
1.2.804.3.1.2.4 — Цільовий профіль безпеки вищих спеціалізованих судів (L3)
1.2.804.3.1.2.4.1 — Вищий суд з питань інтелектуальної власності
1.2.804.3.1.2.4.2 — Вищий антикорупційний суд
1.2.804.3.1.2.4.3 — Спеціалізований окружний адміністративний суд
1.2.804.3.1.2.4.4 — Спеціалізований апеляційний адміністративний суд
1.2.804.3.1.2.5 — Цільовий профіль судів (L3)
1.2.804.3.1.2.5.1 — Цільовий профіль безпеки місцевих судів (L4)
1.2.804.3.1.2.5.2 — Цільовий профіль безпек апеляційних судів (L4)
1.2.804.3.1.2.6 — Цільовий профіль безпеки органів та установ у системі правосуддя (L3)
1.2.804.3.1.2.6.1 — ДСА (L4)
1.2.804.3.1.2.6.2 — ТУ ДСА, допоміжні установи (L4)
1.2.804.3.1.2.6.3 — Рада суддів України (L4)
1.2.804.3.1.2.6.4 — ВРП (L4)
1.2.804.3.1.2.6.5 — ВККСУ (L4)
1.2.804.3.1.2.6.6 — Національна школа суддів України (L4)
1.2.804.3.1.2.6.7 — ГРД та ГРМЕ (L4)
1.2.804.3.1.2.6.8 — Служба судової охорони (L4)

Target Profile

Розширена структура профілів судової системи

Authority to Operate

Авторизація Системи Захисту (АСЗ)

Developer

Проводить оцінку ризиків, обстеження середовища та створює «технічні інструкції» — Технічне завдання (Цільовий профіль безпеки). Здійснює фізичну імплементацію архітектури безпеки: налаштовує криптографію, (АС-25), встановлює сертифікати та здає систему в дослідну експлуатацію.

Auditor

Отримує Технічне завдання від розробника та розробляє Програму експертизи. Проводить незалежний технічний аудит, інструментальне тестування та перевірку імплементованих контролів наживо. У разі успіху видає Експертний висновок для Держспецзв'язку.

Administrative Orders

Державна Судова Адміністрація (ДСА)

Про затвердження політики авторизації

Прийняття політик безпеки.
Формальний запуск процесу.

Про проведення аудиту інформаційної інфраструктури судів та затвердження дорожньої карти переходу від ЄСІТС до ЄСІКС

Наказ про проведення інвентаризації для оцінки ризиків.

Operational Orders

Державне Підприємство (ДП)

Про організацію робіт із розробки та впровадження КСЗІ

Формальний запуск процесу створення Технічного завдання.

Про визначення адміністраторів

Про прийняття рольової моделі.

Про затвердження Переліку осіб, які мають право доступу до приміщення серверної кімнати ЦОД

Про токени доступу.

Про створення Служби захисту інформації

Про зміну штатного розкладу.

Про затвердження Положення про розподіл відповідальності, прав та обов’язків адміністраторів ЄСІКС

Прийняття політик безпеки.

Про затвердження політики постачання

Про зміну політики закупівель, постачання, тестування, прийомки, постановки на баланс інформаційно-комунікаційних систем і підсистем.

2024—2026

maxim@synrc.com

Максим Сохацький