

**МІНІСТЕРСТВО ЮСТИЦІЇ  
УКРАЇНИ**

**АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ  
СЛУЖБИ СПЕЦІАЛЬНОГО  
ЗВ'ЯЗКУ ТА ЗАХИСТУ  
ІНФОРМАЦІЇ УКРАЇНИ**

**НАКАЗ**

м. Київ

№ \_\_\_\_\_ / \_\_\_\_\_

**Про внесення змін до наказу  
Міністерства юстиції України,  
Адміністрації Державної служби  
спеціального зв'язку та захисту  
інформації України від 05 грудня  
2013 року № 2563/5/645**

Відповідно до Закону України «Про електронний цифровий підпис», підпунктів 76, 77 пункту 4 Положення про Міністерство юстиції України, затвердженого постановою Кабінету Міністрів України від 02 липня 2014 року № 228, підпункту 2 пункту 3 та підпункту 7 пункту 4 Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 03 вересня 2014 року № 411, та з метою забезпечення технічного регулювання інфраструктури відкритих ключів та надання послуг електронного цифрового підпису

**НАКАЗУЄМО:**

1. Унести до наказу Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 05 грудня 2013 року № 2563/5/645 «Про затвердження переліків стандартів у сфері електронного цифрового підпису, перспективних для перегляду та гармонізації з європейськими та міжнародними стандартами відповідно до встановлених законодавством процедур» такі зміни:

- 1) заголовок наказу викласти у такій редакції:  
«Про затвердження Переліку міжнародних та європейських стандартів, інших актів технічного регулювання для гармонізації з метою реформування,

розвитку та забезпечення інтероперабельності системи електронного цифрового підпису»;

2) пункт 1 наказу викласти у такій редакції:

«1. Затвердити Перелік міжнародних та європейських стандартів, інших актів технічного регулювання для гармонізації з метою реформування, розвитку та забезпечення інтероперабельності системи електронного цифрового підпису.»;

3) пункт 2 замінити двома новими пунктами такого змісту:

«2. Міністерство юстиції України та Адміністрація Державної служби спеціального зв'язку та захисту інформації України як центральні органи виконавчої влади, на які постановою Кабінету Міністрів України від 13 березня 2002 року № 288 «Про затвердження переліків центральних органів виконавчої влади, на які покладаються функції технічного регулювання у визначених сферах діяльності та розроблення технічних регламентів» покладено функції технічного регулювання у сфері електронного цифрового підпису та захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом надають пропозиції щодо коригування цього переліку.

3. Установити, що цей перелік є підставою для розроблення пропозицій до Плану національної стандартизації на відповідний рік Міністерством юстиції України та Адміністрацією Державної служби спеціального зв'язку та захисту інформації України як центральними органами виконавчої влади, на які постановою Кабінету Міністрів України від 13 березня 2002 року № 288 «Про затвердження переліків центральних органів виконавчої влади, на які покладаються функції технічного регулювання у визначених сферах діяльності та розроблення технічних регламентів» покладено функції технічного регулювання у сфері електронного цифрового підпису та захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом.».

У зв'язку з цим пункти 3, 4 вважати відповідно пунктами 4, 5;

2. Визнати таким, що втратив чинність, Перелік стандартів у сфері електронного цифрового підпису, що підлягають перегляду, затверджений наказом Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 05 грудня 2013 року № 2563/5/645.

3. Перелік стандартів у сфері електронного цифрового підпису для гармонізації з європейськими та міжнародними стандартами викласти у новій редакції, що додається.

4. Контроль за виконанням цього наказу покласти на заступника Міністра юстиції України Бондарчука І.В. та першого заступника Голови Державної служби спеціального зв'язку та захисту інформації України Корнейка О.В.

**Міністр юстиції України**

**Голова Державної служби  
спеціального зв'язку та захисту  
інформації України**

\_\_\_\_\_ **П.Д. ПЕТРЕНКО**

\_\_\_\_\_ **В.П. ЗВЕРЄВ**

## ЗАТВЕРДЖЕНО

Наказ Міністерства юстиції України,  
Адміністрації Державної служби  
спеціального зв'язку та захисту  
інформації України

05 грудня 2013 року № 2563/5/645

(у редакції наказу Міністерства юстиції  
України, Адміністрації Державної  
служби спеціального зв'язку та захисту  
інформації України

від \_\_\_\_\_ № \_\_\_\_\_ / \_\_\_\_\_)

**Перелік міжнародних та європейських стандартів, інших актів  
технічного регулювання для гармонізації з метою реформування,  
розвитку та забезпечення інтероперабельності системи електронного  
цифрового підпису**

**I. Криптографічні механізми та протоколи електронного цифрового підпису**

1. ISO/IEC 9796-2:2010  
«Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms».
2. ISO/IEC 9796-3:2006  
«Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms».
3. ISO/IEC 14888-1:2008  
«Information technology – Security techniques – Digital signatures with appendix – Part 1: General».
4. ISO/IEC 14888-2:2008  
«Information technology – Security techniques – Digital signatures with appendix – Part 2: Integer factorization based mechanisms».
5. ISO/IEC 14888-3:2006  
«Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms».
6. ISO/IEC 15946-1:2008  
«Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General».
7. ISO/IEC 15946-5:2009  
«Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 5: Elliptic curve generation».

## **II. Інфраструктура відкритих ключів**

1. ISO/IEC 18014 -1:2008  
«Information technology – Security techniques – Time-stamping services – Part 1: Framework».
2. ISO/IEC 18014-2:2009  
«Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens».
3. ISO/IEC 18014-3:2009  
«Information technology – Security techniques – Time-stamping services – Part 3: Mechanisms producing linked tokens».
4. ISO/IEC 9594-8:2008  
«Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks».

## **III. Управління ключами**

1. ISO/IEC 11770-1:2010  
«Information technology – Security techniques – Key management – Part 1: Framework».
2. ISO/IEC 11770-2:2008  
«Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques».
3. ISO/IEC 11770-3:2008  
«Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques».
4. ISO/IEC 11770-4:2006  
«Information technology – Security techniques – Key management – Part 4: Mechanisms based on weak secrets».
5. ISO/IEC 11770-5:2011  
«Information technology – Security techniques – Key management – Part 5: Group key management».

## **IV. Геш-функції та коди автентифікації повідомлень**

1. ISO/IEC 9797-1:2011  
«Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher».
2. ISO/IEC 9797-2:2011  
«Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function».
3. ISO/IEC 9797-3:2011  
«Information technology – Security techniques – Message Authentication Codes (MACs) – Part 3: Mechanisms using a universal hash-function».
4. ISO/IEC 10118-1:2003  
«Information technology – Security techniques – Hash-functions – Part 1: General».
5. ISO/IEC 10118-2:2010  
«Information technology – Security techniques – Hash-functions – Part 2: Hash-functions using an n-bit block cipher».

6. ISO/IEC 10118-3:2005  
«Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions».
7. ISO/IEC 10118-4:1998  
«Information technology – Security techniques – Hash-functions – Part 4: Hash-functions using modular arithmetic».

#### **V. Криптографічні протоколи автентифікації та ідентифікації**

1. ISO/IEC 9798-1:2010  
«Information technology – Security techniques – Entity authentication – Part 1: General».
2. ISO/IEC 9798-2:2008  
«Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms».
3. ISO/IEC 9798-3:1998  
«Information technology – Security techniques – Entity authentication – Part 3: Mechanisms using digital signature techniques».
4. ISO/IEC 9798-4:1999  
«Information technology – Security techniques – Entity authentication – Part 4: Mechanisms using a cryptographic check function».
5. ISO/IEC 9798-5:2009  
«Information technology – Security techniques – Entity authentication – Part 5: Mechanisms using zero-knowledge techniques».
6. ISO/IEC 9798-6:2010  
«Information technology – Security techniques – Entity authentication – Part 6: Mechanisms using manual data transfer».
7. ISO/IEC FDIS 29115  
«Information technology – Security techniques – Entity authentication assurance framework».
8. ISO/IEC 29191:2012  
«Information technology – Security techniques – Requirements for partially anonymous, partially unlink able authentication».

#### **VI. Алгоритми генерації та тестування послідовностей випадкових чисел**

1. ISO/IEC 18031:2011  
«Information technology – Security techniques – Random bit generation».
2. ISO/IEC 18032:2005  
«Information technology – Security techniques – Prime number generation».

#### **VII. Механізми неспростовності**

1. ISO/IEC 13888-1:2009  
«Information technology – Security techniques – Non-repudiation – Part 1: General».
2. ISO/IEC 13888-2:2010  
«Information technology – Security techniques – Non-repudiation – Part 2: Mechanisms using symmetric techniques».
3. ISO/IEC 13888-3:2009  
«Information technology – Security techniques – Non-repudiation – Part 3:

Mechanisms using asymmetric techniques».

### **VIII. Методи шифрування**

1. ISO/IEC 10116:2006  
«Information technology – Security techniques – Modes of operation for an n-bit block cipher».
2. ISO/IEC 18033-1:2005  
«Information technology – Security techniques – Encryption algorithms – Part 1: General».
3. ISO/IEC 18033-2:2006  
«Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers».
4. ISO/IEC 18033-3:2010  
«Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers».
5. ISO/IEC 18033-4:2011  
«Information technology – Security techniques – Encryption algorithms – Part 4: Stream ciphers».

### **IX. Вимоги до криптомодулів**

1. ISO/IEC 19790:2012  
«Information technology – Security techniques – Security requirements for cryptographic modules».
2. ISO/IEC DIS 24759  
«Information technology – Security techniques – Test requirements for cryptographic modules».

### **X. Механізми приватності**

1. ISO/IEC 29100:2011  
«Information technology – Security techniques – Privacy framework».

### **XI. Методи та механізми захисту від несанкціонованого доступу**

1. ISO/IEC 15408-1:2009  
«Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model».
2. ISO/IEC 15408-2:2008  
«Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components».
3. ISO/IEC 15408-3:2008  
«Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components».
4. ISO/IEC TR 15446:2009  
«Information technology – Security techniques – Guide for the production of Protection Profiles and Security Targets».
5. ISO/IEC 18045:2008  
«Information technology – Security techniques – Methodology for IT security evaluation».
6. ISO/IEC TR 19791:2010  
«Information technology – Security techniques – Security assessment of

operational systems».

## **XII. Стандартизація у сфері біометрики**

1. ISO/IEC 19792:2009  
«Information technology – Security techniques – Security evaluation of biometrics».
2. ISO/IEC 24745:2011  
«Information technology – Security techniques – Biometric information protection».
3. ISO/IEC 24761:2009  
«Information technology – Security techniques – Authentication context for biometrics».

## **XIII. Стандарти CWA**

1. CWA 14167-1:2003  
«Security Requirements for Trust worthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements».
2. CWA 14167-2:2004  
«Cryptographic module for CSP signing operations with backup – Protection profile – CMCSOB PP».
3. CWA 14167-4:2004  
«Cryptographic module for CSP signing operations – Protection profile – CMCSO PP».
4. CWA 14169:2004  
«Secure signature-creation devices «EAL 4+».
5. CWA 16093:2010  
«Feasibility Study for a Global eBusiness Interoperability Test Bed (GTIB)».
6. CWA 16022:2009  
«Project Schedule and Cost Performance Management (PSCPM)».
7. CWA 15994:2009  
«eTendering Process)».
8. CWA 15666:2007  
«Business Requirements Specification, Cross industry e-Tendering process».
9. CWA 15667:2007  
«Business Requirements Specification, Cross industry Catalogue Process».
10. CWA 15668:2007  
«Business Requirements Specification, Cross industry Invoicing Process».
11. CWA 15669-1:2007  
«Business requirements specification – Cross industry ordering process – Part 1: Global ordering process model definition».
12. CWA 15669-2:2007  
«Business requirements specification – Cross industry ordering process – Part 2: Order transaction».
13. CWA 15669-3:2007  
«Business requirements specification – Cross industry ordering process – Part 3: Order change transaction».
14. CWA 15669-4:2007



- «Business requirements specification – Cross industry ordering process – Part 4: Order response transaction».
15. CWA 15670:2007  
«Business Requirements Specification, Cross industry Remittance Advice Process».
  16. CWA 15671:2007  
«Business Requirements Specification, Cross industry Scheduling Process».
  17. CWA 15672:2007  
«Business Requirements Specification, Cross industry Despatch and Receive Process».
  18. CWA 15066:2004  
«SAD Transit Declaration – Implementation Model».
  19. CWA 15065:2004  
«SAD Exports Declaration – Implementation Model».
  20. CWA 15672:2007  
«Business Requirements Specification, Cross industry Despatch and Receive Process».
  21. CWA 15066:2004  
«SAD Transit Declaration – Implementation Model».
  22. CWA 15065:2004  
«SAD Exports Declaration – Implementation Model».
  23. CWA 15064:2004  
«SAD Imports Declaration – Implementation Model».
  24. CWA 14729-1:2003  
«The Intrastat System – Part 1: The Implementation Model».
  25. CWA 14729-3:2003  
«The Intrastat System – Part 3: Message Implementation Guideline of INSRES/XML».

#### **XIV. Стандарты ETSI**

1. ETSI TS 101 456:2005  
«Electronic Signatures and Infrastructures (ESI). Policy Requirements for certification authorities issuing qualified certificates».
2. ETSI TR 102 437:2006  
«Electronic Signatures and Infrastructures (ESI); Guidance on TS 101 456 (Policy Requirements for certification authorities issuing qualified certificates)».
3. ETSI TS 102 778:2009  
«Electronic Signatures and Infrastructures (ESI). – PDF Advanced Electronic Signature Profiles; CMS Profile based on ISO 32000-1».
4. ETSI TS 102 778-1:2009  
«Electronic Signatures and Infrastructures (ESI). – PDF Advanced Electronic Signature Profiles. – Part 1: PAdES Overview – a framework document for PAdES».
5. ETSI TS 102 778-2:2009  
«Electronic Signatures and Infrastructures (ESI) – PDF Advanced Electronic

- Signature Profiles – Part 2: PAdES Basic – Profile based on ISO 32000-1».
6. ETSI TS 102 778-3:2009  
«Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced – PadES-BES and PAdES-EPES Profiles».
  7. ETSI TS 102 778-4:2009  
«Electronic Signatures and Infrastructures (ESI) – PDF Advanced Electronic Signature Profiles – Part 4: PAdES Long Term – PadES LTV Profile».
  8. ETSI TS 102 778-5:2009  
«Electronic Signatures and Infrastructures (ESI) – PDF Advanced Electronic Signature Profiles – Part 5: PAdES for XML Content – Profiles for XAdES signatures».
  9. ETSI TS 102 231:2006  
«Electronic Signatures and Infrastructures (ESI) – Provision of harmonized Trust-service status information».
  10. ETSI TR 102 272:2003  
«Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies».
  11. ETSI TR 102 158:2003  
«Electronic Signatures and Infrastructures (ESI); Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates».

#### **XV. Рекомендації RFC**

1. RFC 3739 Internet X.509  
«Public Key Infrastructure: Qualified Certificates Profile».
2. RFC 4510  
«Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map».
3. RFC 4511  
«Lightweight Directory Access Protocol (LDAP): The Protocol»
4. RFC 4512  
«Lightweight Directory Access Protocol (LDAP): Directory Information Models».
5. RFC 4513  
«Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms».
6. RFC 4514  
«Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names».
7. RFC 4515  
«Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters».
8. RFC 4516  
«Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator».

9. RFC 4517  
«Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules».
10. RFC 4518  
«Lightweight Directory Access Protocol (LDAP): Internationalized String Preparation».
11. RFC 4519  
«Lightweight Directory Access Protocol (LDAP): Schema for User Applications».
12. RFC 4523  
«Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates».
13. RFC 4211  
Internet X.509 «Public Key Infrastructure Certificate Request Message Format (CRMF)».
14. RFC 5652  
«Cryptographic Message Syntax (CMS)».
15. RFC 2560  
«Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP».
16. RFC 2631  
«Diffie-Hellman Key Agreement Method», June 1999».
17. RFC 3161  
«Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)».
18. RFC 3370  
«Cryptographic Message Syntax (CMS) Algorithms», August 2002».
19. RFC 3852  
«Cryptographic Message Syntax (CMS)», July 2004».

#### **XVI. Рекомендації PKCS**

1. PKCS #5  
«Password-Based Cryptography Standard».
2. PKCS #8  
«Private-Key Information Syntax Standard».
3. PKCS #10  
«Certification Request Syntax Specification».
4. PKCS #11  
«Cryptographic Token Interface (Cryptoki)».
5. PKCS #12  
«Personal Information Exchange Syntax Standard»
6. PKCS #15  
«Cryptographic Token Information Format Standard».
7. W3C  
Recommendation 10 June 2008 XML «Signature Syntax and Processing (Second Edition)».

**XVII. Управління інформаційною безпекою**

1. ISO/IEC 27000: 2013  
«Information technology – Security techniques – Information security management systems – Overview and vocabulary».
2. ISO/IEC 27001: 2013  
«Information technology – Security techniques – Information security management systems – Requirements».
3. ISO/IEC 27002: 2013  
«Information technology – Security techniques – Code of practice for information security controls».
4. ITAF, 3d Edition  
«A Professional Practices Framework for IS Audit/Assurance».
5. ISO/IEC 27005: 2011  
«Information technology – Security techniques – Information security risk management».
6. ISO/IEC 27006:2007  
«Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems».
7. ISO/IEC 27007:2011  
«Information technology – Security techniques – Guidelines for information security management systems auditing».
8. ISO/IEC TR 27008:2011  
«Information technology – Security techniques – Guidelines for auditors on information security management systems controls».
9. ISO/IEC 27010: 2012  
«Information technology – Security techniques – Information security management for inter-sector and inter-organizational communications».
10. ISO/IEC 27031: 2011  
«Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity».
11. ISO/IEC 27033-1: 2009  
«Information technology – Security techniques – Network security – Part 1: Overview and concepts».
12. ISO/IEC 27033-2: 2012  
«Information technology – Security techniques – Network security – Part 2: Guidelines for the design and implementation of network security».
13. ISO/IEC 27033-3: 2010  
«Information technology – Security techniques – Network security – Part 3: Reference networking scenarios – Threats, design techniques and control issues».
14. ISO/IEC 27033-4: 2013  
Information technology – Security techniques – Network security – Part 4: Securing communications between networks using security gateways
15. ISO/IEC 27033-5: 2013

«Information technology – Security techniques – Network security – Part 5: Securing communications across networks using Virtual Private Network (VPNs)».

16. ISO/IEC27035: 2011

«Information technology – Security techniques – Information security incident management».

**Начальник Управління  
функціонування центрального  
засвідчувального органу  
Міністерства юстиції України**

**О.В. Костенко**

**Директор Департаменту криптографічного  
захисту інформації Адміністрації  
Державної служби спеціального зв'язку  
та захисту інформації України**

**А.І. Пушкарьов**