ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України
\_\_ \_\_\_\_\_\_\_\_\_\_ 20\_\_ року № \_\_\_\_\_

ПЕРЕЛІК
стандартів та технічних специфікацій,
дозволених для реалізації в засобах криптографічного захисту інформації

**І. Стандарти, що визначають вимоги до блокових шифрів (block ciphers)**

1. ДСТУ 7624:2014 “Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення”.

2. ДСТУ ISO/IEC 18033-3:2015 (ISO/IEC 18033-3:2010, IDT) “Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 3. Блокові шифри”.

3. ДСТУ ГОСТ 28147:2009 “Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования”.

4. ДСТУ ISO/IEC 10116:2019 (ISO/IEC 10116:2017, IDT) “Інформаційні технології. Методи захисту. Режими роботи n-бітних блокових шифрів”.

**ІІ. Стандарти, що визначають вимоги до потокових шифрів (stream ciphers)**

1. ДСТУ 8845:2019 “Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення”.

2. ДСТУ ISO/IEC 18033-4:2015 (ISO/IEC 18033-4:2011, IDT) “Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 4. Потокові шифри”.

**ІІІ. Стандарти, що визначають вимоги до асиметричних криптографічних алгоритмів та методів (asymmetric algorithms and techniques**)

1. ДСТУ 4145-2002 “Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння”.

2. ДСТУ ISO/IEC 9796-2:2015 (ISO/IEC 9796-2:2010, IDT) “Інформаційні технології. Методи захисту. Схеми цифрового підпису, які забезпечують відновлення повідомлення. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел”.

3. ДСТУ ISO/IEC 9796-3:2015 (ISO/IEC9796-3:2006, IDT) “Інформаційні технології. Методи захисту. Схеми цифрового підпису, які забезпечують відновлення повідомлення. Частина 3. Механізми, що ґрунтуються на дискретному логарифмі”.

4. ДСТУ ISO/IEC 14888-2:2015 (ISO/IEC 14888-2:2008, IDT) “Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел”.

5. ДСТУ ISO/IEC 14888-3:2019 (ISO/IEC 14888-3:2018, IDT) “Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми, що ґрунтуються на дискретному логарифмуванні”.

6. ДСТУ ISO/IEC 15946-5:2019 (ISO/IEC 15946-5:2017) “Інформаційні технології. Методи захисту. Криптографічні методи на основі еліптичних кривих. Частина 5. Генерування еліптичних кривих”.

7. ДСТУ ISO/IEC 18033-2:2015 (ISO/IEC 18033-2:2006, IDT) “Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 2. Асиметричні шифри”.

**IV. Стандарт, що визначає вимоги до кодів автентифікації повідомлень (message authentication codes)**

ДСТУ ISO/IEC 9797-2:2015 (ISO/IEC 9797-2:2011, IDT) “Інформаційні технології. Методи захисту. Коди автентифікації повідомлень (MACs). Частина 2. Механізми що використовують спеціалізовану геш-функцію”.

**V. Стандарти, що визначають вимоги до геш-функцій (hash functions)**

1. ДСТУ 7564:2014 “Інформаційні технології. Криптографічний захист інформації. Функція ґешування”.

2. ДСТУ ISO/IEC 10118-2:2015 (ISO/IEC 10118-2:2010; Cor 1:2011, IDT) “Інформаційні технології. Методи захисту. Геш-функції. Частина 2. Геш-функції, що використовують n-бітний блоковий шифр”.

3. ДСТУ ISO/IEC 10118-3:2005 (ISO/IEC 10118-3:2004; Cor 1:2011, IDT) “Інформаційні технології. Методи захисту. Геш-функції. Частина 3. Спеціалізовані геш-функції”.

4. ДСТУ ISO/IEC 10118-4:2015 (ISO/IEC 10118-4:1998; Cor 1:2014; Amd 1:2014, IDT) “Інформаційні технології. Методи захисту. Геш-функції. Частина 4. Геш-функції, що використовують модульну арифметику”.

5. ГОСТ 34.311-95 “Информационная технология. Криптографическая защита информации. Функция хэширования”.

**VІ. Стандарти, що визначають вимоги до автентифікації сутності
(entity authentication)**

1. ДСТУ ISO/IEC 9798-2:2015 (ISO/IEC 9798-2:2008; Cor 3:2013, IDT) “Інформаційні технології. Методи захисту. Автентифікація об’єктів. Частина 2. Механізми, що використовують симетричні алгоритми шифрування”.

2. ДСТУ ISO/IEC 9798-3:2002 (ISO/IEC 9798-3:1998; Cor 1:2009; Cor 2:2012) “Інформаційні технології. Методи захисту. Автентифікація суб’єктів. Частина 3. Механізми з використанням методу цифрового підпису”.

3. ДСТУ ISO/IEC 9798-4:2015 (ISO/IEC 9798-4:1999; Cor 1:2009; Cor 2:2012, IDT) “Інформаційні технології. Методи захисту. Автентифікація об’єктів. Частина 4. Методи, що використовують криптографічну перевірочну функцію”.

4. ДСТУ ISO/IEC 9798-5:2015 (ISO/IEC 9798-5:2009, IDT) “Інформаційні технології. Методи захисту. Автентифікація об’єктів. Частина 5. Механізми, що використовують методи нульової обізнаності”.

5. ДСТУ ISO/IEC 9798-6:2015 (ISO/IEC 9798-6:2010, IDT) “Інформаційні технології. Методи захисту. Автентифікація об’єктів. Частина 6. Механізми, що використовують ручне передавання даних”.

**VІІ. Стандарти, що визначають вимоги до управління ключами
(key management)**

1. ДСТУ ISO/IEC 11770-2:2015 (ISO/IEC 11770-2:2008; Cor 1:2009, IDT) “Інформаційні технології. Методи захисту. Керування ключами. Частина 2. Механізми з використанням симетричних методів”.

2. ДСТУ ISO/IEC 11770-3:2015 (ISO/IEC 11770-3:2008; Cor 1:2009, IDT) “Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми з використанням асиметричних методів”.

3. ДСТУ ISO/IEC 11770-4:2015 (ISO/IEC 11770-4:2008; Cor 1:2009, IDT) “Інформаційні технології. Методи захисту. Керування ключами. Частина 4. Механізми , засновані на нестійких секретах”.

4. ДСТУ ISO/IEC 11770-5:2015 (ISO/IEC 11770-5:2008, IDT) “Інформаційні технології. Методи захисту. Керування ключами. Частина 5. Керування груповими ключами”.

**VІІІ. Стандарти, що визначають вимоги до випадкової генерації біт (random bit generation)**

1. ДСТУ ISO/IEC 18031:2015 (ISO/IEC 18031:2011; Cor 1:2014, IDT) “Інформаційні технології. Методи захисту. Генерування випадкових бітів”.

2. ДСТУ ISO/IEC 20543 “Інформаційні технології. Методи захисту. Методи тестування та аналізу для генерування випадкових бітів”.

**ІХ. Стандарти, що визначають вимоги до методів встановлення чутливих параметрів безпеки (sensitive security parameter establishment methods)**

1. ДСТУ ISO/IEC 11770-2:2015 (ISO/IEC 11770-2:2008; Cor 1:2009, IDT) “Інформаційні технології. Методи захисту. Керування ключами. Частина 2. Механізми з використанням симетричних методів”.

2. ДСТУ ISO/IEC 11770-3:2015 (ISO/IEC 11770-3:2008; Cor 1:2009, IDT) “Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми з використанням асиметричних методів”.

**Х. Стандарти, що визначають вимоги до тестових метрик пом’якшення неінвазійних атак (non-invasive attack mitigation test metrics)**

1. ДСТУ ISO/IEC 20085-1 “Методи захисту ІТ. Вимоги до засобів тестування та методів калібрування засобів тестування для застосування у методах тестування пом’якшення неінвазійних атак на криптографічні модулі. Частина 1. Методи та засоби тестування”.

2.ДСТУ ISO/IEC 20085-2 “Методи захисту ІТ. Вимоги до засобів тестування та методів калібрування засобів тестування для застосування у методах тестування пом’якшення неінвазійних атак на криптографічні модулі. Частина 2. Методи та прилади тестового калібрування”.

**ХІ. Стандарти та технічні специфікації, що визначають вимоги до форматів криптографічних повідомлень**

RFC 5652 “Cryptographic Message Syntax (CMS)” з використання криптографічних алгоритмів згідно з RFC 3370 “Cryptographic Message Syntax (CMS) Algorithms” або Технічних специфікацій до RFC 5652, затверджених наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від \_\_\_\_\_\_ № \_\_\_ «Про затвердження переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації», зареєстрованим в Міністерстві юстиції України \_\_\_\_\_\_ за № \_\_\_.

Т.в.о. директора Департаменту захисту інформації

Адміністрації Державної служби спеціального

зв’язку та захисту інформації України

полковник Ігор СТЕЛЬНИК