ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України 27 жовтня 2020 року № 687

(у редакції наказу Адміністрації Державної служби спеціального зв’язку та захисту інформації України
від _____ № _____)

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

I. 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/Amd 1:2021, IDT) «Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 3. Блокові шифри»

ДСТУ ISO/IEC 18033-3:2015 (ISO/IEC 18033-3:2010, IDT)/Зміна № 1:2023 (ISO/IEC 18033-3:2010/Amd 1:2021, 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/Amd 1:2021, IDT) «Інформаційні технології. Методи захисту. Режими роботи n-бітних блокових шифрів»

ДСТУ ISO/IEC 10116:2019 (ISO/IEC 10116:2017, IDT)/Зміна № 1:2023 (ISO/IEC 10116:2017/Amd 1:2021, IDT) «Інформаційні технології. Методи захисту. Режими роботи n-бітних блокових шифрів»

5. ДСТУ ISO/IEC 18033-7:2023 (ISO/IEC 18033-7:2022, IDT) Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 7. Настроювані блокові шифри»

6. ДСТУ ISO/IEC 19772:2022 (ISO/IEC 19772:2020, IDT) «Інформаційна безпека. Автентифіковане шифрування»

II. 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/Amd 1:2020, IDT) «Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 4. Потокові шифри»

ДСТУ ISO/IEC 18033-4:2015 (ISO/IEC 18033-4:2011, IDT)/Зміна № 1:2023 (ISO/IEC 18033-4:2011/Amd 1:2020, IDT) «Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 4. Потокові шифри»

III. 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/IEC 9796-3:2006, 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/Cor 1:2015, IDT) «Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел»

ДСТУ ISO/IEC 14888-2:2015 (ISO/IEC 14888-2:2008, IDT)/Поправка № 1:2023 (ISO/IEC 14888-2:2008/Cor 1:2015, 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 15946-5:2023 (ISO/IEC 15946-5:2022, IDT) «Інформаційні технології. 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»

ДСТУ ISO/IEC 18033-2:2015 (ISO/IEC 18033-2:2006, IDT)/Зміна № 1:2023 (ISO/IEC 18033-2:2006/Amd 1:2017, IDT) «Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 2. Асиметричні шифри»

8. ДСТУ ISO/IEC 13888-3:2023 (ISO/IEC 13888-3:2020, IDT) «Інформаційні технології. Неспростовність. Частина 3. Механізми із застосуванням асиметричних методів»

9. ДСТУ ISO/IEC 18033-5:2017 (ISO/IEC 18033-5:2015, IDT) «Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 5. Шифри, що ґрунтуються на ідентифікаційних даних»

ДСТУ ISO/IEC 18033-5:2017/Зміна № 1:2023 (ISO/IEC 18033-5:2015/Amd 1:2021, IDT) «Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 5. Шифри, що ґрунтуються на ідентифікаційних даних»

10. ДСТУ ETSI TR 103 616:2022 (ETSI TR 103 616 V1.1.1 (2021–09), IDT) «Кібербезпека. Квантово-безпечні підписи»

11. ДСТУ ETSI TR 103 823:2022 (ETSI TR 103 823 V1.1.2 (2021–10), IDT) «Кібербезпека. Квантово-безпечне шифрування з відкритим ключем та інкапсуляція ключів»

12. ДСТУ ISO/IEC 18033-6:2022 (ISO/IEC 18033-6:2019, IDT) «Інформаційні технології. Методи убезпечення. Алгоритми шифрування. Частина 6. Гомоморфне шифрування» (з обмеженнями у застосуванні).

Алгоритм визначений пунктом 6.2 ДСТУ ISO/IEC 18033-6:2022 не рекомендується до застосування.

13. ДСТУ 8961:2019 «Інформаційні технології. Криптографічний захист інформації. Алгоритми асиметричного шифрування та інкапсуляції ключів»

14. ДСТУ 9041:2020 «Інформаційні технології. Криптографічний захист інформації. Алгоритм шифрування коротких повідомлень, що ґрунтується на скручених еліптичних кривих Едвардса»

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

ДСТУ ISO/IEC 9797-2:2023 (ISO/IEC 9797-2:2021, IDT) «Інформаційні технології. Коди автентифікації повідомлень (MACs). Частина 2. Механізми, що застосовують спеціальну 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 10118-3:2023 (ISO/IEC 10118-3:2018, 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), 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»

6. ДСТУ ISO/IEC 9797-3:2015 (ISO/IEC 9797-3:2011, IDT) «Інформаційні технології. Методи захисту. Коди автентифікації повідомлень (MACs). Частина 3. Механізми, що використовують універсальну геш-функцію»

ДСТУ ISO/IEC 9797-3:2015 (ISO/IEC 9797-3:2011, IDT)/Зміна № 1:2023 (ISO/IEC 9797-3:2011/Amd1:2020, IDT) «Інформаційні технології. Методи захисту. Коди автентифікації повідомлень (MACs). Частина 3. Механізми, що використовують універсальну геш-функцію»

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

1. ДСТУ ISO/IEC 9798-2:2021 (ISO/IEC 9798-2:2019, IDT) «Інформаційні технології. Методи безпеки IT. Автентифікація об’єктів. Частина 2. Механізми, що використовують автентифіковане шифрування»

2. ДСТУ ISO/IEC 9798-3:2021 (ISO/IEC 9798-3:2019, IDT) «Інформаційні технології. Методи безпеки ІТ. Автентифікація об’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»

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

1. ДСТУ ISO/IEC 11770-2:2019 (ISO/IEC 11770-2:2018, IDT) «Інформаційні технології. Методи захисту. Керування ключами. Частина 2. Механізми із застосуванням симетричних методів»

2. ДСТУ ISO/IEC 11770-3:2023 (ISO/IEC 11770-3:2021, IDT) «Інформаційні технології. Керування ключами. Частина 3. Механізми із застосуванням асиметричних методів»

3. ДСТУ ISO/IEC 11770-4:2019 (ISO/IEC 11770-4:2017, IDT) «Інформаційні технології. Методи захисту. Керування ключами. Частина 4. Механізми, ґрунтовані на нестійких секретах»

ДСТУ ISO/IEC 11770-4:2019 (ISO/IEC 11770-4:2017, IDT)/Зміна № 1:2023 (ISO/IEC 11770-4:2017/Amd 1:2019, IDT) «Інформаційні технології. Методи захисту. Керування ключами. Частина 4. Механізми, ґрунтовані на нестійких секретах»

ДСТУ ISO/IEC 11770-4:2019 (ISO/IEC 11770-4:2017, IDT)/Зміна № 2:2023 (ISO/IEC 11770-4:2017/Amd 2:2021, IDT) «Інформаційні технології. Методи захисту. Керування ключами. Частина 4. Механізми, ґрунтовані на нестійких секретах»

4. ДСТУ ISO/IEC 11770-5:2023 (ISO/IEC 11770-5:2020, IDT) «Інформаційні технології. Керування ключами. Частина 5. Керування груповими ключами»

5. ДСТУ ISO/IEC 11770-6:2018 (ISO/IEC 11770-6:2016, IDT) «Інформаційні технології. Методи захисту. Керування ключами. Частина 6. Утворення ключів»

6. ДСТУ ISO/IEC 11770-7:2023 (ISO/IEC 11770-7:2021, IDT) «Інформаційні технології. Керування ключами. Частина 7. Міждоменний автентифікований обмін ключами на основі пароля»

7. ДСТУ 8961:2019 «Інформаційні технології. Криптографічний захист інформації. Алгоритми асиметричного шифрування та інкапсуляції ключів»

8. ДСТУ ETSI TR 103 823:2022 (ETSI TR 103 823 V1.1.2 (2021–10), IDT) «Кібербезпека. Квантово-безпечне шифрування з відкритим ключем та інкапсуляція ключів»

9. ДСТУ ETSI TR 103 570:2022 (ETSI TR 103 570 V1.1.1 (2017–10), IDT) «Кібербезпека. Квантово-безпечний обмін ключами»

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

1. ДСТУ ISO/IEC 18031:2015 (ISO/IEC 18031:2011; Cor 1:2014, Amd 1:2017, IDT) «Інформаційні технології. Методи захисту. Генерування випадкових бітів»

ДСТУ ISO/IEC 18031:2015 (ISO/IEC 18031:2011; Cor 1:2014, IDT)/Зміна № 1:2023 (ISO/IEC 18031:2011/Amd 1:2017, IDT) «Інформаційні технології. Методи захисту. Генерування випадкових бітів»

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

1. ДСТУ ISO/IEC 11770-2:2019 (ISO/IEC 11770-2:2018, IDT) «Інформаційні технології. Методи захисту. Керування ключами. Частина 2. Механізми із застосуванням симетричних методів»

2. ДСТУ ISO/IEC 11770-3:2023 (ISO/IEC 11770-3:2021, IDT) «Інформаційні технології. Керування ключами. Частина 3. Механізми із застосуванням асиметричних методів»

3. ДСТУ ISO/IEC 18032:2022 (ISO/IEC 18032:2020, IDT) «Інформаційні технології. Методи захисту. Генерування простого числа»

X. 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

Директор Департаменту захисту інформації
Адміністрації Державної служби спеціального
зв’язку та захисту інформації України
полковник Ігор СТЕЛЬНИК