НАЦІОНАЛЬНИЙ ОРГАН СТАНДАРТИЗАЦІЇ

ДЕРЖАВНЕ ПІДПРИЄМСТВО
«УКРАЇНСЬКИЙ НАУКОВО-ДОСЛІДНИЙ
І НАВЧАЛЬНИЙ ЦЕНТР ПРОБЛЕМ СТАНДАРТИЗАЦІЇ,
СЕРТИФІКАЦІЇ ТА ЯКОСТІ»
(ДП «УкрНДНЦ»)

Н А К А З

від 15 червня 2023 р. Київ № 135

Про прийняття національних
стандартів, змін, поправки до них
та скасування національних стандартів

Відповідно до пункту 2 частини 2 статті 11 Закону України «Про стандартизацію», розпорядження Кабінету Міністрів України від 26.11.2014 № 1163 «Про визначення державного підприємства, яке виконує функції національного органу стандартизації» та на виконання Програми робіт з національної стандартизації, відповідно до протоколу ТК 20 «Інформаційні технології» від 28.03.2023 № 2

НАКАЗУЮ:

1. Прийняти національні стандарти, гармонізовані з європейським та міжнародними стандартами, методом підтвердження з наданням чинності **з 25 червня 2023 року:**

1.	ДСТУ EN 17640:2023 (EN 17640:2022, IDT)	Методологія оцінювання кібербезпеки з фіксованим часом для продуктів ІКТ — Вперше
2.	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 — На заміну ДСТУ ISO/IEC 9797-2:2015 (ISO/IEC 9797-2:2011, IDT)
3.	ДСТУ ISO/IEC 10118-3:2023 (ISO/IEC 10118-3:2018, IDT)	Інформаційні технології. Методи захисту. Геш-функції. Частина 3. Спеціалізовані геш-функції — На заміну ДСТУ ISO/IEC 10118-3:2005

4.	ДСТУ ISO/IEC 11770-3:2023 (ISO/IEC 11770-3:2021, IDT)	Інформаційні технології. Керування ключами. Частина 3. Механізми із застосуванням асиметричних методів — На заміну ДСТУ ISO/IEC 11770-3:2015 (ISO/IEC 11770-3:2008; Cor 1:2009, IDT)
5.	ДСТУ ISO/IEC 11770-5:2023 (ISO/IEC 11770-5:2020, IDT)	Інформаційні технології. Керування ключами. Частина 5. Керування груповими ключами — На заміну ДСТУ ISO/IEC 11770-5:2015 (ISO/IEC 11770-5:2008, IDT)
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 — Вперше
7.	ДСТУ ISO/IEC 13888-3:2023 (ISO/IEC 13888-3:2020, IDT)	Інформаційні технології. Неспростовність. Частина 3. Механізми із застосуванням асиметричних методів — На заміну ДСТУ ISO/IEC 13888-3:2015 (ISO/IEC 13888-3:2009, IDT)
8.	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 — На заміну ДСТУ ISO/IEC 15946-5:2019 (ISO/IEC 15946-5:2017, IDT)
9.	ДСТУ ISO/IEC 18033-7:2023 (ISO/IEC 18033-7:2022, IDT)	Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 7. Настроювані блокові шифри — Вперше
10.	ДСТУ ISO/IEC 27102:2023 (ISO/IEC 27102:2019, IDT)	Керування інформаційною безпекою. Настанови щодо кіберстрахування — Вперше
11.	ДСТУ ISO/IEC TR 27550:2023 (ISO/IEC TR 27550:2019, IDT)	Інформаційні технології. Методи захисту. Розроблення конфіденційності для процесів життєвого циклу системи — Вперше

12.	ДСТУ ISO/IEC TS 27110:2023 (ISO/IEC TS 27110:2021, IDT)	Інформаційна безпека, кібербезпека та захист конфіденційності. Настанови щодо розроблення інфраструктури кібербезпеки — Вперше

2. Прийняти зміни до національних стандартів, гармонізованих з міжнародними стандартами, методом підтвердження з наданням чинності
з 25 червня 2023 року:

1.	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
2.	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
3.	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
4.	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
5.	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
6.	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

7.	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
8.	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
9.	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

3. Прийняти поправку до національного стандарту, гармонізовану з міжнародним стандартом, методом підтвердження з наданням чинності **з 25 червня 2023 року:**

1	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

4. Скасувати чинність національних стандартів **з 25 червня 2023 року:**

1.	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
2.	ДСТУ ISO/IEC 10118-3:2005	Інформаційні технології. Методи захисту. Геш-функції. Частина 3. Спеціалізовані геш-функції

3.	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
4.	ДСТУ ISO/IEC 11770-5:2015 (ISO/IEC 11770-5:2008, IDT)	Інформаційні технології. Методи захисту. Керування ключами. Частина 5. Керування груповими ключами
5.	ДСТУ ISO/IEC 13888-3:2015 (ISO/IEC 13888-3:2009, IDT)	Інформаційні технології. Методи захисту. Неспростовність. Частина 3. Механізми з використанням асиметричних методів
6.	ДСТУ ISO/IEC 15946-5:2019 (ISO/IEC 15946-5:2017, IDT)	Інформаційні технології. Методи захисту. Криптографічні методи на основі еліптичних кривих. Частина 5. Генерування еліптичних кривих

5. Начальнику відділу інформаційних технологій Костянтину Шелестюку забезпечити оприлюднення цього наказу на офіційному вебсайті ДП «УкрНДНЦ».

6. Начальнику Національного фонду нормативних документів Людмилі Слепченко забезпечити опублікування цього наказу в черговому виданні щомісячного інформаційного покажчика «Стандарти».

7. Контроль за виконанням цього наказу залишаю за собою.

В. о. генерального директора **Олександр КИР’ЯНОВ**