ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ’ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Законодавство у сфері захисту інформації та кіберзахисту. Сучасні вимоги з його розвитку

Пушкарьов А.І., Мялковський Д.В.

КИЇВ-2017

Державна політика у сфері захисту інформації

- забезпечення функціонування та розвиток системи захисту інформації
- нормативно-правове регулювання у сфері захисту інформації
- технічне регулювання у сфері захисту інформації та підтвердження відповідності засобів захисту інформації встановленим вимогам
- координація діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій у сфері захисту інформації

Державна політика у сфері захисту інформації (продовження)

- координація впровадження і використання криптографічних методів в інфраструктурі відкритих ключів електронного цифрового підпису
- ліцензування у сфері захисту інформації
- забезпечення виконання Україною зобов’язань щодо міжнародних режимів обмеження експорту товарів подвійного використання та військового призначення

Основні напрямки модернізації:

1. Запровадження електронних сервісів:

- електронне підтвердження (фіксація) погодження ТЗ на комплекси ТЗІ та КСЗІ, ТУ, ТВ, ТЗ на засоби ТЗІ та КЗІ, програми та методики експертизи КСЗІ, відповідності (сертифікації, позитивних результатів державної експертизи) засобів ТЗІ та КЗІ, комплексів ТЗІ (на підставі атестації), КСЗІ (у тому числі на підставі декларування), експлуатаційної документації до них
- Забезпечення наповнення та роботи з електронними даними Реєстру (ATripleSL)

Основні напрямки модернізації:

2. Активізація регіональних органів Держспецзв’язку:

- децентралізація та делегування повноважень регіональним органам і територіальним підрозділам Адміністрації Держспецзв’язку щодо реєстрації декларацій про відповідність КСЗІ та результатів атестацій комплексів ТЗІ щодо тих ІТС та об’єктів інформаційної діяльності, які експлуатуються в межах відповідної адміністративно-територіальної одиниці

Основні напрямки модернізації:

3. Типові рішення для КСЗІ:

- розроблення та впровадження керівництв з застосування типових рішень з побудови КСЗІ;
- встановлення порядку та делегування повноважень зі створення КСЗІ на АС класів 1 та 2, а також КСЗІ на об’єктах інформаційної діяльності – органам державної влади, що мають дозволи на виконання відповідних робіт у сфері ТЗІ для власних потреб

Основні напрямки модернізації:

4. Удосконалення роботи служб захисту інформації:

- розроблення та впровадження механізмів та систем управління інформаційною безпекою та ризиками за рівнем не нижче вимог стандартів ISO/IEC 27k, 31k,
- розширення прав, повноважень та відповідальності керівників державних органів та служб захисту інформації;
- відновлення дієвого механізму планування витрат на удосконалення не тільки КТЗІ ДІР, а й заходів з кіберзахисту

Основні напрямки модернізації:

5. Створення та організація функціонування «Реєстру засобів, систем, комплексів та типових рішень у сфері захисту інформації, з підтвердженою відповідністю» (Authority Secure Suits&Solution List, ATripleSL)

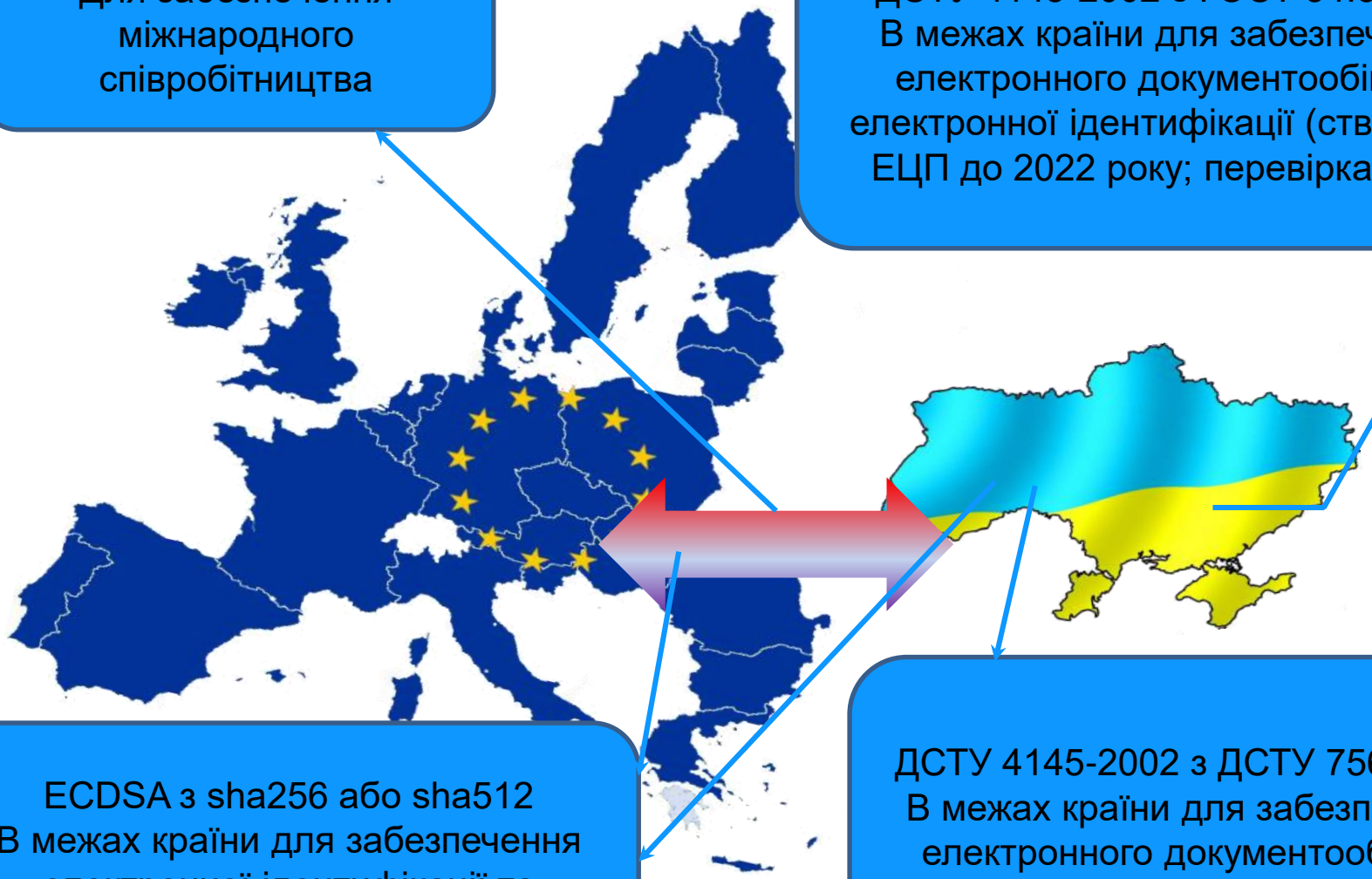
Основні напрямки модернізації:

6. Імплементація стандартів НАТО

Застосування ЕЦП суб’єктами правових відносин, які використовують у своїй діяльності посилені сертифікати відкритих ключів

RSA з sha256
Для забезпечення міжнародного співробітництва

ДСТУ 4145-2002 з ГОСТ 34.311-95
В межах країни для забезпечення електронного документообігу та електронної ідентифікації (створення ЕЦП до 2022 року; перевірка ЕЦП)



ECDSA з sha256 або sha512
В межах країни для забезпечення електронної ідентифікації та міжнародного співробітництва

ДСТУ 4145-2002 з ДСТУ 7564-2014
В межах країни для забезпечення електронного документообігу та електронної ідентифікації

Застосування ЕЦП суб’єктами правових відносин на внутрішньому ринку країни

Сучасний стан

ECDSA з sha256 або sha512

в межах країни для забезпечення електронної ідентифікації та міжнародного співробітництва

ДСТУ 4145-2002 з ДСТУ 7564-2014

в межах країни для забезпечення електронного документообігу та електронної ідентифікації

Перспектива

ECDSA = ДСТУ 4145-2002

для забезпечення електронного документообігу та електронної ідентифікації

Цифрові докази

Доповнення Кримінального процесуального кодексу України наступними положеннями:

- Цифровим доказом є інформація, що зберігається або передається у цифровій (електронній) формі та яка може бути використана як доказ факту чи обставини, що встановлюється під час кримінального провадження.
- Цифрові докази отримані шляхом копіювання (відтворення) та/чи збереження інформації у цифровій формі із застосуванням методів, що дозволяють точно відтворити оригінал та забезпечити їх цілісність і неспростовність, шляхом накладення на них електронного цифрового підпису, визнаються допустимими доказами у кримінальному провадженні.

Дякую за увагу!

dzi@dsszzi.gov.ua