Постанова КМУ №518 «Про затвердження Загальних вимог з кіберзахисту об’єктів критичної інфраструктури» від 19 червня 2019 р. Проблеми впровадження

Бакалинський О.О.

Заступник директора Департаменту формування та реалізації державної політики в сфері кіберзахисту Адміністрації Держспецзв'язку

cyber@dsszzi.gov.ua

Вступ

Ці Вимоги є ***обов'язковими*** до виконання підприємствами, установами та організаціями, які згідно до законодавства віднесені до об'єктів критичної інфраструктури.

Критично важливі об'єкти інфраструктури (далі - *об'єкти критичної інфраструктури*) - підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан *національної безпеки і оборони України*, *навколишнього природного середовища*, заподіяти *майнову шкоду* та/або *становити загрозу для життя і здоров'я людей*.

(***Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII***)

Терміни, які вживаються у Постанові

Кіберзахист - сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем. (***Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII***)

Інші терміни вживаються у значенні, наведеному в Законах України «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-телекомунікаційних системах», Правилах забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених постановою Кабінету Міністрів України від 29.03.2006 № 373, НД ТЗІ 1.1-003-99, ДСТУ ISO/IEC 27000:2015.

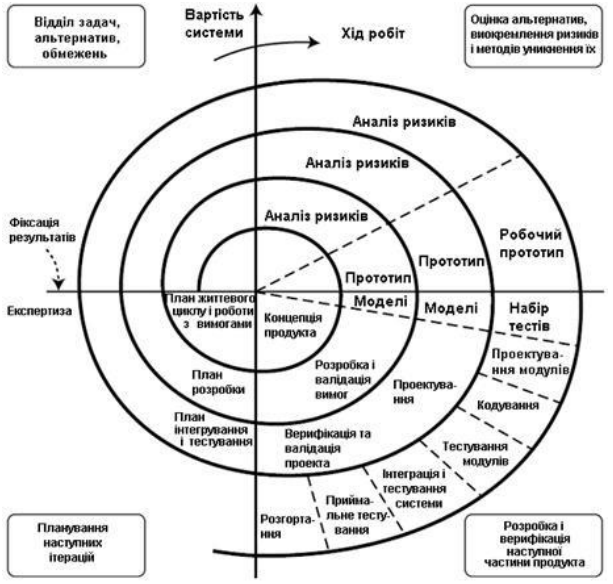
Вперше введено визначення

СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ - сукупність *організаційних* та *технічних* заходів, а також *засобів* і *методів* захисту інформації, які впроваджуються на ОКІІ ОКІ з метою запобігання кіберінцидентам, виявлення та захисту від кібератак, порушення конфіденційності, цілісності та доступності інформаційних ресурсів, що обробляються (передаються, зберігаються) на ОКІІ ОКІ, запобігання порушенню режиму функціонування та/або недоступності служб (функцій) ОКІІ ОКІ, порушенню функціонування компонентів ОКІІ ОКІ; забезпечення спостережності за діями користувачів ОКІІ ОКІ та функціонуванням засобів захисту ОКІІ ОКІ.

Життєвий цикл кіберзахисту ОКІ

Кіберзахист ОКІ є складовою частиною робіт із створення (модернізації) та експлуатації ОКІІ ОКІ. Заходи з кіберзахисту передбачаються та впроваджуються на всіх стадіях життєвого циклу ОКІІ ОКІ.

Кіберзахист ОКІ забезпечується власником та/або керівником ОКІ відповідно до цих Загальних вимог та законодавства в сфері захисту інформації та кібербезпеки.



В ОКІІ обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом

- Створюється (модернізується) КСЗІ + застосуються Загальні вимоги.
- Перевірка відповідності - державна експертиза в сфері ТЗІ.

+

- Будується відповідно до вимог законодавства в сфері захисту інформації.
- ТЗ КСЗІ ОКІІ - погоджується з Адміністрацією Держспецзв’язку України.

- Засоби захисту інформації - підтверджена відповідність, якщо ні - оцінювання проводиться під час її державної експертизи КСЗІ ОКІІ в сфері ТЗІ.

В ОКІІ не обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом

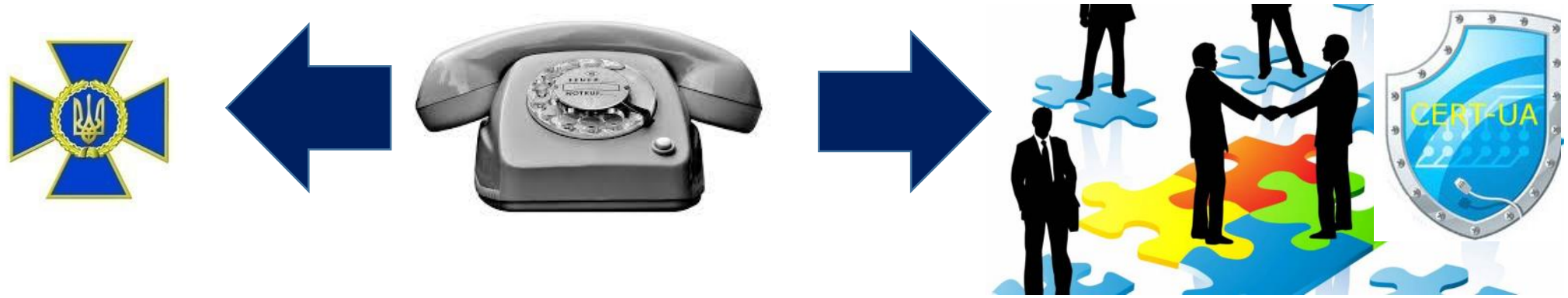
- Створюється (модернізується) система інформаційної безпеки ОКІ.
- Відповідність перевіряється під час незалежного аудиту інформаційної безпеки ОКІІ.

+

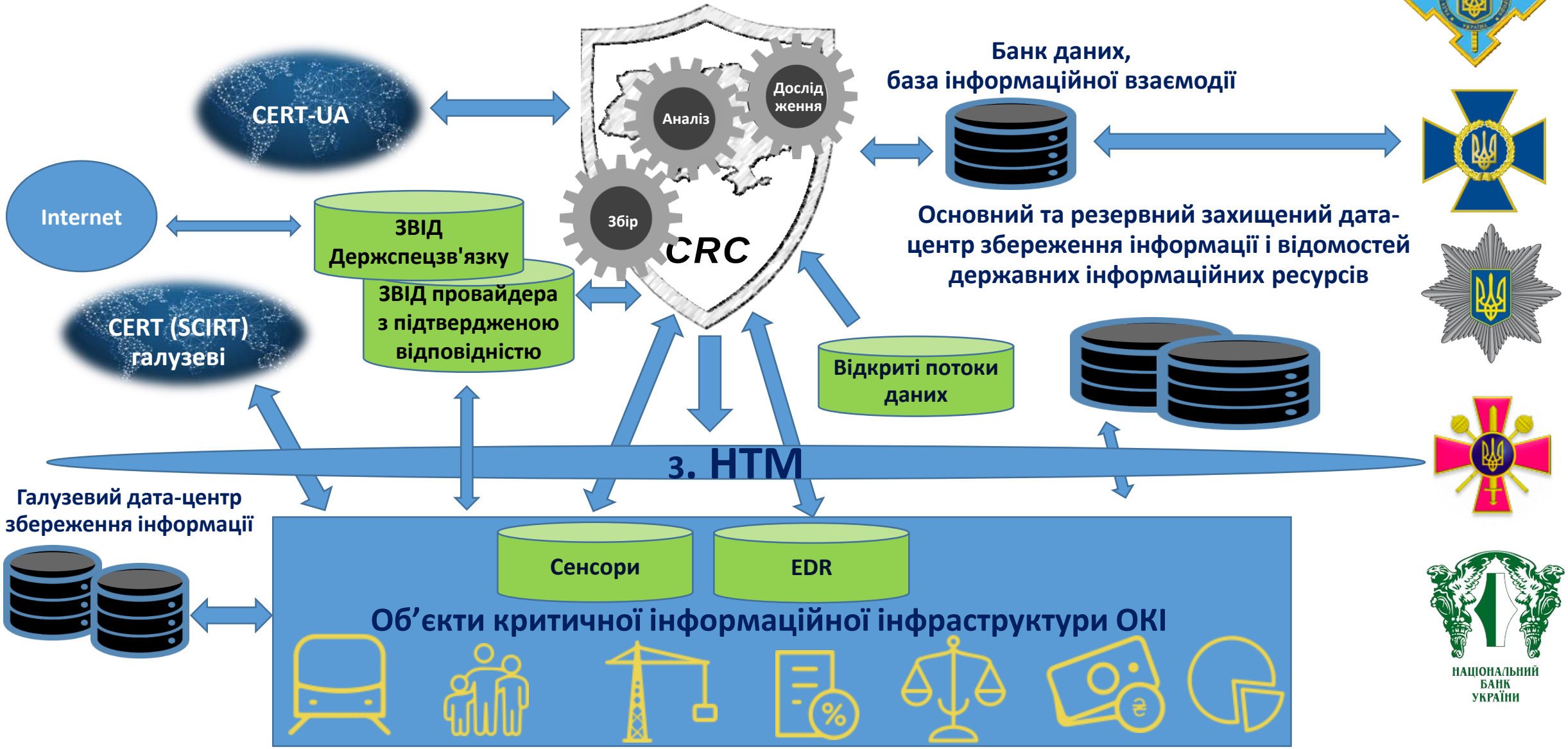
- Створення СІБ ОКІІ здійснюється відповідно до вимог ТЗ.
- ТЗ формується за результатами оцінки загроз інформації та **ризиків**, які викладаються в Звіті. Методична основа - стандарт ДСТУ ISO/IEC 27005.
- ТЗ СІБ - погоджується з Адміністрацією Держспецзв’язку України.
- Незалежний аудит ІБ на ОКІ організовує власник та/або керівник ОКІ, порядок аудиту визначає КМУ.

Інформування та взаємозв'язок

Власник та/або керівник ОКІ організовує невідкладне інформування урядової команди реагування на комп’ютерні надзвичайні події України **CERT-UA** (у разі наявності - галузевої команди реагування на комп’ютерні надзвичайні події), а також функціонального підрозділу контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Центрального управління СБУ (**Ситуаційний центр забезпечення кібербезпеки СБУ**) або відповідного підрозділу регіонального органу СБУ про кіберінциденти та кібератаки, які стосуються його ОКІІ ОКІ.

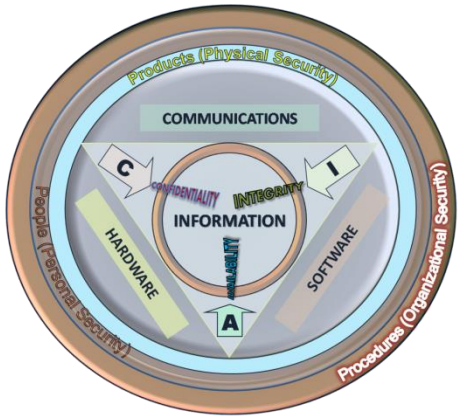


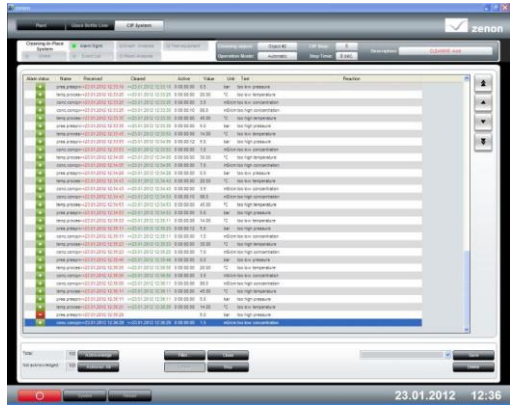
Загальні вимоги та можливості Центру реагування на кіберзагрози Держспецзв’язку, взаємозв'язок



Організаційні та технічні заходи з кіберзахисту, які впроваджуються в ОКІІ, повинні забезпечувати:

- визначення в ОКІ загальної політики інформаційної безпеки;
- визначення суб’єктів доступу до об’єктів захисту ОКІІ;
- ідентифікацію та автентифікацію суб’єктів доступу та об’єктів захисту ОКІІ;
- реєстрацію подій компонентами ОКІІ та їх періодичний аудит;





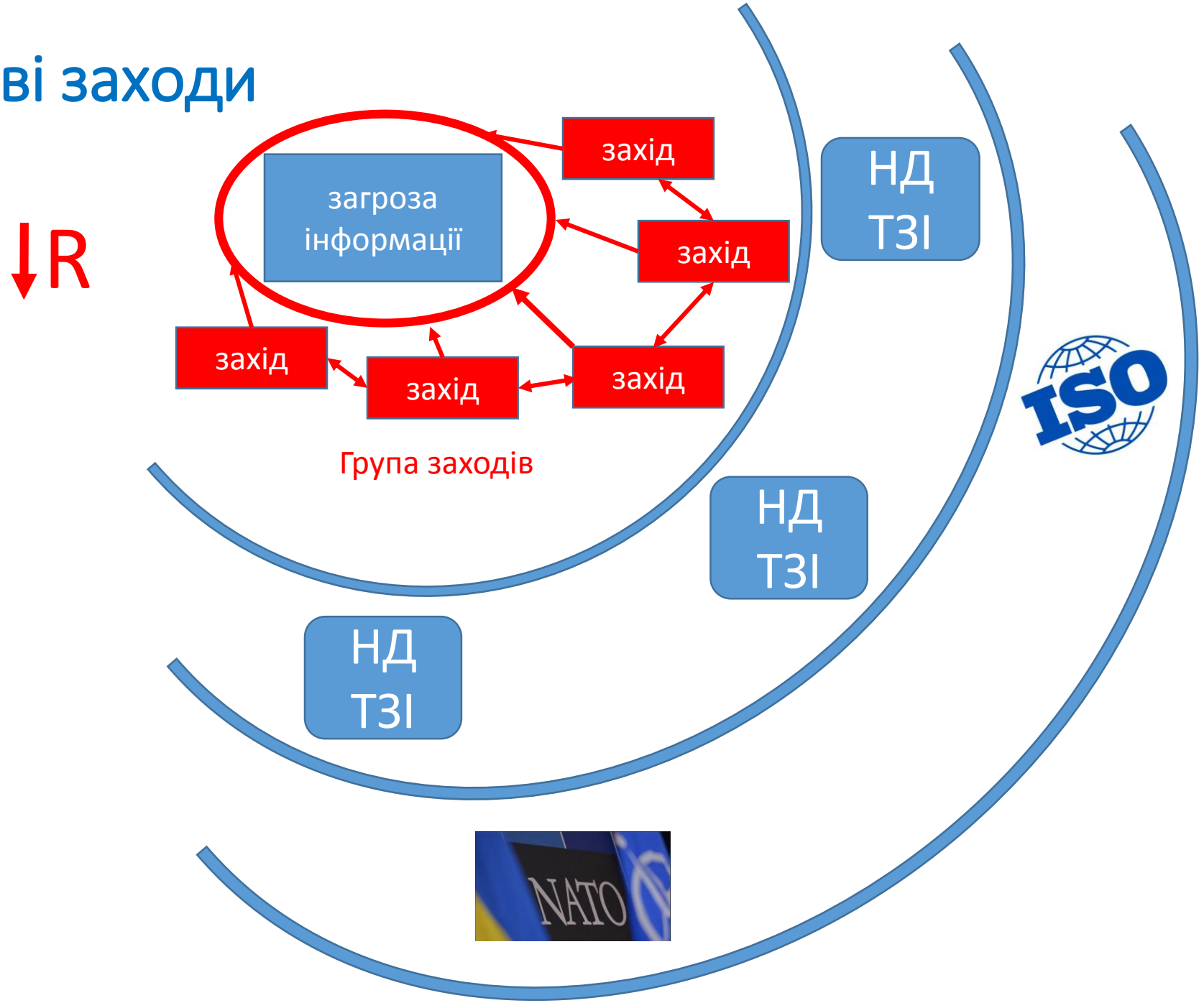
Організаційні та технічні заходи з кіберзахисту, які впроваджуються в ОКІІ, повинні забезпечувати:

- мережевий захист компонентів та інформаційних ресурсів ОКІІ;
- забезпечення доступності та відмовостійкості компонентів та ОКІІ;
- визначення умов використання змінних носіїв в ОКІІ;
- визначення умов використання програмного та апаратного забезпечення ОКІІ;
- визначення умов розміщення компонентів ОКІІ.

ПЕРЕЛІК
базових вимог із забезпечення кіберзахисту об’єктів критичної інфраструктури

- Мінімальний склад заходів із забезпечення кіберзахисту ОКІ наведений у **Додатку** до цих Вимог.
- Може бути доповнений з урахуванням:
  - ✓технології обробки інформації в ОКІІ,
  - ✓особливостей функціонування та програмно-апаратного складу Системи,
  - ✓складу інформаційних ресурсів та компонентів ОКІІ, які підлягають захисту, тощо.

Додаткові заходи



Виключення

Якщо

відсутня можливість реалізації окремих заходів з кіберзахисту

і/або неможливо застосувати Вимоги до окремих об’єктів захисту чи суб’єктів доступу, в тому числі внаслідок їх можливого негативного впливу на функціонування ОКІ

або неможливо реалізувати Вимоги в ОКІ через особливості функціонування або складу компонентів ОКІ

Обґрунтування, документальне підтвердження рішення

необхідно розробити та впровадити

або

обґрунтовано виключити

Підпис

компенсуючі заходи
що забезпечують блокування (нейтралізацію) загроз інформації в ОКІ

окремі заходи
з мінімального складу заходів із забезпечення кіберзахисту ОКІ

Конкретизовані вимоги з кіберзахисту ОКІ

- ЦОВВ можуть розробляти конкретизовані вимоги з кіберзахисту ОКІ підприємств, установ та організацій, які відносяться до сфери їх регулювання.
- Конкретизовані вимоги повинні враховувати специфіку функціонування ОКІІ.
- Конкретизовані вимоги повинні бути погоджені з Адміністрацією Держспецзв’язку.

Проблемні питання

Порядок визначення ОКІ?
Реєстр ОКІ?

Взаємодія в рамках ДПП?

Юридична відповідальність за не виконання Загальних вимог?

Відсутність системи незалежного аудиту

Відсутність страхових продуктів із страхування ризиків ІБ

Мотивація власників ОКІ?

Розвиток системи CERT, CSIRT

Дякую за увагу!