# ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ

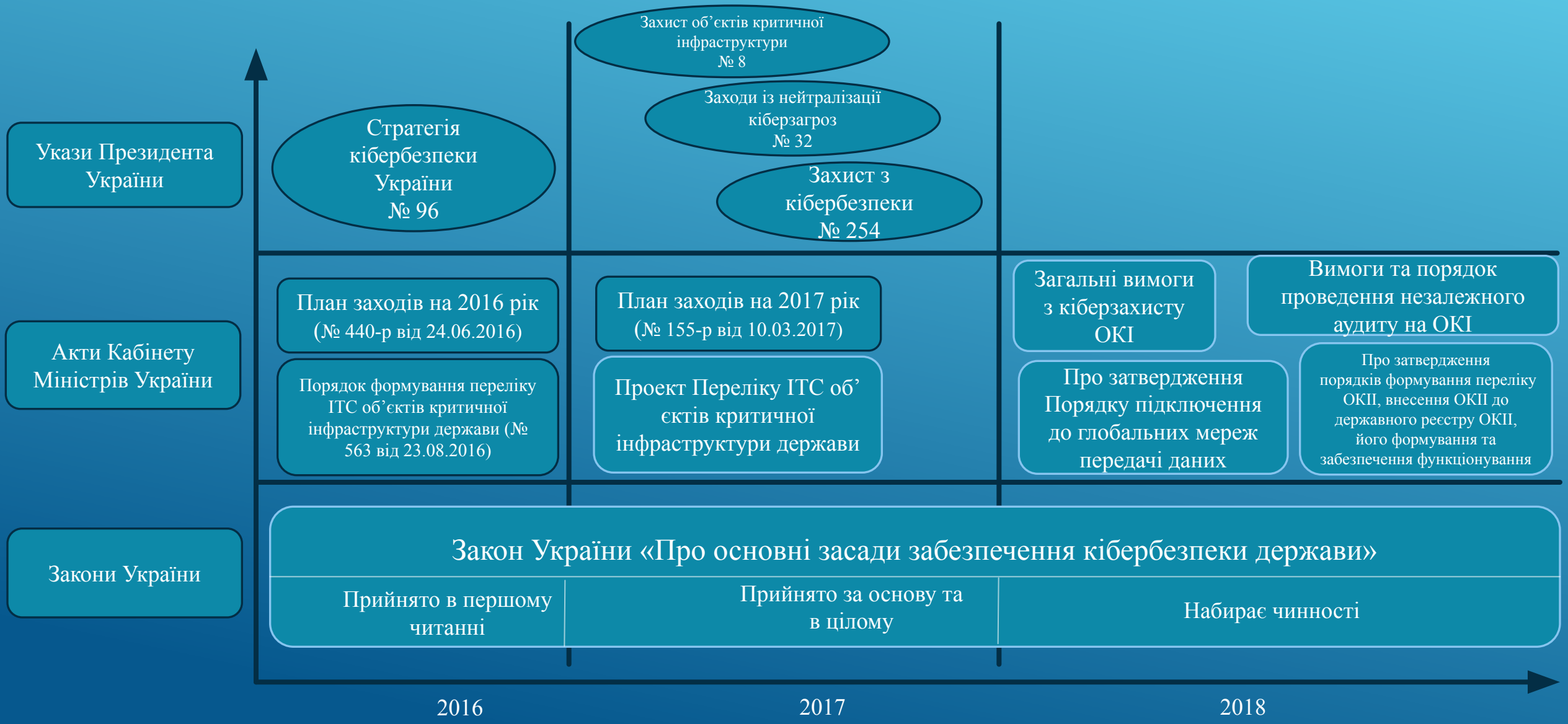
# ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Закон України «Про основні засади забезпечення кібербезпеки України» та інші нормативно-правові акти з питань забезпечення кібербезпеки як основа формування державної політики забезпечення кібербезпеки в Україні

Перший заступник Голови Державної служби спеціального зв’язку та захисту інформації України

Чаузов Олександр Миколайович

# БАЗОВІ ДОКУМЕНТИ З ПИТАНЬ КІБЕРБЕЗПЕКИ



# ЗАКОН УКРАЇНИ «ПРО ОСНОВНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ»

05.10.2017
прийнято
Верховною Радою України

20.10.2017
підписано Головою
Верховної Радою України

07.11.2017
підписано
Президентом України

09.05.2018
набирає чинності

**Є основоположним нормативно-правовим актом у сфері забезпечення кібербезпеки держави**

# ОСНОВНІ НАПРЯМИ РЕАЛІЗАЦІЇ ЗАКОНУ

ЗАКОН Є «РАМКОВИМ» – ОСНОВОЮ ДЛЯ УХВАЛЕННЯ ІНШИХ ЗАКОНОДАВЧИХ ТА ПІДЗАКОННИХ АКТІВ, А ТАКОЖ МІСТИТЬ НИЗКУ НОРМ ПРЯМОЇ ДІЇ, ЩО ДАЄ ЗМОГУ ЗАСТОСОВУВАТИ ЗНАЧНУ ЧАСТИНУ НОВИХ ІНСТРУМЕНТІВ ДЕРЖАВНОЇ ПОЛІТИКИ ТА РЕАЛІЗОВУВАТИ НОВІТНІ ТЕХНОЛОГІЧНІ ПРОЕКТИ

- Розвиток кіберпростору (системи/мережі е-комунікацій, ІТ-сфера, е-довірчі послуги)
- Боротьба з кібертероризмом (ОРД, розвідка, контррозвідка)
- Кібероборона (активний захист, міжнародна військова співпраця)
- Кіберзахист (базові вимоги захисту ІТС/КЗІ/ТЗІ, орг-тех модель, НТМ, виявлення, протидія, відновлення)
- Аудит інформаційної безпеки (ІТС критичної інфраструктури, ризик орієнтовані підходи, тестування вразливостей)
- Взаємодія, фахові і ресурсні спроможності, законодавче врегулювання, обмежувальні заходи
- Протидія кіберзлочинності (розслідування, притягнення до відповідальності)

Майже 80% дій і заходів, визначених Законом – компетенції Держспецзв'язку

# НОВАЦІЇ ЗАКОНУ (ОСНОВНІ, ЗА КОМПЕТЕНЦІЄЮ ДЕРЖСПЕЦЗВ'ЯЗКУ)

- Вводить новий сучасний термінологічний і понятійний апарат основних визначень таких як кіберпростір, кібербезпека, кіберзахист, кіберзлочин (комп'ютерний злочин), кібершпіонаж, кібертероризм, кібероборона, кіберзагроза, кібератака, інцидент кібербезпеки, об'єкт критичної (критичної інформаційної) інфраструктури, національні електронні інформаційні ресурси, аудит інформаційної безпеки
- Визначає основних суб'єктів забезпечення кібербезпеки, їх повноваження , протоколи взаємодії, систему координації та контролю їх діяльності
- Врегульовує питання кібербезпеки об'єктів критичної інфраструктури усіх форм власності, кіберзахисту їх ІТС, а також запроваджує систему незалежного аудиту інформаційної безпеки
- Встановлює відповідальність власників та/або керівників об’єктів критичної інфраструктури за забезпечення кіберзахисту, невідкладне інформування про інциденти кібербезпеки, організацію проведення незалежного аудиту інформаційної безпеки
- Визначає та врегульовує діяльність Державного центру кібербезпеки, урядової команди реагування на комп’ютерні надзвичайні події України CERT-UA

# СИСТЕМА КІБЕРБЕЗПЕКИ В УКРАЇНІ

Рада національної безпеки і оборони України
(Національний координаційний центр кібербезпеки)

Основні суб’єкти забезпечення кібербезпеки

Державна служба спеціального зв’язку та захисту інформації України (Урядовий CERT-UA)

Служба безпеки України

Міністерство внутрішніх справ України (Національна поліція)

Міністерство оборони України (Генеральний штаб ЗСУ)

Розвідувальні органи України

Національний банк України

Інші суб’єкти забезп. кібербезпеки

інші державні органи
розпорядники інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури та інших об’єктів кібербезпеки, які провадять діяльність із надання інформаційних та/або телекомунікаційних послуг
незалежні організації та експерти

# СКЛАДОВІ СИСТЕМИ КІБЕРБЕЗПЕКИ

**РНБО**

Національний координаційний центр кібербезпеки

## Організаційно-технічна складова кіберзахисту

організаційно-технічна модель кіберзахисту, система аудиту інформаційної безпеки

## Оперативна складова кібербезпеки

розвідувальні, контррозвідувальні, оперативно-розшукові, правоохоронні заходи

### ОБ ’ ЄКТИ

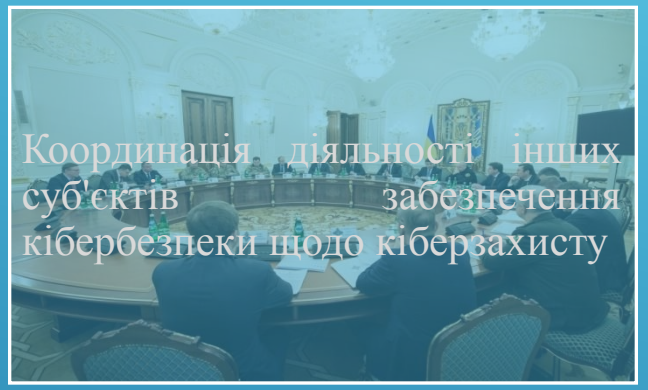
- Сектор профдіяльності (оператори, провайдери )
- ІТ-системи дежорганів
- Приватний сектор
- Критична інфраструктура

### ОСНОВНІ СУБ’ЄКТИ

| Захищеність *(ІТС, інформресурс)* | Активний захист *(реагування, протидія)* | Боротьба з кіберзлочинністю | Кіберрозвідка, протидія кібертероризм |
|---|---|---|---|
| Держспецзв'язку, НБУ | Держспецзв'язку, НБУ, МОУ, Генштаб ЗСУ | СБУ, Нацполіція | СБУ, СЗР, ГУР МО |

# ЗАВДАННЯ АДМІНІСТРАЦІЇ ДЕРЖСПЕЦЗВ’ЯЗКУ

Формування та реалізація державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом

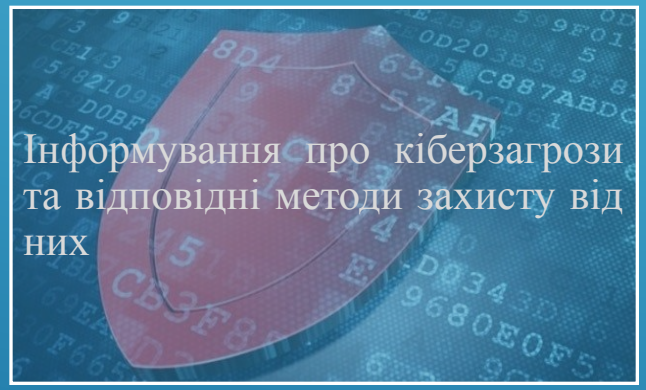


Координація діяльності інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту

Формування та реалізація державної політики щодо кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснення державного контролю у цих сферах

Забезпечення створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту

Здійснення організаційно-технічних заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків



Інформування про кіберзагрози та відповідні методи захисту від них

Забезпечення впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлення вимог до аудиторів інформаційної безпеки, визначення порядку їх атестації (переатестації)

Координація, організація та проведення аудиту захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість

Забезпечення функціонування Державного центру кіберзахисту, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA

# КІБЕРБЕЗПЕКА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

## Об’єкти критичної інфраструктури

Основні засади забезпечення кібербезпеки

Кібербезпека об'єктів критичної інфраструктури, кіберзахист ІТС таких об'єктів

*Закон України «Про основні засади забезпечення кібербезпеки України»*

Критерії віднесення об'єктів (підприємств, установ, організацій незалежно від форми власності) до критичної інфраструктури, вимоги до їх кібербезпеки

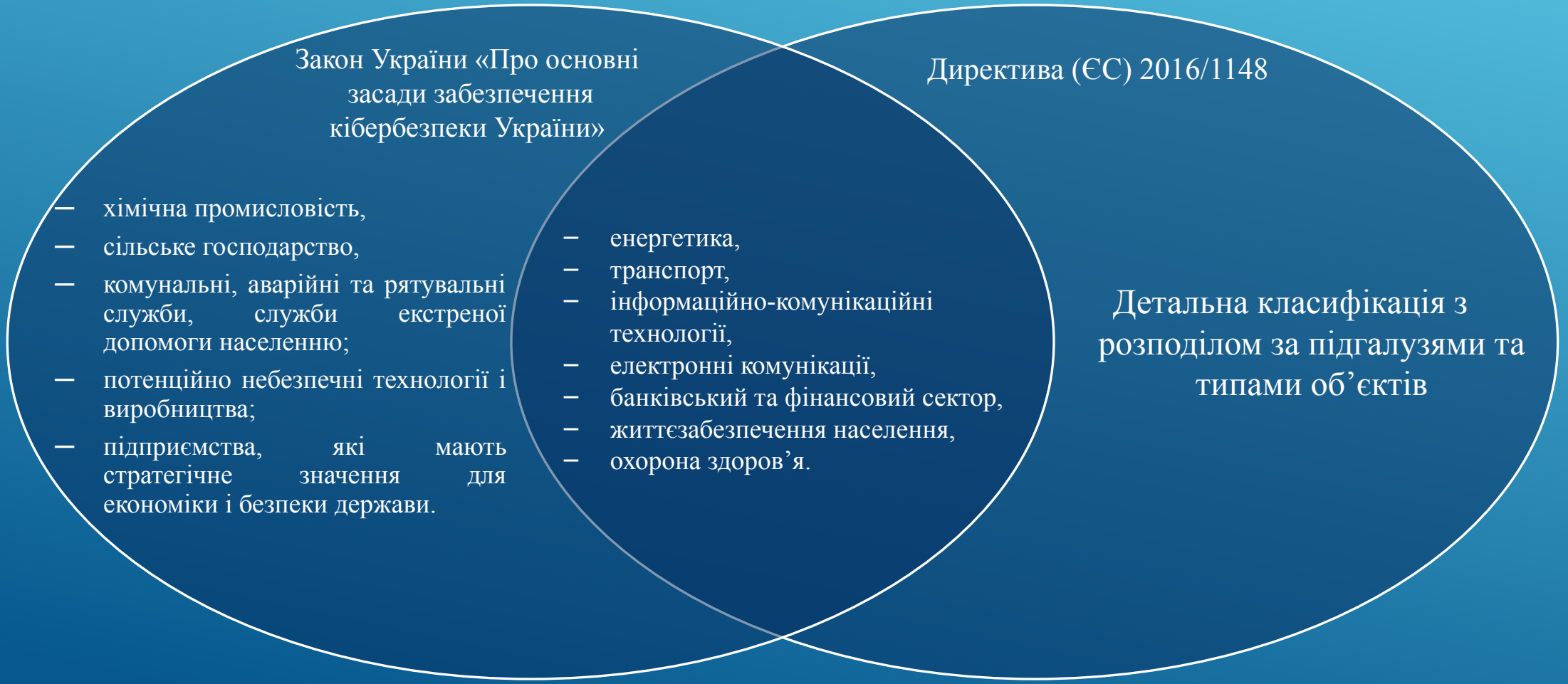
*Закон України «Про критичну інфраструктуру та її захист» (розробляється Мінекономрозвитку)*

Порядок формування переліку ІТС об’єктів критичної інфраструктури держави *(постанова КМУ № 563 від 23.08.2016)*

*Зміни до Порядку формування переліку ІТС (розробляються Держспецзв’язку)*

Перелік ІТС об’єктів критичної інфраструктури

# КЛАСИФІКАЦІЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ



# ПЕРСПЕКТИВНІ НАПРЯМИ РОЗВИТКУ СИСТЕМИ КІБЕРЗАХИСТУ

- Нормативно-правове врегулювання питань кіберзахисту та кібербезпеки
- Налагодження міжнародного співробітництва з питань кіберзахисту та кібербезпеки
- Дооснащення Команди реагування на комп'ютерні надзвичайні події України CERT-UA
- Побудова оперативного центру реагування на кіберінциденти
- Модернізація центрального сегменту Системи захищеного доступу державних органів до Інтернету
- Побудова Національної телекомунікаційної мережі

**ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ**

**ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ**

# ДЯКУЮ ЗА УВАГУ!

Київ, 23.11.2017