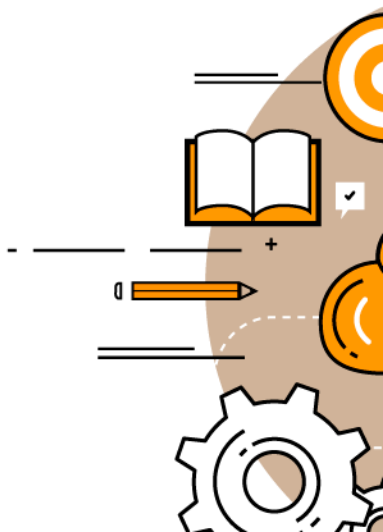
Основи інформаційної та кібербезпеки

Лекція 2.
Законодавчий та адміністративний рівні інформаційної безпеки

1. **Конституційно-правові засади забезпечення інформаційної безпеки в Україні**
2. **Правові засади інформаційної безпеки в умовах гібридної війни**
3. **Інституційне забезпечення інформаційної безпеки України**
4. **Адміністративний рівень інформаційної безпеки**



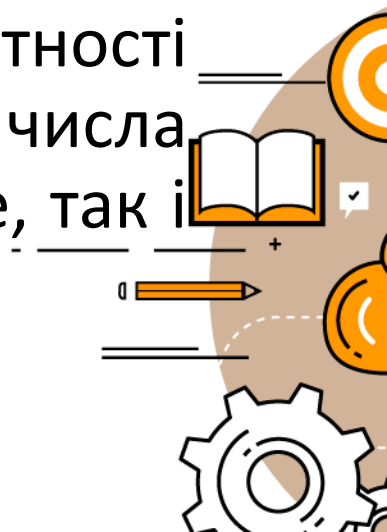
1 Конституційно-правові засади забезпечення ІБ в Україні

В Законі України «Про Концепцію Національної програми інформатизації» від 4 лютого 1998 р. офіційно визнано **інформаційну безпеку (ІБ)** як невід'ємну частину політичної, економічної, оборонної та інших складових національної безпеки.

Законом України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» було вперше законодавчо закріплено поняття інформаційна безпека як ***стан захищеності життєво важливих інтересів людини, суспільства і держави.***

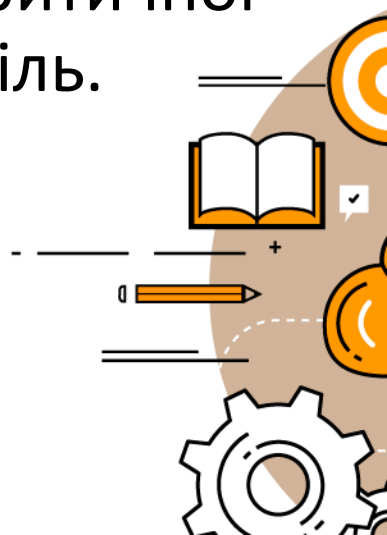
1 Конституційно-правові засади забезпечення ІБ в Україні

Труднощі у визначенні поняття «**інформаційна безпека**» (**ІБ**), обумовлені тим фактом, що феномен інформаційної безпеки наповнюється власним змістом в різних наукових областях: **технічній, правовій, психологічній, соціальній**, тим самим ще раз підкреслюючи її багатогранну природу. Тому спроби виробити дефініцію робляться постійно, оскільки визначення сутності інформаційної безпеки відноситься до числа проблем, вирішення яких має як теоретичне, так і практичне значення.



1 Конституційно-правові засади забезпечення ІБ в Україні

Якщо навести приклади, то **інформаційна безпека** – це про захист коштів на банківській картці, цілісність медичних даних у системі helsi, не заборонений контент у соціальних мережах, неможливість стороннього редагування законів на rada.gov.ua, конфіденційність повідомлень у месенджерах, а також захист від кібератак об’єктів критичної інфраструктури, наприклад аеропорту Бориспіль.



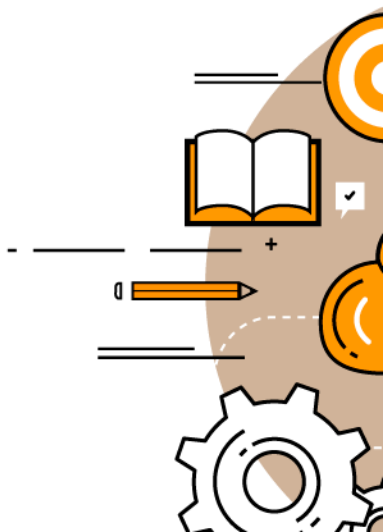
1 Нормативна база ІБ

Інформаційну безпеку України становлять три структурні елементи:

1. Інформаційна безпека у сфері прав і свобод людини та громадянина.

2. Інформаційно-психологічна безпека.

3. Інформаційно-технічна безпека.



1 Нормативна база ІБ

Нормативна база інформаційної безпеки повинна виконувати в першу чергу **три основні функції**:

1. Регулювати взаємовідносини між суб’єктами інформаційної безпеки, визначати їх права, обов’язки та відповідальність.

2. Нормативно забезпечувати дії суб’єктів інформаційної безпеки на всіх рівнях, а саме - людини, суспільства, держави.

3. Встановлювати порядок застосування різних сил і засобів забезпечення інформаційної безпеки.

1 Нормативна база ІБ

Структура правових актів, орієнтованих на забезпечення інформаційної безпеки держави :

1. Конституційне законодавство. Норми, що стосуються питань інформатизації, інформаційної безпеки тощо, входять у нього як складові елементи.

2. Загальні закони, кодекси (про власність, про надра, про землю, про права громадян, про громадянство, про податки, про антимонопольну діяльність тощо), які включають норми з питань інформаційної безпеки.

3. Закони про організацію управління, що стосуються окремих структур господарства, економіки, системи державних органів та визначаючих їх статус. Вони включають окремі норми по забезпеченню ІБ.

4. Спеціальні закони, які регламентують конкретні сфери відносин, галузі господарства, процеси. До них входить і Закон України «Про інформацію» та інші. Саме складі зміст цього блоку законів і створює спеціальне законодавство як основу правового забезпечення інформаційної безпеки.

5. Підзаконні нормативні акти із забезпечення інформаційної безпеки.

6. Законодавство, що містить норми про відповідальність за правопорушення у сфері ІБ.

Слід зауважити, що ІБ регулюється більш ніж **30 Законами**.

1 Нормативна база ІБ

Основою нормативно-правового регулювання системи забезпечення ІБ в Україні є

- Конституція України,
- Закон України «Про основи національної безпеки України»,
- Закон України «Про інформацію»,
- Закон України «Про Концепцію Національної програми інформатизації», інші нормативно-правові акти.

Від початку 2000-х рр. в Україні реалізовано комплекс заходів щодо удосконалення правового забезпечення інформаційної безпеки держави, прийнято Закони України «Про інформацію» (перший базовий нормативний закон у цій галузі) (1992 р.); Закон України «Про друковані засоби масової інформації (пресу в Україні)» (1992 р.), Закон України «Про авторське право і суміжні права» (1993 р.), «Про телебачення і радіомовлення» (1993 р.), «Про інформаційні агентства» (1995 р.), Закон України «Про рекламу» (1996 р.), «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації» (1997 р.), «Про електронні документи та електронний документообіг» (2003 р.), «Про захист персональних даних» (2010 р.) та ін.

1 Нормативна база ІБ

ст. 17 Конституції наголошує, що **забезпечення інформаційної безпеки** – “одна з найважливіших функцій держави, справа всього українського народу”, а Закон України “**Про Концепцію Національної програми інформатизації**” проголошує, що “інформаційна безпека є невід’ємною частиною політичної, економічної, оборонної та інших складових національної безпеки”

В ній, зокрема, є норми, що стосуються забезпечення ІБ України та які є визначальними для побудови національної системи інформаційної безпеки (статті 1—8; 15; 18; 19; 34; 73; пункти 2 і 9 ч. 1 ст. 85; пункти 19—20 ч. 1 ст. 106; ст. 132; пункти 7 і 10 ст. 138).

1 Нормативна база ІБ

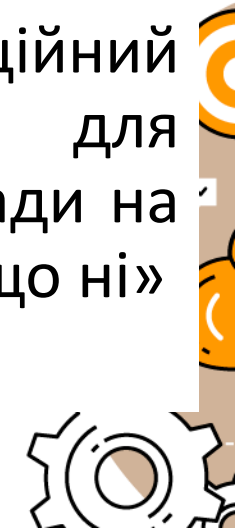
- У січні 1997 р. Верховна Рада України схвалила «**Концепцію (основи державної політики) національної безпеки України**».
- **Доктрина інформаційної безпеки України**, затверджена Указом Президента України від 8 липня 2009 р. № 514/2009 визначає інформаційну безпеку як самостійну сферу забезпечення національної безпеки України та одночасно як невід'ємну складову кожної з її сфер.
- Закон України «Про **Основні засади розвитку інформаційного суспільства** в Україні на 2007-2015 роки.

1 Нормативна база ІБ

Аналіз чинної законодавчої та нормативно-правової бази з позиції забезпечення інформаційної безпеки України свідчить, що у цій галузі характерна **термінологічна невизначеність**, неоднозначність та певна непослідовність.

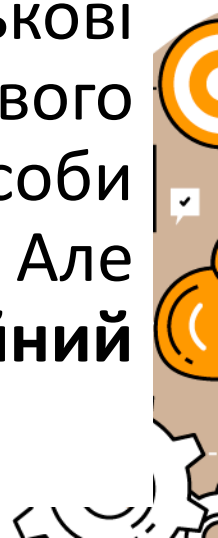
Наприклад, у експертному середовищі **Доктрина** отримала переважно негативну оцінку на кшталт “Доктрина інформаційної безпеки України – це лише декларація” або

«Замість повної інтеграції в міжнародний інформаційний простір, Україна встановлює паркан. Підстави для блокування сайтів настільки абстрактні, що орган влади на свій розсуд зможе тлумачити, що загрожує безпеці, а що ні»



2 Правові засади ІБ в умовах гібридної війни

- «**Гібридна війна**» – термін, що з’явився в кінці ХХ століття в США, який позначає введення війни проти будь-якої держави як традиційними (тобто за участю регулярних військових підрозділів, розвідки тощо), так і нетрадиційними способами.
- Гібридну війну називають війною четвертого покоління, «війною, яка сполучає традиційні та нетрадиційні форми, військові та невійськові тактики». Серед основних напрямів невійськового впливу використовуються всі відомі невоєнні засоби тиску – політичні, економічні, гуманітарні. Але пріоритетним тут, без сумніву, є **інформаційний компонент.**



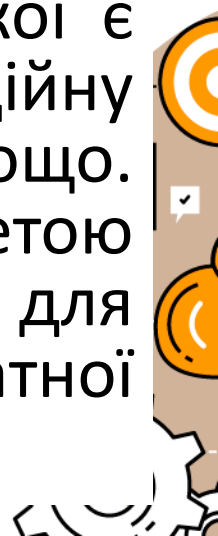
2 Правові засади ІБ в умовах гібридної війни

- У ході гібридної війни в інформаційному полі можливе досягнення таких результатів, як **втрата державних територій без пострілів**, за використанням однієї тільки дезінформації чи налаштування населення проти державної влади.
- Інформаційна складова гібридної війни Російської Федерації проти України є мабуть наймасштабнішою в новітній історії за часом та задіяними ресурсами. Так, у вересні 2014 р. Верховний головнокомандуючий Об'єднаних збройних сил НАТО в Європі генерал Філіп Брідлав назвав її «найдивовижнішим бліцкригом інформаційної війни, який ми колись бачили в історії».
- У квітні 2015 р. на парламентській асамблеї НАТО було представлено доповідь «Гібридна війна: новий стратегічний виклик НАТО?»

2 Правові засади ІБ в умовах гібридної війни

Головними викликами та загрозами інформаційної безпеки сьогодні для України є **інформаційна війна, інформаційний тероризм** та **інформаційні злочини**. Їх причиною є глобальні процеси інформатизації, прогрес у сфері розвитку інформаційних технологій та інформаційна складова гібридної війни Російської Федерації проти України.

Вкрай гострою залишається інформаційна складова гібридної війни РФ проти України, елементом якої є **кібертероризм**, втручання у критичну інформаційну інфраструктуру України вірусів-шпигунів тощо. **Інформаційний тероризм** застосовується з метою дезінформації, дезорієнтації та профанації для помилкового сприймання, розуміння і неадекватної поведінки суспільства.



2 Правові засади ІБ в умовах гібридної війни

- До виявів інформаційної війни може бути зарахована так звана «інформаційна злочинність», левова частка якої припадає на кіберзлочини.
- Якщо за станом на 2015 р. Україна посідала 5 місце у світовому рейтингу з ризику зіткнення з Веб-загрозами, то після атаки вірусу «Petya» у 2017 р., від якого постраждали енергетичні компанії, банки, урядові сайти, антирейтинг нашої країни в питаннях кібербезпеки відчутно зріс.
- Загалом за 2019 рік фахівці Служби Безпеки України нейтралізували понад 480 кіберінцидентів та кібератак на органи державної влади та об’єкти критичної інфраструктури. За цей період також припинено функціонування більше ніж 1000 сайтів, що використовувались у злочинних цілях.

2 Правові засади ІБ в умовах гібридної війни

З 2014 року законодавча база України у сфері інформаційної безпеки відчутно збагатилася. Загалом її можна поділити на 2 групи:

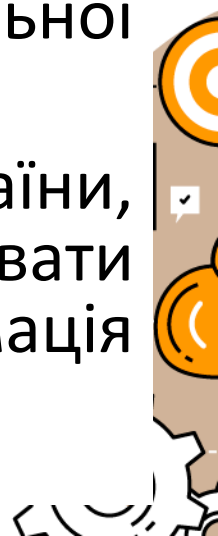
- концептуальні, базові документи, такі як Доктрини та Стратегії, які визначають основні загрози та тенденції в інформаційній безпеці.
- Закони України, Укази Президента, рішення РНБО України, які забороняють контент країни агресора на радіо, телебаченні та в Інтернет просторі України.

2 Правові засади ІБ в умовах гібридної війни

Нормотворчість 2000-х рр. не забезпечила реалізацію ст. 17 Конституції, яка ставить інформаційну безпеку до ряду найважливіших функцій держави, таких як захист суверенітету та територіальної цілісності.

Однією з причин теперішньої ситуації на Сході України стала нездатність держави дотриматись саме цієї функції у своїй внутрішній політиці. Відповідно, незабезпечення інформаційної безпеки призвело до втрати частини суверенітету та територіальної цілісності нашої держави.

З початком російської військової агресії проти України, у якій інформаційний супровід почав відігравати ключову роль, розпочалася трансформація національного інформаційного законодавства.



2 Правові засади ІБ в умовах гібридної війни

24 вересня 2015 року була прийнята оновлена **Воєнна Доктрина України**.

Доктрина чітко визначає **інформаційну війну** Російської Федерації проти України, модернізацію та вдосконалення спеціальними службами іноземних держав систем і комплексів технічної розвідки, нарощування їх можливостей, спроби несанкціонованого доступу до об’єктів інформаційної інфраструктури України.

Значна увага інформаційній складовій у Доктрині приділена у ст. 32.

2 Правові засади ІБ в умовах гібридної війни

Воєнна Доктрина України

Доктрина визначає **актуальними воєнними загрозами** для України: діяльність на території України не передбачених законом збройних формувань, спрямована на дестабілізацію внутрішньої соціально-політичної ситуації в Україні, **залякування населення, позбавлення його волі** до опору, порушення функціонування органів державної влади, місцевого самоврядування, важливих об'єктів промисловості та інфраструктури;

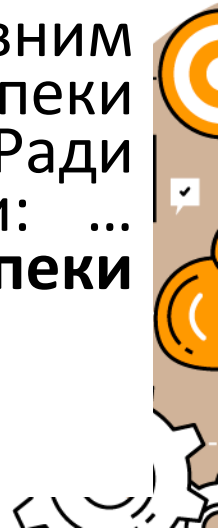
цілеспрямований **інформаційний (інформаційно-психологічний) вплив** з використанням сучасних **інформаційних технологій**, спрямований на формування негативного міжнародного іміджу України, а також на дестабілізацію внутрішньої соціально-політичної обстановки, загострення міжетнічних та міжконфесійних відносин в Україні або її окремих регіонах і місцях компактного проживання національних меншин;

2 Правові засади ІБ в умовах гібридної війни

6 травня 2015 року РНБО схвалила проект нової **Стратегії національної безпеки**, яка розрахована до 2020 року. Усі попередні стратегічні документи у сфері безпеки носили більш декларативний, аніж практичний характер. Даний документ базується на науковому підході. До його розроблення долучилися вітчизняні та міжнародні експерти, представники ЄС та НАТО.

Рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «**Про Стратегію національної безпеки України**»:

Вказано, що Кабінетові Міністрів України, державним органам за відповідними сферами національної безпеки подати у шестимісячний строк на розгляд Ради національної безпеки і оборони України проекти: … **Стратегії інформаційної безпеки**, **Стратегії кібербезпеки України**, …



2 Правові засади ІБ в умовах гібридної війни

Окремими загрозами інформаційній кібербезпеці, а також інформаційним ресурсам **Стратегія** визначає:

– ведення інформаційної війни проти України;

– відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства;

– уразливість об’єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак;

– фізичну і моральну застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом.

2 Правові засади ІБ в умовах гібридної війни

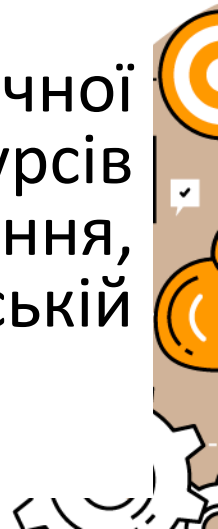
Пріоритетами забезпечення кібербезпеки і безпеки інформаційних ресурсів **Стратегія** визначає:

– розвиток інформаційної інфраструктури держави;

– створення системи забезпечення кібербезпеки, розвиток мережі реагування на комп'ютерні надзвичайні події (**CERT** https://cert.gov.ua/);

– розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів;

– забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, відмова від програмного забезпечення, зокрема антивірусного, розробленого у Російській Федерації;



2 Правові засади ІБ в умовах гібридної війни

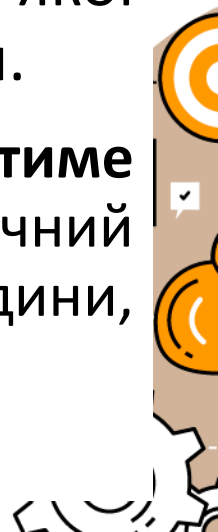
- **Стратегія кібербезпеки України**, затверджена Указом Президента України від 15 березня 2016 року № 96/2016, у розділі «Загальні положення» акцентує увагу на те, що стрімкий розвиток інформаційних технологій поступово трансформує світ. Стратегія кібербезпеки України має на меті створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.
- Розділ 4 «**Загрози кібербезпеці**» даної Стратегії вказує, що кіберпростір поступово перетворюється на окрему, поряд із традиційними "Земля", "Повітря", "Море" та "Космос", сферу ведення бойових дій, у якій все більш активно діють відповідні підрозділи збройних сил провідних держав світу.

2 Правові засади ІБ в умовах гібридної війни

- **Стратегія кібербезпеки України**, затверджена Указом Президента України від **26 серпня 2021** року № 447/2021

…Російська Федерація залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у гібридній війні проти України.

Відповідно до затвердженої Стратегії **Україна створюватиме** максимально відкритий, вільний, стабільний і безпечний кіберпростір в інтересах забезпечення прав і свобод людини, соціального, політичного і економічного розвитку держави.



2 Правові засади ІБ в умовах гібридної війни

- **Стратегія кібербезпеки України**, затверджена Указом Президента України від **26 серпня 2021** року

Ключову об’єднувальну та координаційну роль у цьому процесі відіграватиме **Національний координаційний центр кібербезпеки**.

Для формування потенціалу стримування (С) взято орієнтир на досягнення таких стратегічних цілей:

- – ціль С.1. Дієва кібероборона;
- – ціль С.2. Ефективна протидія розвідувально-підривній діяльності у кіберпросторі та кібертероризму;
- – ціль С.3. Ефективна протидія кіберзлочинності;
- – ціль С.4. Розвиток асиметричних інструментів стримування.

2 Правові засади ІБ в умовах гібридної війни

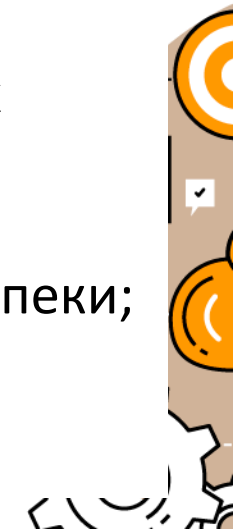
- **Стратегія кібербезпеки України**, затверджена Указом Президента України від **26 серпня 2021** року

Для набуття кіберстійкості (К) необхідним є досягнення таких стратегічних цілей:

- – ціль К.1. Національна кіберготовність та надійний кіберзахист;
- – ціль К.2. Професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки;
- – ціль К.3. Безпечні цифрові послуги.

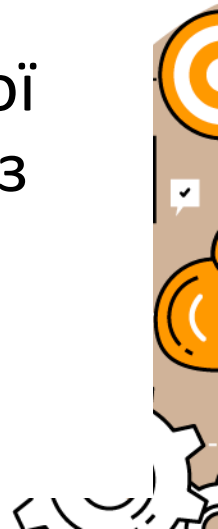
Для вдосконалення взаємодії (В) необхідним є досягнення таких стратегічних цілей:

- – ціль В.1. Зміцнення системи координації;
- – ціль В.2. Формування нової моделі відносин у сфері кібербезпеки;
- – ціль В.3. Прагматичне міжнародне співробітництво.



2 Правові засади ІБ в умовах гібридної війни

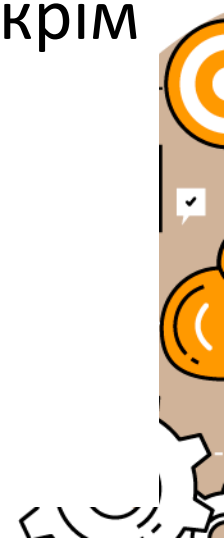
- 5 жовтня 2017 року Верховна Рада України ухвалила Закон «**Про основні засади забезпечення кібербезпеки України**». Відтепер за кібербезпеку, у рамках своїх повноважень, відповідальні міністерства, місцеві держадміністрації, органи місцевого самоврядування, правоохоронні органи, розвідка і контррозвідка, суб'єкти оперативно-розшукової діяльності.
- Закон визначає необхідність впровадження єдиної (універсальної) **системи індикаторів кіберзагроз** з урахуванням міжнародних стандартів з питань кібербезпеки і кіберзахисту.



2 Правові засади ІБ в умовах гібридної війни

Закон «Про основні засади забезпечення кібербезпеки України»

- Фахівці з інтернет-безпеки ввважають, що Закон досить узагальнений і до якихось безпосередніх дій не приведе. А ось закони і постанови, які будуть на його основі зроблені і реалізовані, мають бути більш конкретні. Експерти зауважили, що відтепер до кіберзахисту залучили Міністерство оборони, крім ДСТСЗІ і СБУ, які займалися цим раніше.



2 Правові засади ІБ в умовах гібридної війни

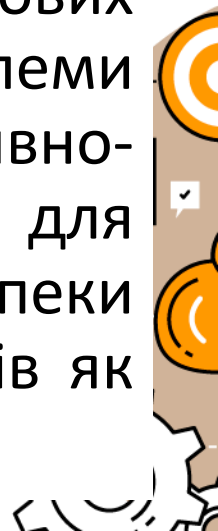
Важливим і визначним документом стала **Доктрина Інформаційної безпеки**, яка була введена в дію Указом Президента України від 25 лютого 2017 року № 47/2017.

У загальних положеннях Доктрини вказується, що «…застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Саме проти України Російська Федерація використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України».

2 Правові засади ІБ в умовах гібридної війни

Основною рисою **Доктрини інформаційної безпеки** 2017 року, яка відрізняється від попередньої Доктрини (2009 року) є спроба збалансувати повноваження між гілками влади та силових структур у сфері інформаційної безпеки.

- особливим недоліком нормативно-правового регулювання інформаційної безпеки України є розпорошення його у численних нормативно-правових актах різної юридичної сили. Причому важливі проблеми нормативно закріплюються підзаконними нормативно-правовими актами. Не менш важливою проблемою для ефективного забезпечення інформаційної безпеки України є неузгодженість нормативно-правових актів як між собою, так і з чинною Конституцією



2 Правові засади ІБ в умовах гібридної війни

- У побудові системи інформаційної безпеки, особливо телекомунікаційних мереж, важливе значення має Інтернет. Українське законодавство більше актуалізує **питання доступу до Інтернету**, а не сам контент. До прикладу, у європейській законодавчій практиці прийнято ряд планів дій та резолюцій, що дають змогу у певній мірі контролювати зміст інформації у мережі Інтернет.
- Указ Президента № 133/2017, яким увів в дію рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «**Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)**». Серед іншого, цим Указом було заборонено доступ до таких популярних до того в Україні інформаційних ресурсів як «1С», «В Контактє», «Однокласників», «Яндекс», «Mail.ru» та інших.

2 Правові засади ІБ в умовах гібридної війни

РІШЕННЯ РНБО України від 2 лютого 2021 року

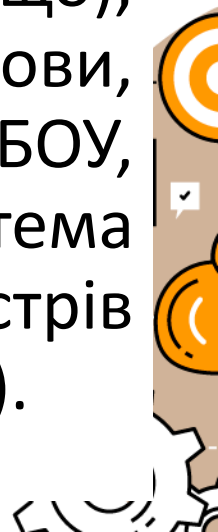
«**Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)**».

Рішення передбачає запровадження санкцій проти народного депутата України Тараса Козака та компаній, які володіють ліцензіями телеканалів «групи Медведчука» — «112», NewsOne і ZIK.

Також запроваджені санкції проти юридичних осіб телеканалів «112» (ТОВ «ТРК-112-ТВ» має супутникову ліцензію), NewsOne (ТОВ «Новини 24 години» має супутникову ліцензію), ZIK (ТОВ «ТРК Нові комунікації» має цифрову та супутникову ліцензії), а також регіональних телекомпаній, які до 2019 року мовили під логотипом «112 Україна», але Нацрада не продовжила їм у 2019 році ліцензії: «Новий формат», «Аріадна ТВ», «ТВ Вибір», «Партнер ТВ» та «Лідер ТВ».

3 Інституційне забезпечення ІБ України

Одним із найважливіших питань у сфері розбудови забезпечення інформаційної безпеки в Україні є впровадження **системи стратегічного управління**. Його основні складники – це **система інформаційно-аналітичного забезпечення** (джерела інформації, критерії і показники загроз, методики оброблення інформації, моніторинг, документування, банки даних паспортів загроз та антикризових механізмів тощо), **система обґрунтування рішень** (наукові установи, апарат РНБОУ), система ухвалення рішень (РНБОУ, Президент України, Верховна Рада України), система забезпечення реалізації рішень (Кабінет Міністрів України через стратегії, програми, плани, бюджети).



3 Інституційне забезпечення ІБ України

У зв’язку зі створенням ряд нових інституцій у сфері інформаційної безпеки, функції яких є дещо розмитими та нечіткими і часто дублюються, пропонуються: здійснити **перерозподіл повноважень** між органами державної влади та підпорядкувати сферу інформаційної безпеки одному керуючому органу з метою виконання чіткого виконання завдань, визначених у Стратегії національної безпеки та Доктрині інформаційної безпеки;

сформувати незалежний інститут інформаційного омбудсмена – як незалежного органу, діяльність якого спрямована на захист прав і свобод людини в інформаційній сфері.

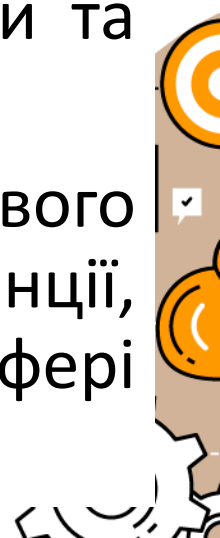
3 Інституційне забезпечення ІБ України

- До основних **суб'єктів забезпечення** інформаційної безпеки відносять Президента України, Кабінет Міністрів України та Верховну Раду України.
- **РНБО України** має повноваження координувати та контролювати діяльність органів виконавчої влади з реалізації політики інформаційної безпеки України та вносити Президенту України пропозиції щодо її уточнення та ресурсного забезпечення.
- при РНБО з 2002 року існує консультативно-дорадчий орган «Міжвідомча комісія з питань інформаційної політики та інформаційної безпеки».
- До складу Верховної Ради входять три профільні парламентські комітети:

Комітет з питань національної безпеки, оборони та розвідки,
Комітет з питань гуманітарної та інформаційної політики,
Комітет з питань цифрової трансформації, які виконують завдання щодо підготовки законопроектів з питань розвитку інформаційної сфери та інформаційної безпеки.

3 Інституційне забезпечення ІБ України

- До інституцій інформаційної безпеки прямо чи опосередковано відносяться міністерства та інші центральні органи виконавчої влади;
- Державний комітет телебачення і радіомовлення України; Державна служба спеціального зв’язку та захисту інформації України; Збройні Сили України, Служба безпеки України, Служба зовнішньої розвідки України, Державна прикордонна служба України та інші військові формування.
- Місцеві державні адміністрації та органи місцевого самоврядування, відповідно до їхньої компетенції, забезпечують вирішення питань у сфері інформаційної безпеки на регіональному рівні.



3 Модель системи забезпечення ІБ

Система утворюється об’єктами та суб’єктами інформаційної безпеки відповідно.

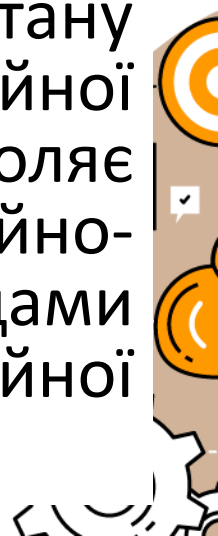
При цьому до **об’єктів інформаційної безпеки** належать:

- конституційні права і свободи людини і громадянина, фізичне та психологічне здоров’я населення,
- захищеність людини від деструктивного та маніпулятивного інформаційного впливів;
- інформаційне забезпечення, гарантії інформаційних прав та права на розвиток населення всіх регіонів України;
- інформаційний суверенітет, безпека національного сегмента глобального інформаційного простору, інформаційної інфраструктури, захищеність, цілісність, доступність та безпечність інформаційних ресурсів, продукції і послуг.

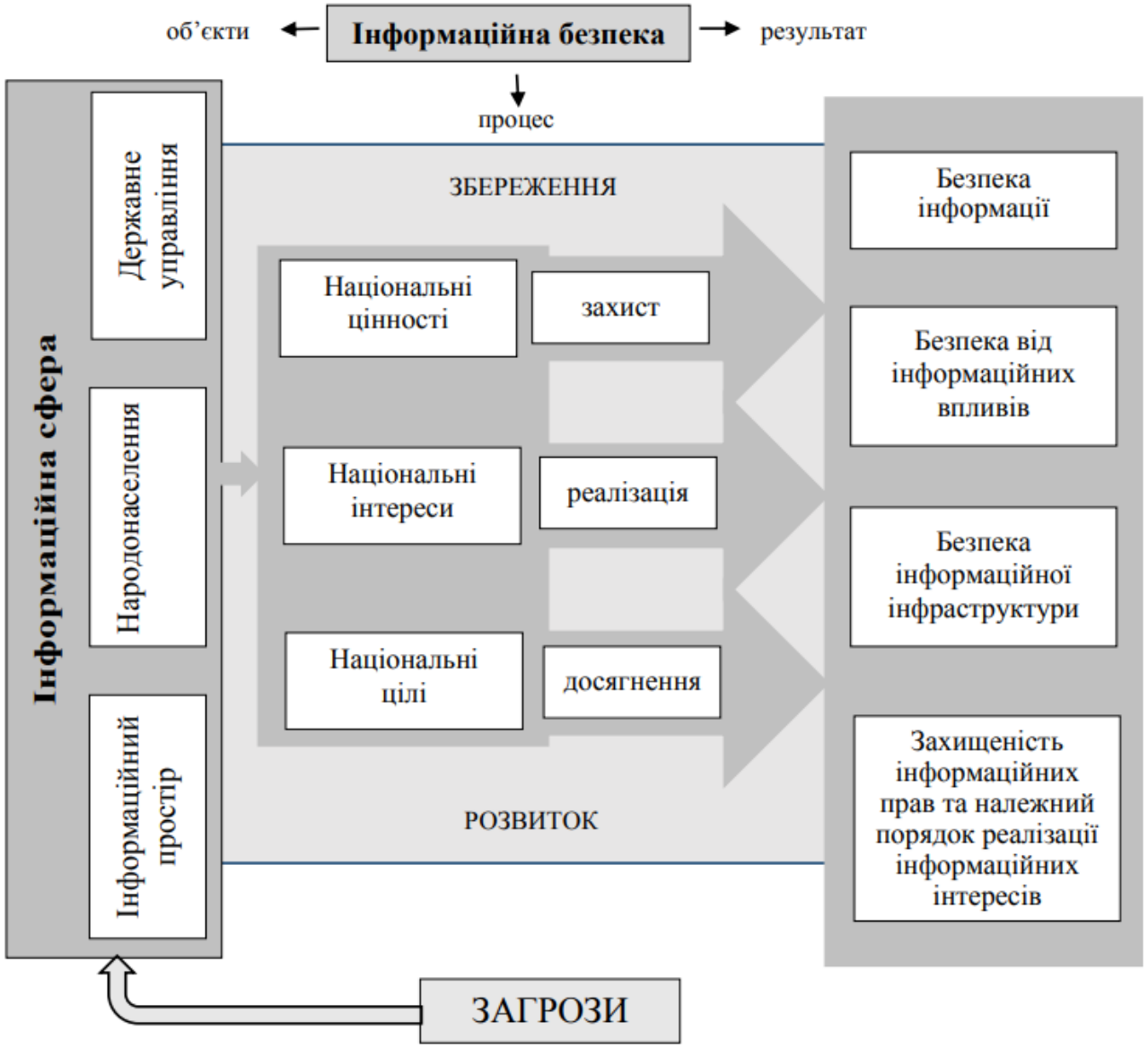
3 Модель системи забезпечення ІБ

Система ІБ з точки зору її об’єктів відповідає класичній формулі для об’єктів національної безпеки “територія – народонаселення – система державного управління”, однак замість території для інформаційної безпеки вважаємо за доцільне використовувати поняття “інформаційний простір”, яке в т.ч. охоплюватиме інформаційну модель території та її інформаційне обслуговування.

Розмежування інформаційної безпеки як стану динамічної системи та забезпечення інформаційної безпеки як процесу підтримання цього стану дозволяє певним чином зняти протиріччя між організаційно-структурним і функціонально-діяльнісним підходами до визначення сутності феномену інформаційної безпеки та її системи.



3 Модель системи забезпечення ІБ



3 Модель системи забезпечення ІБ

Розглядаючи інформаційну безпеку України у **соціальній та гуманітарній сферах**, необхідно зазначити, що основними реальними та потенційними загрозами в цій галузі є:

- відставання України від розвинутих держав за рівнем інформатизації соціальної та гуманітарної сфер, насамперед освіти, охорони здоров'я, соціального забезпечення, культури;
- недодержання прав людини і громадянина на одержання інформації, необхідної для захисту їх соціально-економічних прав;
- поширення в засобах масової інформації невластивих українській культурній традиції цінностей і способу життя, культу насильства, жорстокості, порнографії, зневажливого ставлення до людської і національної гідності;
- тенденція до витіснення з інформаційного простору та молодіжної культури українських мистецьких творів, народних традицій і форм дозвілля;
- послаблення суспільно-політичної, міжетнічної та міжконфесійної єдності суспільства;
- відставання рівня розвитку українського кінематографу, книговидання, книгорозповсюдження та бібліотечної справи від рівня розвинутих держав.

3 Модель системи забезпечення ІБ

Розглядаючи загрози інформаційної діяльності, нам також необхідно розглянути проблеми, які виникають з цього приводу **в науково-технологічній сфері**. Ці загрози:

- витоку за кордон наукових кадрів та суб'єктів права інтелектуальної власності;
- низька конкурентоспроможність вітчизняної інформаційної продукції на світовому ринку;
- недостатній захист від несанкціонованого доступу до інформації внаслідок використання іноземних інформаційних технологій та техніки.

До загальних загроз ми відносимо:

1) розрив потоків інформації між: а) наукової та науково-технічної сферами; б) науково-технічної та економічної сферами;
2) односторонній характер зовнішніх зв'язків з акцентом на надання науковотехнічної інформації зовнішньому споживачеві;
3) обмеженість доступу до світових інформаційних ресурсів;
4) неясність державної науково-технічної політики;
5) відхід науковотехнічних кадрів – носіїв інформації в інші сфери діяльності.

3 Модель системи забезпечення ІБ

Розглядаючи інформаційну безпеку України в **екологічній сфері**, необхідно зазначити, що основними реальними та потенційними загрозами в цій галузі є:

- приховування, несвоєчасне надання інформації або надання недостовірної інформації населенню про надзвичайні екологічні ситуації чи надзвичайні ситуації техногенного та природного характеру;
- недостатня надійність інформаційно-телекомунікаційних систем збирання, обробки та передачі інформації в умовах надзвичайних ситуацій;
- низький рівень інформатизації органів державної влади, що унеможливлює здійснення оперативного контролю та аналізу стану потенційно небезпечних об’єктів і територій, завчасного прогнозування та реагування на надзвичайні ситуації.

3 Модель системи забезпечення ІБ

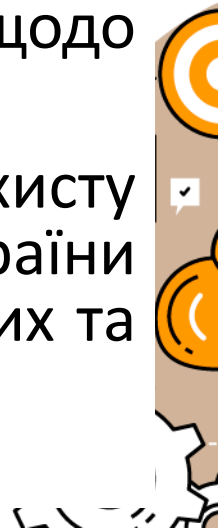
Окремою складовою вважаємо **політичне забезпечення інформаційної безпеки**, сутністю якої є утвердження демократичних форм і інститутів.

Чітке розмежування компетенції органів законодавчої, виконавчої та судової влади у сфері інформаційної безпеки.

Основним завданням органів законодавчої влади є встановлення найважливіших правил поведінки у сфері інформаційної діяльності,

виконавчої влади – здійснення державної політики щодо забезпечення інформаційної безпеки,

судової – утвердження верховенства права шляхом захисту гарантованих Конституцією і законами України інформаційних інтересів держави, суспільства, фізичних та юридичних осіб.



4 Адміністративний рівень ІБ

Зарубіжне законодавство в галузі інформаційної безпеки

Законодавчий рівень інформаційної безпеки найбільше забезпечений у **США**, де нараховується близько 500 законодавчих актів.

Ключову роль грає "**Закон про інформаційну безпеку**" (Computer Security Act of 1987, Public Law 100-235 (H.R. 145), January 8, 1988). Його мета – реалізація мінімально достатніх дій щодо забезпечення безпеки інформації у федеральних комп'ютерних системах, без обмежень всього спектра можливих дій.

На початку Закону називається конкретний виконавець – **Національний інститут стандартів і технологій (NIST)**, що відповідає за випуск стандартів і положень, спрямованих на захист від знищення і несанкціонованого доступу до інформації, а також від крадіжок і фальсифікацій, що здійснюють-ся за допомогою комп'ютерів. Таким чином, увага приділя-ється як регламентації дій фахівців, так і підвищенню інфор-мованості всього суспільства.

4 Адміністративний рівень ІБ

Зарубіжне законодавство в галузі інформаційної безпеки

- У законодавстві **ФРН** основним є “**Закон про захист даних**” (Federal Data Protection Act of December 20, 1990 (BGBl.I 1990 S.2954), amended by law of September 14, 1994 (BGBl. I S. 2325). Він цілком присвячений захисту персональних даних. Як і у всіх інших законах аналогічної спрямо-ваності, в даному випадку встановлюється пріоритет інтересів національної безпеки над збереженням таємниці приватного життя.
- У законодавстві **Великої Британії** є сімейство так званих добровільних стандартів **BS 7799**, що допомагають організаціям на практиці сформувати програми безпеки. Цей стандарт сфокусований на підвищенні ефективності інформаційної безпеки шляхом реалізації безперервної програми дій з управління ризиками. Інструкції, що містяться в цьому стандарті, призначені для застосування в будь-яких організаціях, незалежно від їх типу, розміру і характеру бізнесу. Актуальною версією стандарту є BS 7799-3:2017. Контент стандарту є платним.

4 Адміністративний рівень ІБ

Зарубіжне законодавство в галузі інформаційної безпеки

- У сучасному світі глобальних мереж законодавча база повинна бути узгоджена з міжнародною практикою. В цьому плані повчальний приклад Аргентини.
- В 1996 році в Аргентині був заарештований системний оператор електронної дошки оголошень. Йому ставилися в провину систематичні вторгнення в комп'ютерні системи ВМС США, НАСА, а також у комп'ютерні системи Бразилії, Чилі, Кореї, Мексики і Тайваню. Проте, його відпустили без офіційного висування звинувачень, оскільки за аргентинським законодавством вторгнення в комп'ютерні системи не вважається злочином.

4 Стандарти і специфікації в галузі безпеки інформаційних систем

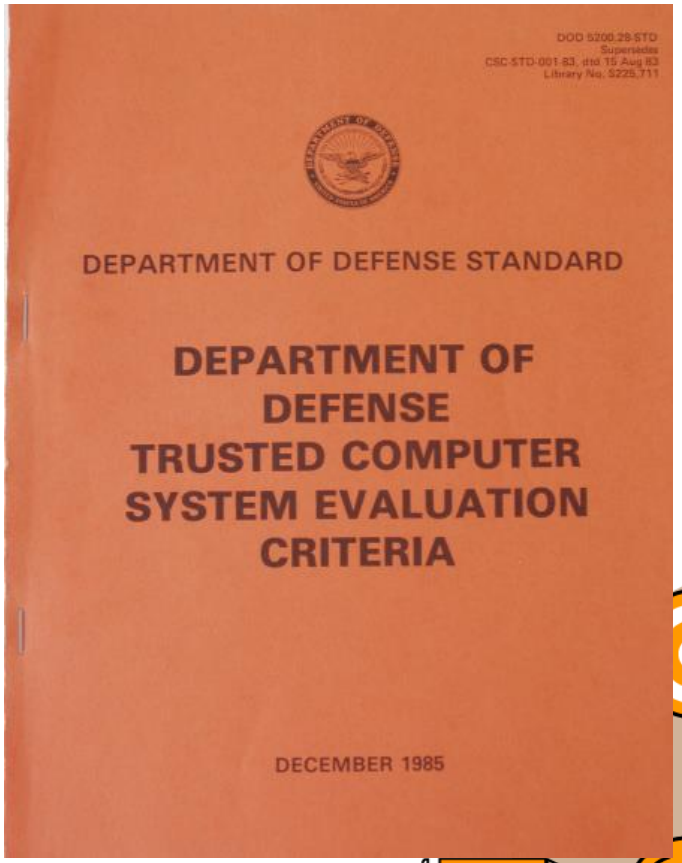
Особливе місце на законодавчому рівні займають стандарти і специфікації, до яких належать:

- оцінні стандарти, спрямовані на класифікацію інформаційних систем і засобів захисту за вимогами безпеки;
- технічні специфікації, що регламентують різні аспекти реалізації засобів захисту.

Оцінні стандарти виділяють найважливіші, з погляду інформаційної безпеки, аспекти ІС, які виконують роль архітектурних специфікацій. Інші технічні специфікації визначають, як будувати ІС указаної архітектури.

4 Стандарти і специфікації в галузі безпеки інформаційних систем

“Помаранчева книга” як оцінний стандарт



- Історично першим оцінним стандартом, що набув значного поширення і зробив величезний вплив на базу стандартизації інформаційної безпеки у багатьох країнах, став стандарт Міністерства оборони США “Критерії оцінювання довірених комп’ютерних систем” (1983 р.).

В ній мова йде не про безпечні, а про **довірені системи**, тобто системи, яким можна надати певний ступінь довіри.

4 Стандарти і специфікації в галузі безпеки інформаційних систем

“Помаранчева книга” як оцінний стандарт

Очевидно, що абсолютно безпечних систем не існує, це абстракція. Є сенс оцінювати лише **ступінь довіри**, яку можна надати тій чи іншій системі.

Довірена система – це система, що використовує достатні апаратні і програмні засоби для забезпечення одночасного оброблення інформації різного ступеня секретності групою користувачів без порушення права доступу.

Ступінь довіри оцінюється за двома критеріями: **політика безпеки і рівень гарантованості**.

Політика безпеки – це набір законів, правил і норм поведінки, що визначають, як організація обробляє, захищає і поширює інформацію.

Рівень гарантованості – це міра довіри, яка може бути надана архітектурі і реалізації ІС.

4 Стандарти і специфікації в галузі безпеки інформаційних систем

“Помаранчева книга” як оцінний стандарт

У “Помаранчевій книзі” визначається чотири рівні довіри – D, C, B і A. Рівень D призначений для систем, визнаних незадовільними. По мірі переходу від рівня C до рівня A висуваються все більш жорсткі вимоги до систем. Рівні C і B поділяються на класи (C1, C2, B1, B2, B3) з поступовим зростанням ступеня довіри.

Усього є шість класів безпеки – C1, C2, B1, B2, B3, A1. Щоб в результаті процедури сертифікації систему можна було віднести до деякого класу, її політика безпеки і рівень гарантованості повинні задовольняти заданим вимогам.

4 Стандарти кібербезпеки

BS 7799-1: 2005 — Британський стандарт BS 7799 перша частина. BS 7799 Частина 1 — Кодекс практики управління інформаційною безпекою (Практичні правила управління інформаційної безпеки) описує 127 механізмів контролю, необхідних для побудови системи управління інформаційною безпекою (СУІБ) організації, визначених на основі кращих прикладів світового досвіду в цій області . Цей документ служить практичним керівництвом по створенню СУІБ.

BS 7799-2: 2005 — Британський стандарт BS 7799 друга частина стандарту. BS 7799 Частина 2 — Управління інформаційною безпекою — специфікація систем управління інформаційною безпекою (Специфікація системи управління інформаційної безпеки) визначає специфікацію СУІБ. Друга частина стандарту використовується як критерії при проведенні офіційної процедури сертифікації СУІБ організації.

BS 7799-3: 2006 — Британський стандарт BS 7799 третя частина стандарту. Новий стандарт в області управління ризиками інформаційної безпеки.

ISO/IEC 17799: 2005 — «Інформаційні технології — Технології безпеки — Практичні правила управління інформаційної безпеки». Міжнародний стандарт, базувався на BS 7799-1: 2005.

ISO/IEC 27001 — «Інформаційні технології — Методи забезпечення безпеки — Системи управління інформаційної безпеки — Вимоги». Міжнародний стандарт, базувався на BS 7799-2: 2005.

ISO/IEC 27001:2013 — версія друга. Поточна. **ДСТУ ISO/IEC 27001:2015**

ISO/IEC 27002 — Зараз: ISO/IEC 17799: 2005. «Інформаційні технології — Технології безпеки — Практичні правила управління інформаційної безпеки».

ISO/IEC 27005 — Зараз: **ISO/IEC 27005:2018** — Керівництво з управління ризиками ІБ.