

Національний юридичний університет
імені Ярослава Мудрого

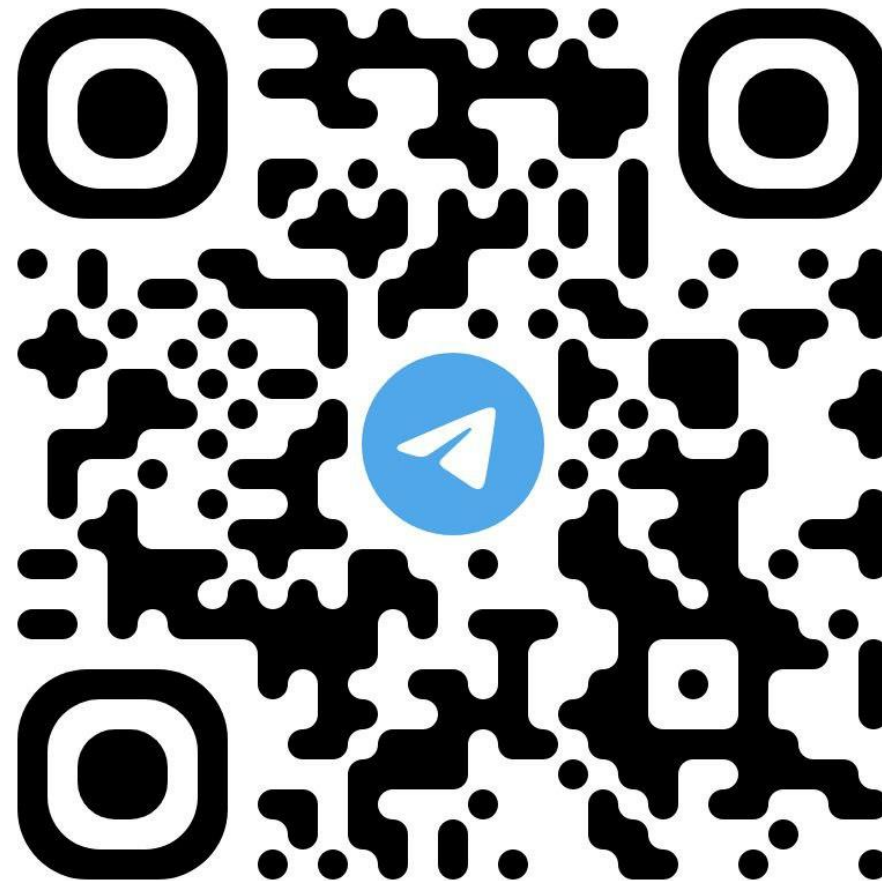
Лекція на тему:

Основні цілі, напрями та принципи державної політики у сфері кібербезпеки.

Лектор:
доцент **Таволжанський
Олексій Володимирович**



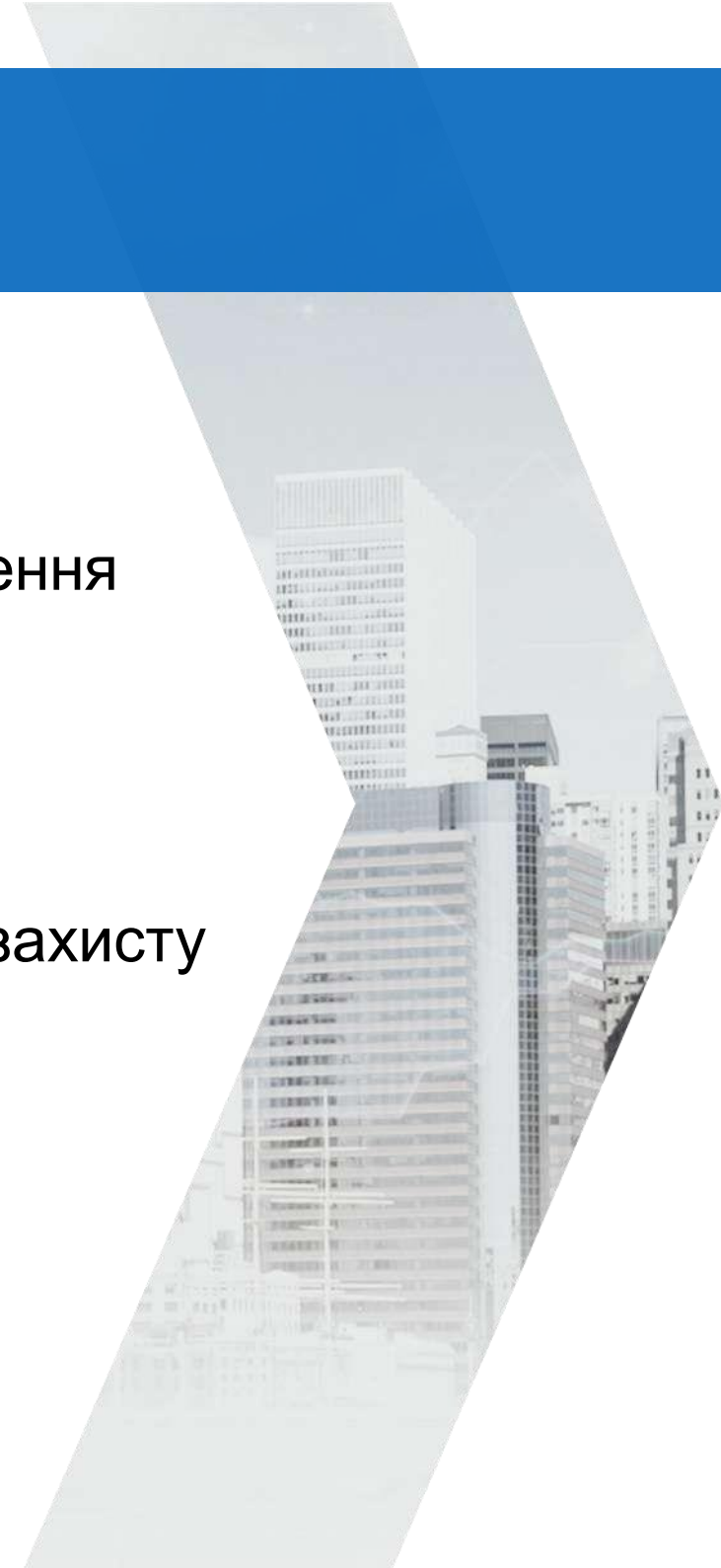
Група у телеграм





План:

1. Правові основи забезпечення кібербезпеки України. Визначення кіберпростору
2. Об'єкти кібербезпеки та кіберзахисту





План:

3. Суб'єкти забезпечення кібербезпеки
4. Передумови та чинники кіберзагроз
5. Заходи забезпечення кібербезпеки



Принципи державної політики у сфері кібербезпеки

1) мінімально необхідного регулювання, згідно з яким рішення (заходи) суб'єктів владних повноважень повинні бути необхідними і мінімально достатніми для досягнення мети і завдань, визначених цим Законом;

ЗУ «Про основні засади забезпечення кібербезпеки України» (2017)

Принципи державної політики у сфері кібербезпеки

2) об'єктивності та правової визначеності, максимально можливого застосування національного та міжнародного права щодо повноважень і обов'язків державних органів, підприємств, установ, організацій, громадян у сфері кібербезпеки;



Принципи державної політики у сфері кібербезпеки

3) забезпечення захисту прав користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій, та/або послуг із захисту інформації, кіберзахисту, у тому числі прав щодо невтручання у приватне життя і захисту персональних даних;



Принципи державної політики у сфері кібербезпеки

4) прозорості, згідно з яким рішення (заходи) суб'єктів владних повноважень мають бути належним чином обґрунтовані та повідомлені суб'єктам, яких вони стосуються, до набрання ними чинності (їх застосування);



Принципи державної політики у сфері кібербезпеки

5) збалансованості вимог та відповідальності, згідно з яким має бути забезпечено баланс між встановленням відповідальності за невиконання вимог кібербезпеки та кіберзахисту, а також за запровадження надмірних вимог та обмежень;



Принципи державної політики у сфері кібербезпеки

б) недискримінації, згідно з яким рішення, дії та бездіяльність суб'єктів владних повноважень не можуть призводити до юридичного або фактичного обсягу прав та обов'язків особи, який є:

відмінним від обсягу прав та обов'язків інших осіб у подібних ситуаціях, якщо тільки така відмінність не є необхідною та мінімально достатньою для задоволення загальносуспільного інтересу;

таким, як і обсяг прав та обов'язків інших осіб у неподібних ситуаціях, якщо така однаковість не є необхідною та мінімально достатньою для задоволення загальносуспільного інтересу;

Принципи державної політики у сфері кібербезпеки

7) еквівалентності вимог до забезпечення кібербезпеки об'єктів критичної інфраструктури, згідно з яким застосування правових норм повинно бути якомога більш рівнозначним щодо кіберзахисту комунікаційних та технологічних систем об'єктів критичної інфраструктури, що належать до одного сектору економіки та/або які здійснюють аналогічні функції.

Загальні уявлення про кіберпростір



Легальне визначення кіберпростору

КІБЕРПРОСТІР - середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) **комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних.**

ЗУ «Про основні засади забезпечення кібербезпеки України» (2017)



Загальні уявлення про кіберпростір

Розрізняють поняття:

комунікаційної системи і системи комунікацій.

Під **системою комунікацій** зазвичай розуміють комплекси засобів зв'язку і передачі інформації.

Комунікаційна система є структурована (впорядкована певним чином) сукупність комунікаторів, реципієнтів, смислових повідомлень, комунікаційних каналів (включаючи комунікаційні служби, які мають матеріально-технічними ресурсами і професійними кадрами) і засоби комунікації (знаки і символи).

Визначення системи комунікацій

ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА -

сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле

ОБ'ЄКТАМИ ЗАХИСТУ в системі є:

- інформація, що обробляється в ній, та*
- програмне забезпечення, яке призначено для обробки цієї інформації.*

ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах» (1994)

Визначення системи комунікацій

СИСТЕМИ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ (далі - комунікаційні системи) - системи передавання, комутації або маршрутизації, обладнання та інші ресурси (включаючи пасивні мережеві елементи, **які дають змогу передавати сигнали** за допомогою провідових, радіо-, оптичних або інших електромагнітних засобів, мережі мобільного, супутникового зв'язку, електричні кабельні мережі в частині, **в якій вони використовуються для цілей передачі сигналів**), що забезпечують електронні комунікації (передачу електронних інформаційних ресурсів), у тому числі засоби і пристрої зв'язку, комп'ютери, інша комп'ютерна техніка, інформаційно-телекомунікаційні системи, які мають доступ до мережі **Інтернет та/або інших глобальних мереж передачі даних**.

... Загальні уявлення про кіберпростір

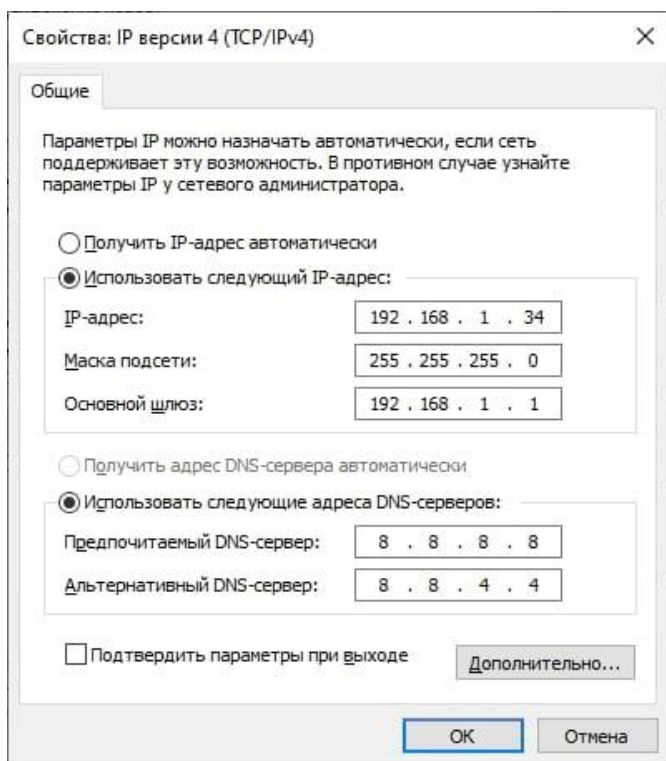


**КІБЕРПРОСТІР —
це**

***цілісна
технічна
система***

Впорядкування інтернет простору

IP-адреса (айпі-адреса, скорочення від англ. Internet Protocol Address) - унікальна мережева адреса вузла в комп'ютерній мережі, побудованій за протоколом IP.



У мережі Інтернет потрібна глобальна унікальність адреси.

У випадку роботи в локальній мережі потрібна унікальність адреси в межах мережі.

Впорядкування інтернет простору

IPv4 та IPv6

В 4-й версії IP-адреса являє собою 32-бітове число. Зручною формою запису IP-адреси (IPv4) є запис у вигляді чотирьох десяткових чисел значенням від 0 до 255, розділених крапками, наприклад: 192.168.0.1.

У 6-й версії IP-адреса (IPv6) має 128-бітове представлення. Адреси розділяються двокрапкою (напр. fe80:0:0:0:200:f8ff:fe21:67cf або 2001:0db8:85a3:0000:0000:8a2e:0370:7334). Велика кількість нульових груп може бути пропущено за допомогою подвійної двокрапки (fe80::200:f8ff:fe21:67cf). Такий пропуск може бути єдиним в адресі.

... Загальні уявлення про кіберпростір



**КІБЕРПРОСТІР —
це**

***чітко
визначена та
впорядкована
система
координат***

Суб'єкти відносин в кіберсфері

Суб'єктами відносин, пов'язаних із захистом інформації в системах, є:

- 1) володільці інформації – **власники або користувачі;**
- 2) власники системи – **оператори/провайдери;**
- 3) користувачі – **споживачі телекомунікаційних послуг;**
- 4) спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації і підпорядковані йому регіональні органи

ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах» (1994)

Впорядкування інтернет простору

IANA (адміністрація адресного простору Інтернету)

ця структура підпорядковується безпосередньо ICANN і займається контролем IP-адрес у всьому світі.

В її завдання входить розподілення IP-адрес і номерів AS між регіонами планети Земля.

Але розподіляє вона не аби кому, а тільки конкретним організаціям, які є головними в своєму регіоні, їх називають RIR

Впорядкування інтернет простору

РЕГІОНАЛЬНІ ІНТЕРНЕТ РЕЄСТРАТОРИ



... Правила реєстрації в мережі Інтернет

✓ **Правила RIPE** - правила щодо номерних ресурсів Інтернету, розроблені, затверджені і опубліковані RIPE NCC відповідно до порядку, встановленого документом «Порядок розробки правил в RIPE», доступним за адресою <http://www.ripe.net>



Місцеві реєстратори IP



LIR ом може стати будь-який бажаючий і який готовий платити гроші, раніше щоб стати LIR, потрібно було взяти 4096 IP-адрес.

LIRи діляться на п'ять категорій, залежно від кількості IP-адрес, які у них є:

Extra Large, Large, Medium, Small і **Extra Small**. Категорію привласнює

RIR.NIR є тільки в деяких країнах, наприклад, в Китаї, N - національний.

Провайдери телекомунікаційних послуг



ПРОВАЙДЕР ТЕЛЕКОМУНІКАЦІЙ - суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій без права на технічне обслуговування та експлуатацію телекомунікаційних мереж і надання в користування каналів електрозв'язку;

*ЗУ «Про телекомунікації» (2004)
втратив силу*

Оператор телекомунікаційних послуг



ОПЕРАТОР ТЕЛЕКОМУНІКАЦІЙ - суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій із правом на технічне обслуговування та експлуатацію телекомунікаційних мереж;

*ЗУ «Про телекомунікації» (2004)
втратив силу*

Реєстр операторів та провайдерів



Сайт НКРЗІ

Впорядкування інтернет простору

01.01.2022 втратив силу Закон України «Про телекомунікації»

слова "оператор телекомунікацій", "провайдер або оператор телекомунікацій" у всіх відмінках і числах замінити словами "**постачальник електронних комунікаційних послуг**" у відповідному відмінку та числі

*Чинний ЗУ «Про електронні комунікації»
з 01.01.2022*

Зберігання інформації в кіберпросторі

ПОСТАЧАЛЬНИК ПОСЛУГ ХОСТИНГУ -



особа, яка надає власникам веб-сайтів послуги і (або) ресурси для розміщення веб-сайтів або їх частин у мережі Інтернет та із забезпечення доступу до них через мережу Інтернет.

Власник веб-сайту, який розміщує свій веб-сайт або його частину в мережі Інтернет на власних ресурсах і (або) самостійно забезпечує доступ до нього з використанням мережі Інтернет, одночасно є постачальником послуг хостингу;

*ЗУ «Про авторське право і суміжні права»
(1994)*

Зберігання інформації в кіберпросторі

ДОМЕННЕ ІМ'Я

- ім'я, що використовується для адресації комп'ютерів і ресурсів в Інтернеті.

У Whois легко перевірити, коли був зареєстрований домен – дізнатися дату реєстрації домену можна в поле «created», час та дату внесення змін «modified», дату закінчення використання (expires), а також джерело даних (source) тощо.

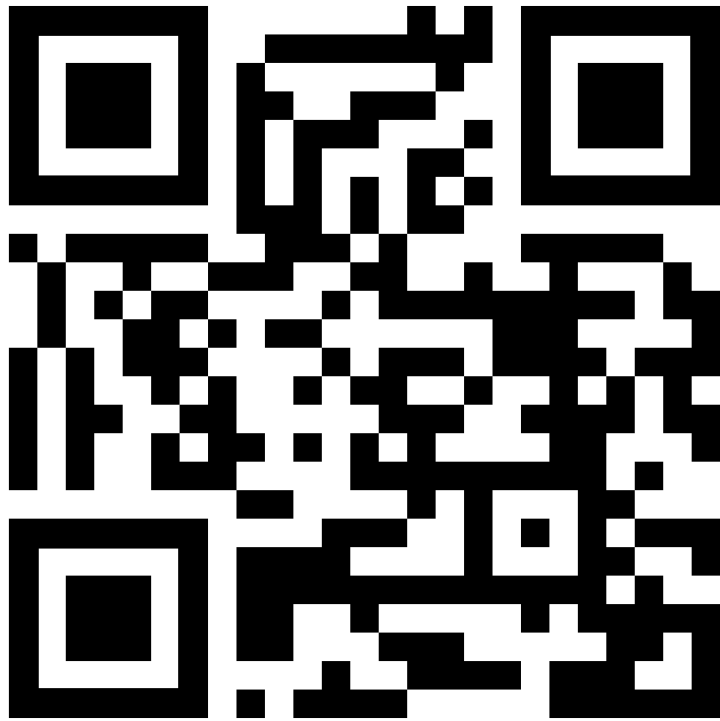
Сервіси:

<https://who.is>

<https://2ip.ru>

«Машина часу» в кіберпросторі

Історія веб-ресурсів



В Інтернеті зберігається інформація що була опублікована раніше.

<https://web.archive.org/>

Загальні уявлення про кіберпростір



**КІБЕРПРОСТІР –
це**

*постачальники
послуг
доступу до
мережі
інтернет та
супутніх послуг*

Програмне забезпечення призначене для обробки інформації

КОМП'ЮТЕРНА ПРОГРАМА -

```
1 sub Calculator()
2   sub addition(self, other)
3     return self + other
4   end
5
6   /** Create a list of 2 numbers. */
7   sub makeFraction(numerator, denominator)
8     return [numerator, denominator]
9   end
10
11   /** Warning: Destroys original fraction! */
12   sub multiplyFracs(frac, otherFrac)
13     frac[0] *= otherFrac[0]
14     frac[1] *= otherFrac[1]
15     return frac
16   end
17 end
18
19 sub InfinityCalculator() ← Class
20   inherit Calculator()
21   /** Create a list of 2 numbers. */
22   sub makeFraction(numerator, denominator)
23     if denominator == 0
24       /* The user is trying to divide by 0.
25        * Use Java's way of handling this: */
26       import math into mathematics
27       return mathematics.INFINITY
28     end
29     return [numerator, denominator]
30   end
31 end
```

набір інструкцій у вигляді слів, цифр, кодів, схем, символів чи у будь-якому іншому вигляді, виражених у формі, придатній для зчитування комп'ютером, які приводять його у дію для досягнення певної мети або результату (це поняття охоплює як операційну систему, так і прикладну програму, виражені у вихідному або об'єктному кодах);

ЗУ «Про розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних» (2000)

Програмне забезпечення призначене для обробки інформації

Мова програмування - це штучна мова, створена для передачі команд машинам, зокрема комп'ютерам.



Програмне забезпечення призначене для обробки інформації

Перша програма програміста «Привіт, світ!»

```
<meta charset="utf-8">
<script>
    alert("Hello, world!");
</script>
```

```
00000000  7f 45 4c 46 01 01 01 00  00 00 00 00 00 00 00 00  |.ELF.....|
00000010  02 00 03 00 01 00 00 00  54 80 04 08 34 00 00 00  |.....T...4...|
00000020  00 00 00 00 00 00 00 00  34 00 20 00 01 00 00 00  |.....4. ....|
00000030  00 00 00 00 01 00 00 00  00 00 00 00 00 80 04 08  |.....|
00000040  00 80 04 08 74 00 00 00  74 00 00 00 05 00 00 00  |....t...t.....|
00000050  00 10 00 00 b0 04 31 db  43 b9 69 80 04 08 31 d2  |.....1.C.i...1.|
00000060  b2 0b cd 80 31 c0 40 cd  80 48 65 6c 6c 6f 20 77  |....1.@..Hello w|
00000070  6f 72 6c 64                                     |orld|
00000074
```

Програмне забезпечення призначене для обробки інформації

«Існують три види брехні: брехня, нагла брехня та статистика», [англ.](#) *There are three kinds of lies: lies, damned lies, and statistics*)

Цифри оманливі, особливо коли я сам займаюся ними; з цього приводу справедливе висловлювання, що приписується Дізраелі: «Існує три види брехні: брехня, нагла брехня і статистика».

Марк Твен, 5 липня 1907 р.

... Загальні уявлення про кіберпростір



**КІБЕРПРОСТІР –
це**

***програмне
забезпечення***

Об'єкти кібербезпеки

Об'єктами кібербезпеки є:

- 1) конституційні права і свободи людини і громадянина;
- 2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;
- 3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;
- 4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;
- 5) об'єкти критичної інфраструктури.

Об'єкти кіберзахисту

Об'єктами кіберзахисту є:

1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;

Об'єкти кіберзахисту

Об'єктами кіберзахисту є:

2) об'єкти критичної інформаційної інфраструктури;

3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

Суб'єкти забезпечення кібербезпеки

1. Координація діяльності у сфері кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України.

Суб'єкти забезпечення кібербезпеки

2. Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України.

Суб'єкти забезпечення кібербезпеки

3. Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (крім об'єктів критичної інфраструктури у банківській системі України).

Суб'єкти забезпечення кібербезпеки

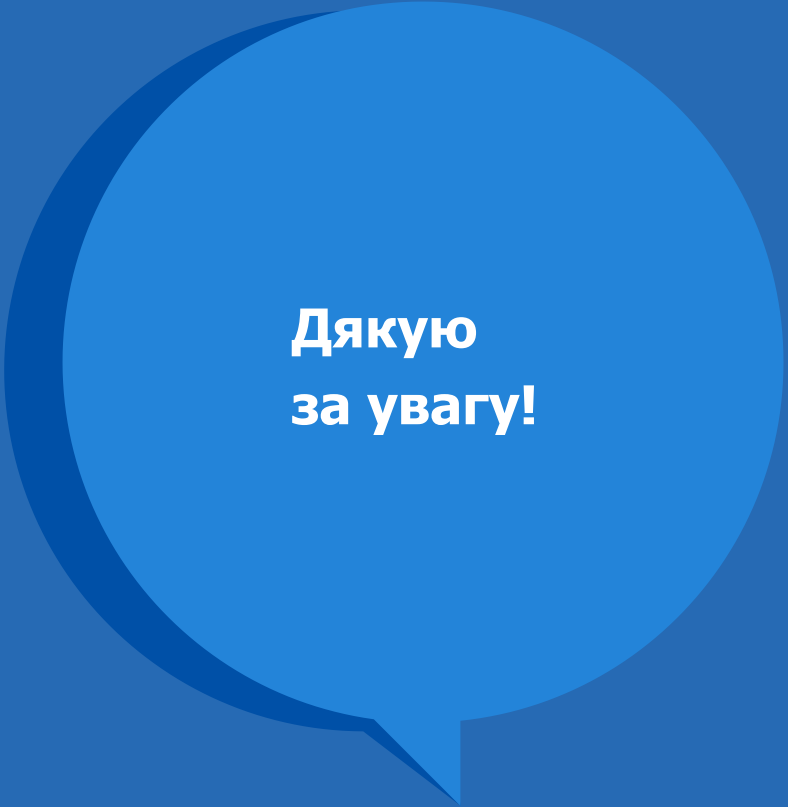
Суб'єктами, які **безпосередньо** здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є:

- 1) міністерства та інші центральні органи виконавчої влади;
- 2) місцеві державні адміністрації;
- 3) органи місцевого самоврядування;
- 4) правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності;
- 5) Збройні Сили України, інші військові формування, утворені відповідно до закону;
- 6) Національний банк України;
- 7) підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури;
- 8) суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

Суб'єкти забезпечення кібербезпеки

Суб'єкти забезпечення кібербезпеки у межах своєї компетенції:

- 1) здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях;
- 2) здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;
- 3) здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз;
- 4) розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту;
- 5) забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління;
- 6) здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору.



**Дякую
за увагу!**