Урок №2. **Тема. Інформація та інформаційні відносини. Суб'єкти інформаційних відносин, їх інтереси та безпека, шляхи нанесення їм шкоди. Безпека інформаційних технологій**

https://learningapps.org/watch?v=poms1j7xc19

*5.*Побудувати демократичну, правову державу неможливо в закритому суспільстві. На сучасному етапі розвиток інформатизації соціуму визначає темпи його розвитку. Тому інформаційні відносини стають об'єктом правового регулювання і насамперед конституційного законодавства. Це підкреслює роль інформації для держави й суспільства. Виходячи з цих міркувань, є всі підстави вважати, що відносини щодо інформації, її збору, використання і поширення мають бути предметом як правової регламентації з боку конституційного права, так і науки конституційного права і навчальної дисципліни.

**Інформаційні відносини** — суспільні відносини, які виникають при збиранні, одержанні, зберіганні, використанні, поширенні та захисту (охороні) інформації.

*6.* Найважливішими **компонентами інформаційної діяльності** є:

* інформація та інформаційні системи;
* суб’єкти-учасники інформаційних процесів;
* правові відносини виробників – споживачів інформаційної продукції.

*7*. **Інформація, що захищається** — це інформація, що є предметом власності.

**Інформація з обмеженим доступом** - інформація, право доступу до якої обмежено встановленими правовими нормами і (чи) правилами.

**Таємна інформація** - інформація з обмеженим доступом, яка містить відомості, що становлять державну або іншу передбачену законом таємницю.

**Конфіденційна інформація** - інформація з обмеженим доступом, якою володіють, користуються чи розпоряджаються окремі фізичні чи юридичні особи або держава (авторизовані суб'єкти системи). Для інших суб'єктів системи ця інформація повинна бути невідомою.

*8.* **Основними принципами інформаційних відносин є:**

* гарантованість права на інформацію;
* відкритість, доступність інформації, свобода обміну інформацією;
* достовірність і повнота інформації;
* свобода вираження поглядів і переконань;
* правомірність одержання, використання, поширення, зберігання та захисту інформації;
* захищеність особи від втручання в її особисте та сімейне життя.

*9*. У якості **об'єктів інформаційної безпеки** (information security object) необхідно розглядати: інформацію та інформаційні ресурси, носії інформації, процеси обробки інформації.

*10.* **Суб'єкти інформаційних відносин** — фізичні та юридичні особи, об'єднання громадян та суб'єкти, наділені владними повноваженнями з метою забезпечення та реалізації своїх прав та свобод в інформаційній та інших сферах життєдіяльності суспільства.

- Хто може бути суб’єктом інформаційних відносин?

- Чи можете Ви бути суб’єктом інформаційних відносин?

*11.* Відповідно до **Закону «Про інформацію**» (ст. 9) всі громадяни України, юридичні особи і державні органи мають право на інформацію, що передбачає можливість вільного одержання, використання і поширення та зберігання відомостей, необхідних їм для реалізації ними своїх прав, свобод і законних інтересів, здійснення завдань і функцій.

<https://zakon.rada.gov.ua/laws/show/2657-12>

*12.* Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «**Про Доктрину інформаційної безпеки України».**

Основні тези:

* захист українського суспільства від агресивного інформаційного впливу, спрямованого на пропаганду війни, розпалювання національної і релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України;
* захист українського суспільства від агресивного впливу деструктивної пропаганди;
* всебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності у доступі до достовірних та об’єктивних відомостей.

<https://zakon.rada.gov.ua/laws/show/47/2017>

*13.* **Право вільного одержання інформації** — це набуття, придбання, накопичення відповідно до чинного законодавства України документованої або публічно оголошуваної інформації громадянами, юридичними особами або державою. **Використання інформації** — це задоволення інформаційних потреб громадян, юридичних осіб і держави. **Поширення інформації** — це розповсюдження, обнародування, реалізація в установленому законом порядку документованої або публічно оголошуваної інформації. **Зберігання інформації** — це забезпечення належного стану інформації та її матеріальних носіїв.

Реалізація права на інформацію громадянами, юридичними особами і державою не повинна порушувати громадянські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб.

*14.* Під **безпекою інформації** розуміють захищеність інформації та інфраструктури, що її підтримує, від випадкових або навмисних впливів природного або штучного характеру, здатних завдати шкоди безпосередньо даним, їхнім власникам і користувачам інформації та інфраструктурі, що підтримує інформаційну безпеку.

*15*. Базовими **принципами інформаційної безпеки** є забезпечення цілісності інформації, її конфіденційності й водночас доступності для всіх авторизованих користувачів.

*16*. **Загроза інформаційної безпеки** — сукупність умов і факторів, що створюють небезпеку порушення інформаційної безпеки.

Під загрозою (в загальному) розуміється потенційно можлива подія, дія (вплив), процес або явище, які можуть призвести до нанесення шкоди чиїм-небудь інтересам.

Під загрозою інтересів суб'єктів інформаційних відносин розуміють потенційно можливу подію, процес або явище, яке з допомогою впливу на інформацію або інші компоненти інформаційної системи, може прямо або опосередковано призвести до нанесення шкоди інтересам даних суб'єктів.

*17.* **Загрози інформації**

Відповідно до властивостей інформації, виділяють такі загрози її [безпеці](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0):

загрози цілісності:

* знищення;
* модифікація;

загрози доступності:

* блокування;
* знищення;

загрози конфіденційності:

* несанкціонований доступ (НСД);
* витік;
* розголошення.

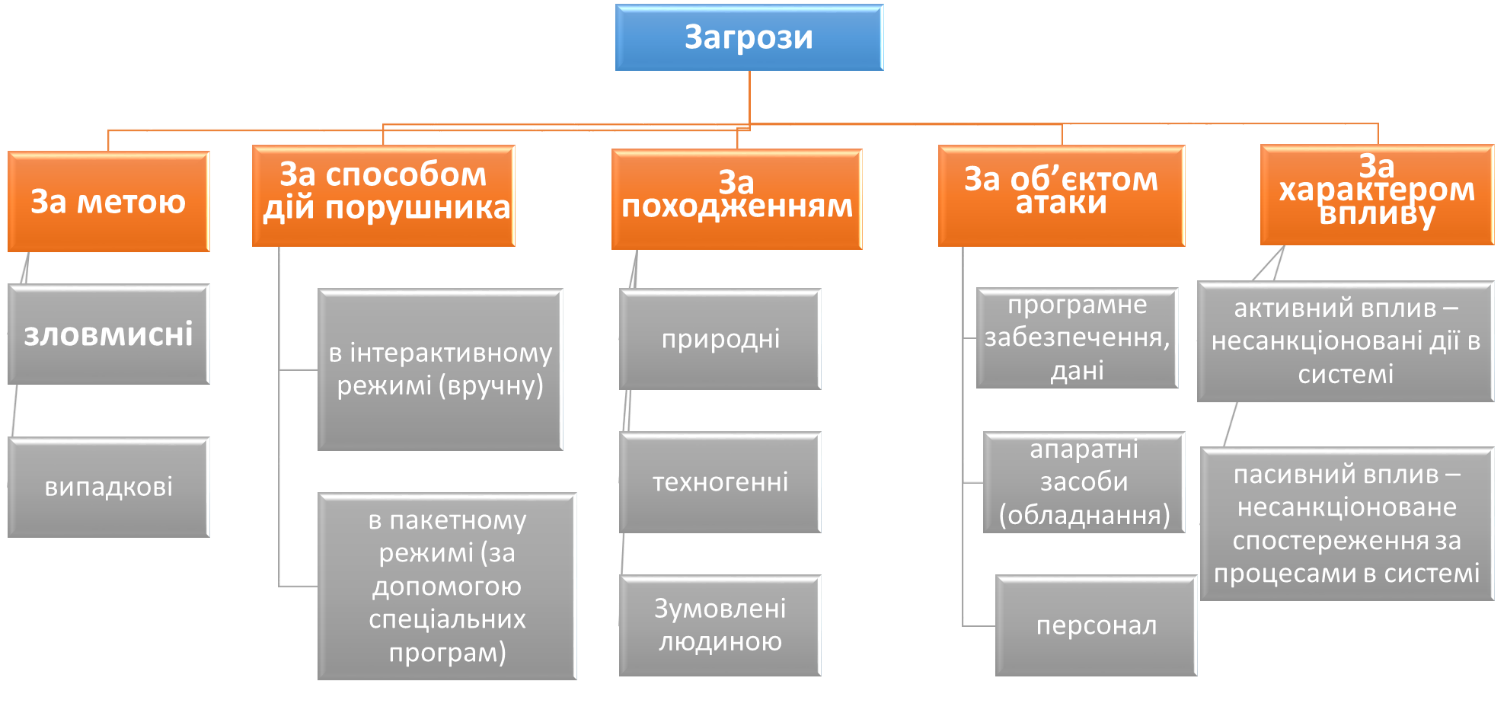
*18.* Із цього погляду основними випадками порушення безпеки інформації можна назвати такі:

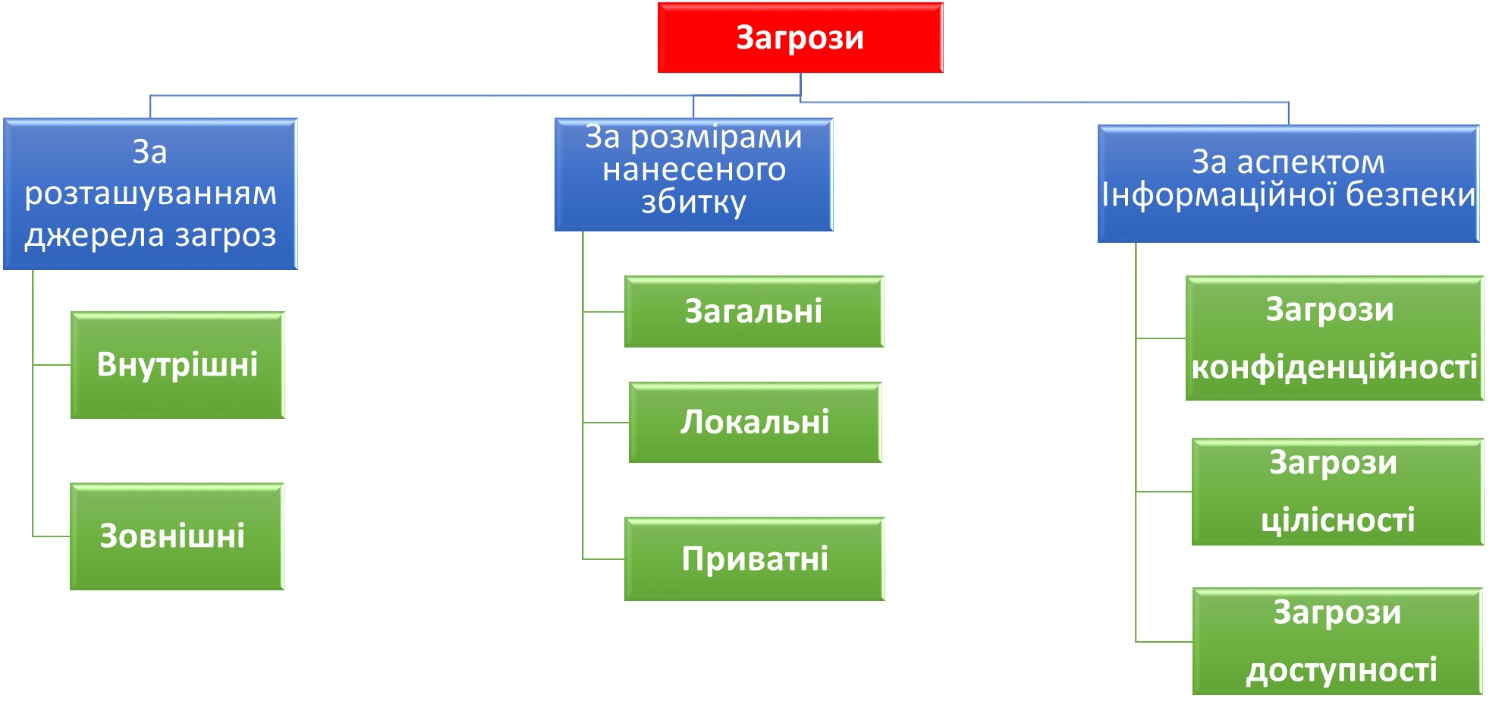
* **несанкціонований доступ** — доступ до інформації, що здійснюється з порушенням установлених в ІC правил розмежування доступу;
* **витік інформації** — результат дій порушника, унаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї;
* **втрата інформації** — дія, внаслідок якої інформація в ІC перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі;
* **підробка інформації** — навмисні дії, що призводять до перекручення інформації, яка має оброблятися або зберігатися в ІC;
* **блокування інформації** — дії, наслідком яких є припинення доступу до інформації;
* **порушення роботи ІC** — дії або обставини, які призводять до спотворення процесу обробки інформації.

*19.* **Причини порушення інформаційної безпеки:**

* **збої обладнання** (збої кабельної системи, перебої в електроживленні, збої серверів, робочих станцій, мережних карт, дискових систем тощо);
* **некоректна робота програмного забезпечення** (втрата або змінювання даних у разі помилок у ПЗ, втрати даних унаслідок зараження системи комп'ютерними вірусами тощо);
* **навмисні дії сторонніх осіб** (несанкціоноване копіювання, знищення, підробка або блокування інформації, порушення роботи ІC, спричинення витоку інформації);
* **помилки обслуговуючого персоналу та користувачів** (випадкове знищення або змінювання даних; некоректне використання програмного та апаратного забезпечення, яке призводить до порушення нормальної роботи системи, виникнення вразливих місць, знищення або змінювання даних, порушення інтересів інших законних користувачів тощо; неефективно організована система захисту; втрата інформації через неправильне зберігання архівних даних тощо);
* **навмисні дії обслуговуючого персоналу та користувачів** (усе сказане у попередніх двох пунктах, а також ознайомлення сторонніх осіб із конфіденційною інформацією).

Зауважимо, що порушенням безпеки можна вважати і дії, які не призводять безпосередньо до втрати або відпливу інформації, але передбачають втручання в роботу системи.

*20.* **Класифікація загроз** **

*21.* **Класифікація загроз****

**V. Фізкультхвилинка**

**VІ. Усвідомлення набутих знань та формування вмінь і навичок**

* ***Практичне завдання***

1. Увійдіть у ваш обліковий запис Google.
2. Відкрийте Google-диск.
3. Складіть карту знань із класифікацією загроз інформаційній безпеці.
4. Надайте доступ учителеві.

*Вправа для профілактики короткозорості та порушення зору*

Не працювати є причина –

Очам даємо відпочинок!

Мерщій рівнесенько сідаймо.

Очима кліпать починаймо.

Навіщо кліпать? Така зарядка-

Вже краще бачать оченятка!

**VII. Підведення підсумків уроку**

* ***Бесіда за питаннями*** *)*

1. Інформаційні відносини - це…
2. Об’єкт і суб’єкт інформаційних відносин – в чому різниця?
3. Назвіть компоненти інформаційних відносин.
4. Назвіть основні причини порушень інформаційної загрози.
5. Інформаційна безпека - це…
6. Назвіть основні класифікації інформаційних загроз.

[**https://learningapps.org/watch?v=pkkpo8nfc19**](https://learningapps.org/watch?v=pkkpo8nfc19)

**VIII. Домашнє завдання**

*27.* Створити колективну Google-презентацію:

*1 група – повідомлення про загрози цілісності;*

*2 група – повідомлення про загрози конфіденційності;*

*3 група – повідомлення про загрози доступності;*

Представлення презентації з виступом повинно займати 2-3 хв.

Надати доступ учителеві.