ІНФОРМАЦІЙНА БЕЗПЕКА ОСОБИСТОСТІ

1.Поннятя про інформаційну безпеку

2. Історія інформаційної безпеки

3.Види інформаційної безпеки

4.Загрози інформаційній безпеці

5. Властивості інформації

6. ІНФОРМАЦІЙНА БЕЗПЕКА – ВАЖЛИВА СКЛАДОВА ОБОРОНИ ДЕРЖАВИ

Інформаційна безпека

пооняття *інформаційної безпеки* можна разглядати у декількох ракурсах. По-перше, це стан захищенності інформаційного середовища суспільства, який забезпечує його формування, використання й розвиток в інтересах громадян, організацій, держави.

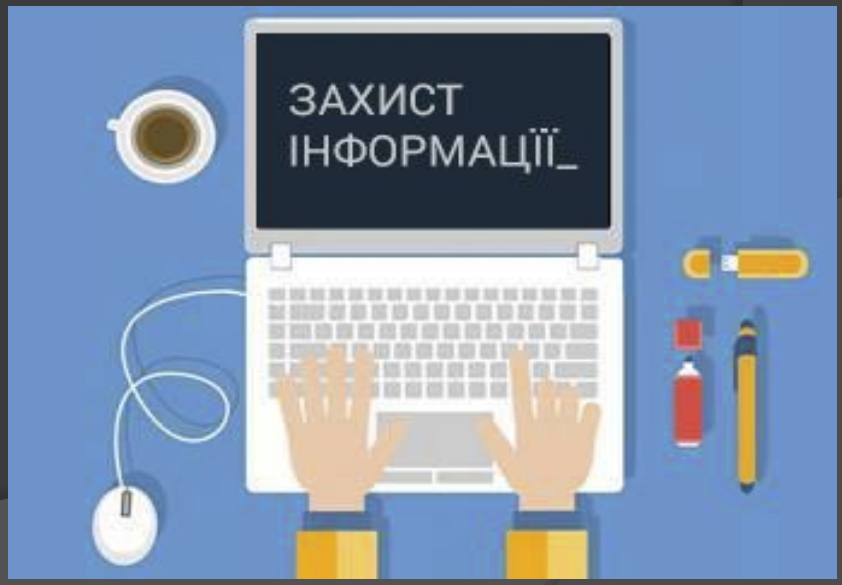
Під *інформаційним середовищем* розуміють сферу діяльності суб'єктів, пов'язану із створенням, обробленням й споживанням інформації.

По-друге, *інформаційна безпека* – це стан захищенності потреб в інформації особи, суспільства й держави, при якому забезпечується їхнє існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз. Стан інформованості визначає ступінь адекватності сприйняття суб'єктами навколишньої дійсності і як наслідок – обгрунтованість рішень і дій, що приймаються.

В інформаційному праві інформаційна безпека – це одна із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позиції захисту життєво важливих інтересів особистості, суспільства, держави і акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами.

Об'єктами інформаційної безпекиможуть бути: свідомість, психіка людини; інформаційні системи різного масштабу й різного призначення. До соціальних об'єктів інформаційної безпеки відносять особистість, колектив, державу, суспільство, світове товариство.

До **суб'єктів інформаційної безпеки** належать: держава, що здійснює свої функції через відповідні органи; громадяни, суспільні або інші організації і об'єднання, що володіють повноваженнями щодо забезпечення інформаційної безпеки відповідно до законодавства.



Історія

Об'єктивно категорія «інформаційна безпека» виникла з появою засобів інформаційних комунікацій між людьми, а також з усвідомленням людиною наявності у людей і їхніх співтовариств інтересів, яким може бути завдано збитку шляхом дії на засоби інформаційних комунікацій, наявність і розвиток яких забезпечує і задає інформаційний обмін між всіма елементами соціуму. Враховуючи вплив на трансформацію ідей інформаційної безпеки, в розвитку засобів інформаційних комунікацій можна виділити декілька етапів[2]:

I етап — до 1816 року — характеризується використанням природно виникаючих засобів інформаційних комунікацій. В цей період основне завдання інформаційної безпеки полягало в захисті відомостей про події, факти, майно, місцезнаходження і інші дані, що мають для людини особисто або співтовариства, до якого вона належала, життєве значення.

II етап — починаючи з 1816 року — пов'язаний з початком використання штучно створюваних технічних засобів електро- і радіозв'язку. Для забезпечення скритності і перешкодостійкості радіозв'язку необхідно було використовувати досвід першого періоду інформаційної безпеки на вищому технологічному рівні, а саме застосування перешкодостійкого кодування повідомлення (сигналу) з подальшим декодуванням прийнятого повідомлення (сигналу).

III етап — починаючи з 1935 року — пов'язаний з появою засобів радіолокацій і гідроакустики. Основним способом забезпечення інформаційної безпеки в цей період було поєднання організаційних і технічних заходів, направлених на підвищення захищеності засобів радіолокацій від дії на їхні приймальні пристрої активними маскуючими і пасивними імітуючими радіоелектронними перешкодами.

IV етап — починаючи з 1946 року — пов'язаний з винаходом і впровадженням в практичну діяльність електронно-обчислювальних машин (комп'ютерів). Завдання інформаційної безпеки вирішувалися, в основному, методами і способами обмеження фізичного доступу до устаткування засобів добування, переробки і передачі інформації.

V етап — починаючи з 1965 року — обумовлений створенням і розвитком локальних інформаційно-комунікаційних мереж. Завдання інформаційної безпеки також вирішувалися, в основному, методами і способами фізичного захисту засобів добування, переробки і передачі інформації, об'єднаних в локальну мережу шляхом адміністрування і управління доступом до мережевих ресурсів.

VI етап — починаючи з 1973 року — пов'язаний з використанням надмобільних комунікаційних пристроїв з широким спектром завдань. Загрози інформаційній безпеці стали набагато серйознішими. Для забезпечення інформаційної безпеки в комп'ютерних системах з безпровідними мережами передачі даних потрібно було розробити нові критерії безпеки. Утворилися співтовариства людей — хакерів, що ставлять собі за мету нанесення збитку інформаційній безпеці окремих користувачів, організацій і цілих країн. Інформаційний ресурс став найважливішим ресурсом держави, а забезпечення його безпеки — найважливішою і обов'язковою складовою національної безпеки. Формується інформаційне право — нова галузь міжнародної правової системи.

VII етап — починаючи з 1985 року — пов'язаний із створенням і розвитком глобальних інформаційно-комунікаційних мереж з використанням космічних засобів забезпечення. Можна припустити що черговий етап розвитку інформаційної безпеки, очевидно, буде пов'язаний з широким використанням надмобільних комунікаційних пристроїв з широким спектром завдань і глобальним охопленням у просторі та часі, забезпечуваним космічними інформаційно-комунікаційними системами. Для вирішення завдань інформаційної безпеки на цьому етапі необхідним є створення макросистеми інформаційної безпеки людства під егідою ведучих міжнародних форумів.

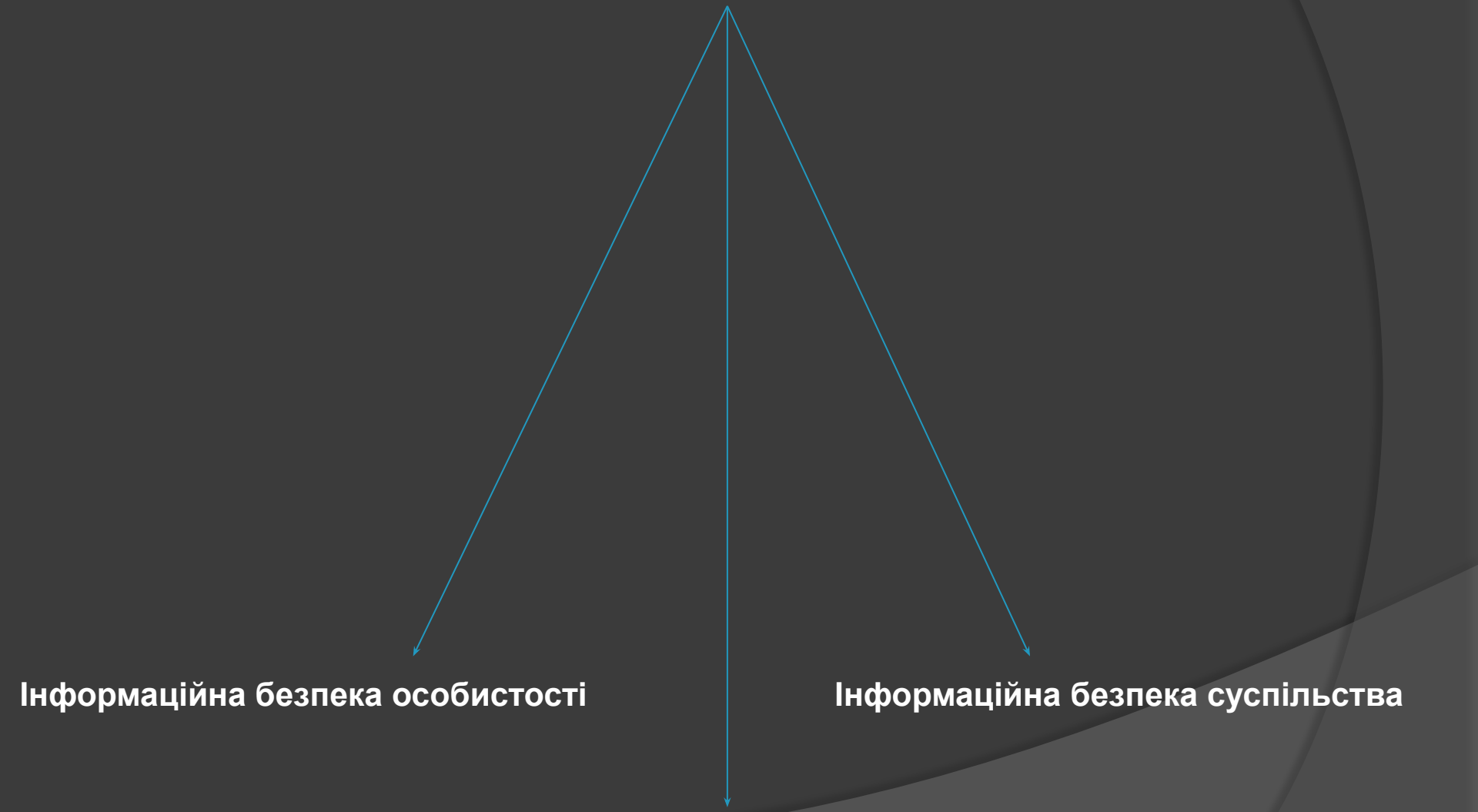
Види інформаційної безпеки

Інформаційна безпека особистості – це захищенність психіки й свідомості людини від небезпечних інформаційних впливів: маніпулювання свідомістю, дезінформування, спонукання до образ, самогубства тощо.

Інформаційна безпека держави характеризується мірою захищенності держави (суспільства) та стійкості основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи тощо) відносно небезпечних (дестабілізуючих) інформаційних впливів, причому як з упровадження, так і добування інформації. Інформаційна безпека держави визначається здатністю нейтралізувати такі впливи. Концепція інформаційної безпеки держави – це систематизована сукупність відомостей про інформаційну безпеку держави та шляхи її забезпечення. В рамках цієї концепції проводиться системна класифікація дестабілізуючих факторів та інформаційних загроз безпеці особистості, суспільства, держави; обгрунтовуються основні положення з організації забезпечення інформаційної безпеки держави; розробляються пропозиції щодо способів і форм забезпечення інформаційної безпеки.

Види інформаційної безпеки

Інформаційна безпека



Інформаційна безпека особистості

Інформаційна безпека суспільства

Інформаційна безпека держави

Загрози інформаційній безпеці

Загрози інформаційній безпеці – сукупність умов і факторів, що створюють небезпеку життєвоважливим інтересам особистості, суспільства й держави в інформаційній сфері. Основні загрози інформаційній безпеці поділяють на три групи:
- загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу;
- загрози несанкціонованого й неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (їх виробництво, системи формування й використання);
- загрози інформаційним правам і свободам особистості (праву на виробництво інформації, її поширення, пошук, одержання, передавання та використання; праву на інтелектуальну власність на інформацію, в тому числі й речову).

Фактори загроз за видовою ознакою поділяються на політичні, економічні і організаційно-технічні.

Явища та процеси природного й штучного походження, що породжують інформаційні загрози, називають *дистабілізуючими факторами.*

Джерелами дестабілізуючих факторів можуть бути як окремі особи, так й організації і їхні об'єднання. Особливу групу джерел складають інформаційні системи та засоби, оскільки вони одночасно є знаряддям приведення в дію інформаційних загроз, каналом їхнього проникнення у свідомість особистості або суспільну свідомість і генератором спонтанних загроз, що виникають внаслідок технічних несправностей та інших причин.

Джерелом дестабілізуючих факторів може бути також природне середовище. Кожному джерелу властиві певні види дестабілізуючих факторів, які можна подати у вигляді міждержавних і внутрішньодержавних.

До *внутрішньодержавних* дестабілізуючих факторів відносять: правовий вакуум у більшості питань забезпечення інформаційної безпеки; порушення законодавства з питань інформаційної безпеки; політичні конфлікти; відмови, збої, технічні помилки інформаційних систем (засобів); природні явища, що ускладнюють передачу, прийом і зберегання інформації або руйнують інформаційні системи.

*Міждержавні*дестабілізуючі фактори – це конфлікти різноманітних масштабів і проявів (в економіці, політиці, ідеології, дипломатії тощо).

Загрози інформаційній безпеці
information security threat

- сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства та держави в інформаційній сфері

Класифікація факторів загроз за видовою ознакою

- Політичні фактори загроз інформаційній безпеці
- Економічні фактори загроз інформаційній безпеці
- Організаційно-технічні фактори загроз інформаційній безпеці

Ієрархічна класифікація факторів загроз

- Глобальні фактори загроз інформаційній безпеці
- Регіональні фактори загроз інформаційній безпеці
- Локальні фактори загроз інформаційній безпеці

Властивості інформації

Для характеристики основних властивостей інформації як об'єкта захисту часто використовується **модель CIA**:
Конфіденційність (англ. *confidentiality*) — властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем
Цілісність (англ. *integrity*) — означає неможливість модифікації неавторизованим користувачем
Доступність (англ. *availability*) — властивість інформації бути отриманою авторизованим користувачем, за наявності у нього відповідних повноважень, в необхідний для нього час
Додатково також використовують такі властивості:
Апелювання (англ. *non-repudiation*) — можливість довести, що автором є саме заявлена людина (юридична особа), і ніхто інший.
Підзвітність (англ. *accountability*) — властивість інформаційної системи, що дозволяє фіксувати діяльність користувачів, використання ними пасивних об ‘єктів та однозначно встановлювати авторів певних дій в системі.
Достовірність (англ. *reliability*) — властивість інформації, яка визначає ступінь об'єктивного, точного відображення подій, фактів, що мали місце.
Автентичність (англ. *authenticity*) — властивість, яка гарантує, що суб'єкт або ресурс ідентичні заявленим.


Властивості інформації
Об'єктивність
Зрозумілість
Достовірність
Доступність
Повнота
Корисність
Актуальність

ІНФОРМАЦІЙНА БЕЗПЕКА – ВАЖЛИВА СКЛАДОВА ОБОРОНИ ДЕРЖАВИ

«Найважливішою складовою національної безпеки у сучасному світі є інформаційна безпека, зокрема, безпека кібернетична. В умовах безпрецедентної, цинічної інформаційної війни, яка ведеться проти України, дуже важливо, щоб у державі було строго відпрацьовано системні дії, спрямовані на захист інформаційного простору від викривленої інформації, яка деформує ментальність громадян, створює високі ризики для економічної стабільності, державності і територіальної цілісності України», - таке заявив з парламентської трибуни, голова парламентського об'єднання «Економічний розвиток", президент УСПП Анатолій Кінах. За його словами, мова йде, зокрема, про складні комплекси стратегічних об'єктів України, починаючи з атомної енергетики.

Об'єднання «Економічний розвиток» наполягає на якнайшвидшому затвердженні парламентом **«**Рекомендацій парламентських слухань на тему: "Законодавче забезпечення розвитку інформаційного суспільства в Україні".У цьому документі, містяться напрацьовані депутатами та експертами рекомендації щодо системи державної політики у галузі інформаційного суспільства, інформаційної та кібербезпеки і освіти у галузі ІКТ, кадрового забезпечення розвитку ІТ-сфери, технічного забезпечення розвитку інформаційного суспільства, розвитку українського сегменту мережі Інтернет та наукового забезпечення Кабінету Міністрів України.

Зокрема, у документі міститься заклик до КМУ розробитиіподати на розгляд парламентубазовий законодавчий акт у системі захисту інформації - Закон України "Про кібернетичну безпеку».

«Україна має величезний кадровий потенціал в ІТ-сфері, сучасні системи та засоби телекомунікацій і зв'язку. Але без підтримки держави ці галузі загальмують у розвитку, особливо - на тлі потужної конкуренції збоку закордонних компаній. Не варто забувати, що інформаційно-комунікаційні технології окрім численних зисків несуть в собі і ризики. Адже в Україні і досі немає чіткої державної політики розвитку ІТ-сфери, а це уже передумови до виникнення залежності від іноземної продукції»,- вважає А.Кінах.

Дякую за увагу

Сподіваюсь що вам сподобалось

Тепер вони допоможуть вам з інформаційною безпекою

<(￣ ﹀ ￣)>