Урок 1.

Основні поняття в області безпеки інформаційних технологій. Місце і роль автоматизованих систем в управлінні бізнес-процесами. Основні причини загострення проблеми забезпечення безпеки інформаційних технологій. Інформація та інформаційні відносини. Суб'єкти інформаційних відносин, їх інтереси та безпека, шляхи нанесення їм шкоди. Безпека інформаційних технологій.

Основні поняття в області безпеки інформаційних технологій.

Точного наукового визначення поняття інформація немає, але:

Під інформацією розуміють

- *відомості про об'єкти, процеси та явища*

Інформація

- *данні про людей, предмети, факти, події, явища і процеси незалежно від форми їхнього представлення. Відомо, що інформація може мати різну форму, зокрема, дані, закладені в комп'ютерах, листи, пам'ятні записи, досьє, формули, креслення, діаграми, моделі продукції і прототипи, дисертації, судові документи й ін.*

У галузі інформаційних систем під інформацією розуміють

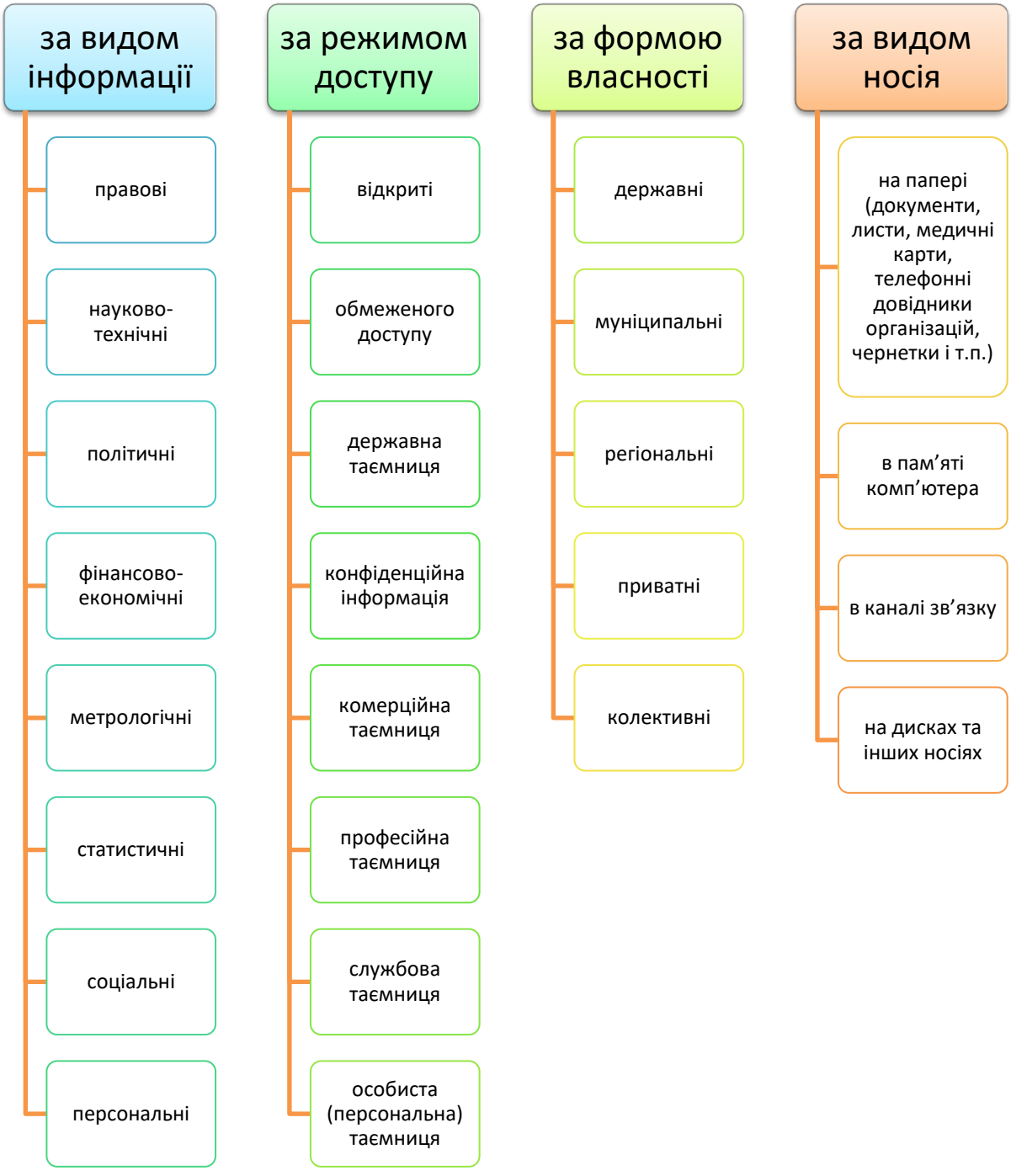
- *відомості, які є об'єктом зберігання, передавання і оброблення. Оскільки інформація представляє інтерес для різних категорій користувачів, то основним призначенням інформації є її використання*

Як і всякий продукт, інформація має споживачів, що потребують її, і тому володіє певними споживчими якостями, а також має і своїх власників або виробників.

Інформаційні ресурси

- *окремі документи та масиви документів, представлені самостійно або в інформаційних системах (бібліотеках, архівах, фондах, базах даних та інших ІС).*

Інформаційні ресурси можна класифікувати:



Інформація, що захищається

- *це інформація, що є предметом власності якого-небудь суб'єкта (держави, відомства, групи осіб або окремого громадянина) і підлягає захисту відповідно до вимог правових документів або вимог, які встановлюються власником інформації.*

Види інформації, які підлягають захисту

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 з обмеженим доступом, якою володіють, користуються чи розпоряджаються окремі фізичні чи юридичні особи або держава і порядок доступу до якої встановлюється ними

Під доступом до інформації розуміється ознайомлення з інформацією, її обробка, зокрема копіювання, модифікація або знищення інформації. Розрізняють санкціонований і несанкціонований доступ до інформації.

Санкціонований доступ до інформації

- це доступ до об’єктів, програм і даних користувачів, що мають право виконувати певні дії, а також права користувачів на використання ресурсів і послуг. Цей доступ не порушує встановлені правила розмежування доступу.

Несанкціонований доступ (НСД) до інформації

- характеризується порушенням встановлених правил розмежування доступу. Це найбільш поширений вид комп’ютерних порушень. Дане поняття також пов’язане з поширенням різного роду комп’ютерних вірусів.

Захист інформації

- це комплекс заходів, спрямованих на забезпечення інформаційної безпеки

Захищена інформація

- інформація, яка не зазнала незаконних змін у процесі передачі, зберігання та збереження, не змінила такі властивості, як достовірність, повнота і цілісність даних

Національна безпека

- це захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам (ст. 1 Закон України „Про основи національної безпеки України").

В інформаційному праві інформаційна безпека

- це одна зі 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.

- Стаття 17 Конституції України задекларувала, що „захист суверенітету і територіальної цілісності України, забезпечення її економічної та Інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу".
- Закон України „Про основи національної безпеки України" від 19 червня 2003 року визначає основні засади державної політики, спрямованої на захист національних інтересів і гарантування в Україні безпеки особи, суспільства і держави від зовнішніх і внутрішніх загроз в усіх сферах життєдіяльності.

Під інформаційним середовищем розуміють сферу діяльності суб'єктів інформаційних відносин, пов'язану зі створенням, пошуком, обробкою, поширенням й споживанням інформації.

У 1988 році американська Асоціація комп'ютерного обладнання оголосила **30 листопада Міжнародним днем захисту інформації** (ComputerSecurityDay). Було зафіксовано першу масову епідемію хробака, якого назвали за іменем його творця — Морріса.

Місце і роль автоматизованих систем в управлінні бізнес-процесами. Основні причини загострення проблеми забезпечення безпеки інформаційних технологій.

Комп'ютери – тільки одна з складових інформаційних систем, і хоча наша увага буде зосереджена в першу чергу на інформації, яка зберігається, обробляється і передається за допомогою комп'ютерів, її безпека визначається всією сукупністю складових і, в першу чергу, найслабкішою ланкою, якою в переважній більшості випадків виявляється людина.

Згідно визначення інформаційної безпеки, вона залежить не тільки від комп'ютерів, але і від інфраструктури, що її підтримує, до якої можна віднести системи електро-, водо- і теплопостачання, кондиціонери, засоби комунікацій і, звичайно, обслуговуючий персонал. Ця інфраструктура має самостійну цінність, але нас цікавитиме лише те, як вона впливає на виконання інформаційною системою своїх функцій.

Автоматизована система (АС)

- організаційно-технічна система, що реалізує інформаційну технологію і об'єднує обчислювальну систему, фізичне середовище, персонал і оброблювану інформацію

Операційна система (ОС)

- сукупність програмно-апаратних засобів, що призначені для обробки інформації. Інформація в АС піддається різним процесам: введення, збереження, обробка, виведення

Найбільш загальними інформаційними процесами, що відбуваються в автоматизованих системах є такі:

інформаційні процесаси

- - інформаційно-довідкове забезпечення;
- - інформаційне забезпечення задач;
- - обслуговування інформаційних баз.

Усі вони реалізуються персоналом за допомогою апаратних засобів, ПЗ та інформаційних баз автоматизованих систем.

Розрізняють два основних напрями технічного захисту інформації в АС

- це захист АС і оброблюваної інформації від несанкціонованого доступу
- та захист інформації від витоку технічними каналами.

Захищена АС:

- АС, що здатна забезпечувати захист інформації, що обробляється, від певних загроз

Захист інформації в АС

- діяльність, спрямована на забезпечення безпеки інформації, що обробляють в АС, і АС в цілому, яка дозволяє запобігти або ускладнити можливість реалізації загроз, а також знизити величину потенціального збитку в результаті реалізації загроз

Комплексна система захисту інформації

- Захист інформації в АС полягає у створенні й підтриманні у працездатному стані системи заходів як технічних (інженерних, програмно-апаратних), так і нетехнічних (правових, організаційних), що дозволяють запобігти або ускладнити можливість реалізації загроз, а також знизити потенційний збиток

Інформація та інформаційні відносини. Суб'єкти інформаційних відносин, їх інтереси та безпека, шляхи нанесення їм шкоди. Безпека інформаційних технологій.

Загальні засади та правове регулювання відносин в сфері інформаційної безпеки

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

Об'єктами інформаційної безпеки є:

- інформаційні права людини і громадянина; свідомість та психіка людини;
- духовні, культурні, історичні, інтелектуальні та матеріальні цінності суспільства, інформаційне середовище й інформаційні ресурси;
- інформаційний суверенітет та недоторканість держави

Суб'єктами забезпечення інформаційної безпеки є:

- Президент України;
- Верховна Рада України;
- Кабінет Міністрів України;
- Рада національної безпеки і оборони України;
- міністерства та інші центральні органи виконавчої влади;
- Національний банк України;
- суди загальної юрисдикції;
- прокуратура України;
- місцеві державні адміністрації та органи місцевого самоврядування;
- Збройні Сили України, Служба безпеки України, Служба зовнішньої розвідки України, Державна прикордонна служба України та інші військові формування, утворені відповідно до законів України;
- громадяни України, об'єднання громадян.

Згідно ст. 7 Закону України „Про основи національної безпеки України" основними реальними та потенційними загрозами національній безпеці України, стабільності в суспільстві в інформаційній сфері на сучасному етапі є:

- прояви обмеження свободи слова та доступу громадян до інформації;
- поширення засобами масової інформації культу насильства, жорстокості, порнографії;
- комп'ютерна злочинність та комп'ютерний тероризм;
- розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;
- намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Основними напрямами державної політики з питань національної безпеки України в інформаційній сфері є (ст. 8):

- забезпечення інформаційного суверенітету України;
- вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;
- активне залучення засобів масової інформації до боротьби з корупцією, зловживаннями службовим становищем, іншими явищами, які загрожують національній безпеці України;
- забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції;
- вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

Таким чином, інформаційна безпека с невід'ємною складовою національної безпеки.
Слід зазначити, що сам термін „інформаційна безпека” нормативно з'явився порівняно нещодавно. В ст. 13 Закону України „Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки” зазначено, що „за умов швидкого розвитку глобального інформаційного суспільства, широкого використання ІКТ у всіх сферах життя особливого значення набувають проблеми інформаційної безпеки”.

Інформаційна безпека

- це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації (ст. 13 Закону).

Життєво важливі інтереси людини, суспільства і держави слід розуміти як сукупність потреб, задоволення яких забезпечує існування та можливість прогресивного розвитку людини, суспільства і держави.
Слід звернути увагу студентів та слухачів на тому, що „комп'ютерна безпека”, як еквівалент або замінник терміну „інформаційна безпека”, уявляється вкрай вузьким. Комп'ютери – це лише одна складових інформаційних систем, і хоча інформація зберігається, обробляється і передається за допомогою комп'ютерів, її безпека визначається всією сукупністю складових і, в першу пергу, найслабкішою ланкою, якою в переважній більшості випадків виявляється людина. До речі лише невелика частина проблем інформаційної безпеки пов'язана із комп'ютерною технікою та комунікаційними технологіями.

Законодавством встановлено, що вирішення проблеми інформаційної безпеки має здійснюватися шляхом:

- створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;
- підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань;
- вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;
- розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

Види інформаційної безпеки:

- інформаційна безпека особистості – це захищеність інформаційних прав людини, механізмів їх реалізації, а також психіки та свідомості. людини від небезпечних інформаційних впливів: нанесення шкоди психічному здоров'ю, маніпулювання свідомістю, дезінформування, спонукання до образ, самогубства тощо;
- інформаційна безпека суспільства – це захищеність духовності, моральних та естетичних ідеалів суспільства, його стабільності та стійкості розвитку від загроз небезпечної, недоброякісної та шкідливої інформації, приховування суспільно важливої інформації тощо;
- інформаційна безпека держави характеризується мірою захищеності держави (суспільства) та стійкості основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи тощо) відносно небезпечних (дестабілізуючих) інформаційних впливів, а також характеризується недоторканістю інформаційних ресурсів з обмеженим доступом, можливістю самостійного формування власних національних інформаційних ресурсів.

Під безпекою ІС розуміється захищеність системи від випадкового або навмисного втручання в нормальний процес її функціонування, від спроб розкрадання (несанкціонованого отримання) інформації, модифікації або фізичного руйнування її компонентів, тобто здатність протидіяти різним підбурює впливів на ІС.

Інформаційне середовище	*•представляється як сукупність інформації, що оточує людину, незалежно від форми її подання (письмовою, усною, графічної)*
Інформаційна загроза	*•потенційна можливість певним чином порушити інформаційну безпеку. Найчастіше ця загроза є наслідком наявності вразливих місць в захисті інформаційних ресурсів або систем. Спроба реалізації інформаційної загрози називається інформаційною атакою*
Інформаційна небезпека	*•обставини, при яких інформація або її похідні можуть вплинути на людину або обставини таким чином, що це призведе до її погіршення або неможливості її функціонування і розвитку. Також під інформаційної небезпекою можна розуміти поява помітною ймовірності настання небажаних подій*
Інформаційний захист	*•процес забезпечення інформаційної безпеки. При цьому варто розуміти, що при якісному забезпеченні процесу інформаційного захисту безпеку буде забезпечена (або зведені до мінімуму небезпеки і загрози). У тому випадку, коли процес забезпечення інформаційного захисту носить формальний або несерйозний характер, безпеку досягнута не буде*
Інформаційна безпека особистості	*•це стан і умови життєдіяльності особистості, при яких реалізуються її інформаційні права і свободи*
Інформаційна безпека суспільства	*•це стан суспільства, в якому йому не може бути завдано істотної шкоди шляхом впливу на його інформаційну сферу*

Інформаційна війна

- *використання і управління інформацією з метою отримання конкурентної переваги над противником. Інформаційна війна може включати в себе збір тактичної інформації, забезпечення безпеки власних інформаційних ресурсів, поширення пропаганди або дезінформації, щоб деморалізувати противника і населення, підрив якості інформації противника і попередження можливості збору інформації противником*

Інформаційний тероризм

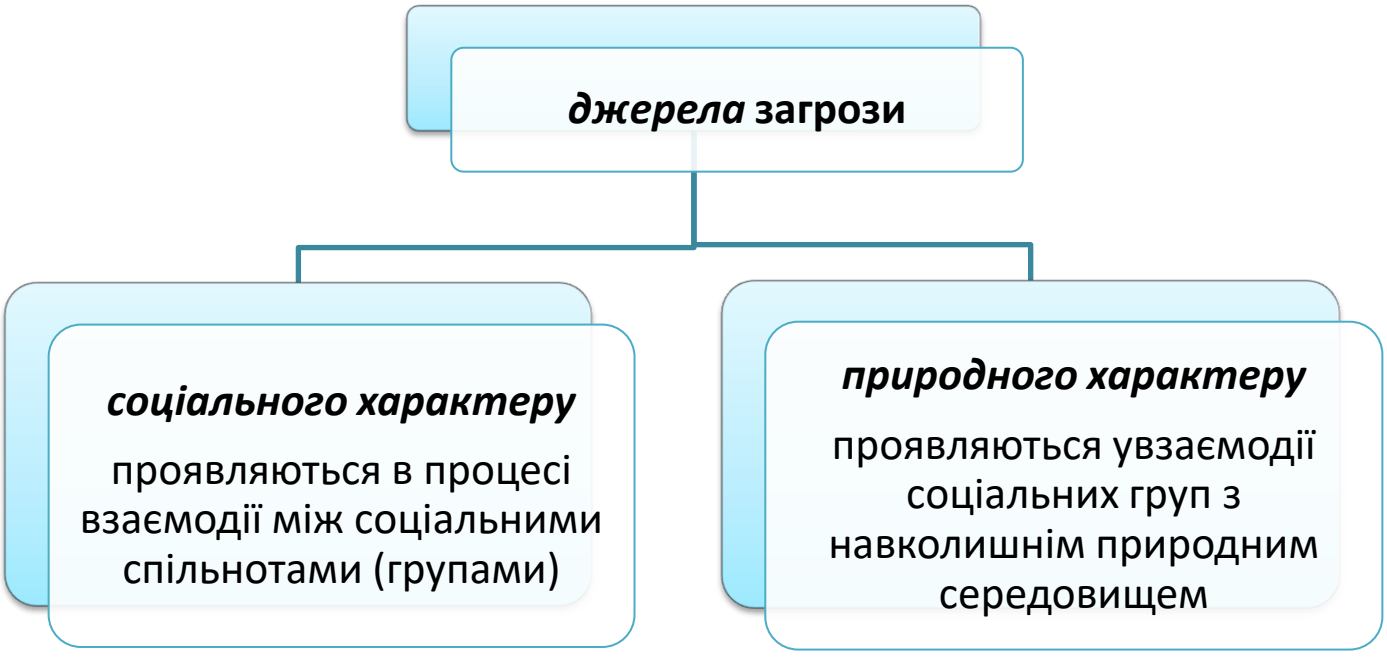
- *гранично небезпечне соціальне явище, спрямоване на дезорієнтацію свідомості людей з метою деструктивного видозміни істинності знань, світогляду і думок мирного населення шляхом застосування інформаційних ресурсів і систем*

Інформаційна залежність

- *залежність від різних джерел інформації, нав'язливе бажання отримувати інформацію будь-яким доступним способом і хвороблива нездатність відмовитися від безперервного отримання інформації усіма можливими способами*

Джерела загроз інформаційній безпеці

- *розуміються як вихідні підстави (причини) небезпечного впливу на життєво важливі інтереси особистості, суспільства і держави в інформаційній сфері*



Залежно від ***характеру прояву*** небезпечного впливу на об'єкти інформаційної безпеки джерела загроз можуть носити зовнішній або внутрішній характер.

До ***зовнішніх джерел*** загроз інформаційної безпеки відносяться:

- діяльність іноземних політичних, економічних, військових, розвідувальних та інформаційних структур
- загострення міжнародної конкуренції за володіння інформаційними технологіями та ресурсами;

До ***внутрішнім джерелам*** загроз інформаційної безпеки відносяться:

- недостатня розробленість нормативної правової бази, що регулює відносини в інформаційній сфері, а також недостатня правозастосовна практика;
- несприятлива криміногенна обстановка, що супроводжується тенденціями зрощування державних і кримінальних структур в інформаційній сфері