5.КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

## *5.1. ОСНОВИ КІБЕРБЕЗПЕКИ (МАМЧЕНКО С.М.)*

### 5.1.1. ПОНЯТТЯ КІБЕРПРОСТОРУ ТА ІНФОРМАЦІЙНОГО ПРОСТОРУ

Загальне ***визначення*** простору та інформаційного простору.

**Простір** [space] це одна з основних форм існування матерії (філос.), яка характеризується протяжністю і обсягом. Відповідно до спеціальної теорії відносності існує тісний зв'язок простору і часу.

На рівні практичного сприйняття під простором розуміють місце, у якому можливий рух. різноманітні положення і розташування об’єктів, відношення близькості-дальності, поняття спрямованості, місце, де відбуваються події і дії. ЩО містить всі місця, об'єкти і структури.

Інформаційний простір [information space] — одне з первинних понять, що не може бути точно визначене. Найчастіше термін розуміють як логічне зіставлення об'єктному (предметному, фізичному, матеріальному) світу. З практичної точки зору вважається, що інформаційний простір — це теж саме, що семантичний простір.

Для практичного застосування краще використати визначення інформаційного простору як будь-якого середовища, де інформація створюється, через яке передається, приймається, в якому зберігається, обробляється і знищується.

*Основними* компонентами інформаційного простору є:

— інформаційні ресурси:
— засоби інформаційної взаємодії:
— інформаційна інфраструктура.

**Основні положення інформаційного простору**

*Інформаційні ресурси*

У загальному випадку під інформаційними ресурсами розуміють результат об'єктивного цілеспрямованого відображення закономірностей і фактів реалізації будь-яких процесів, що відбуваються у суспільстві та в навколишньому середовищі (природі). Вони являють собою сукупність наукових знань, зафіксованих на паперових чи інших носіях.

Класифікація інформаційних ресурсів:

= видам інформації – інформаційні ресурси, що можуть містити формацію наступних видів;

— правову;
— науково-технічну:
— політичну;
— економічну, фінансово-економічну;
— статистичну;
— інформацію про стандарти і регламенти тощо;
— соціальну:

— інформацію про охорону здоров'я:
— інформацію про надзвичайні ситуації:
— особисту інформацію (персональні дані;:
— кадастри (земельний, містобудівний, лісовий, майновий тощо);
— інформацію іншого виду:

за режимом доступу — інформаційні ресурси, що містять відкриту інформацію (без обмежень) або інформацію обмеженого доступу (державну таємницю, конфіденційну інформацію, комерційну таємницю, професійну таємницю, службову таємницю, особисту (персональну; таємницю

за видом носія — інформаційні ресурси, інформація в яких може бути записана на папері, на машино читаних носіях, у вигляді зображення на папері, на екрані ЕОМ, в пам'яті ЕОМ, у каналах зв'язку, на інших носіїв;

за способом формування і розповсюдження — інформаційні ресурси, що знаходяться у стаціонарному або рухомому (мобільному) стані;

за способом організації зберігання і використання — інформаційні ресурси, для зберігання і використання інформації, в яких можуть використовуватися традиційні форми (масиви документів**,** фонди документів**,** архіви) або автоматизовані форми (банки даних, інформаційні системи, бази знань);

за формою власності — інформаційні ресурси, що можуть складати:
— загальнодержавне національне надбання;
— держави}' власність; муніципальну власність;
— приватну власність;
— колективну власність.

**Засоби інформаційної взаємодії**

*Умови інформаційної взаємодії*

Термін «інформація» походить від лат. informatio, що означає «роз'яснення» і передбачає наявність будь-якої форми діалогу між відправниками і одержувачами інформації.

Усі якісні і кількісні визначення інформації також передбачають наявність відправників і одержувачів інформації, тобто мова йде про деякий вид взаємодії об'єктів.

Взаємодію об'єктів, яка призводить до зміни знань хоч би одного з них, можна назвати інформаційною взаємодією, а сукупність засобів, що забезпечують взаємодію об'єктів — засобами інформаційної взаємодії.

Умови інформаційної взаємодії на прикладі передачі знань за допомогою усного мовлення можна сформулювати наступним чином.

Для того, щоб процес передачі знань від одного об'єкта до іншого був успішним, слід дотримуватися низки умов. Процес інформаційної взаємодії на прикладі передачі знань за допомогою усного мовлення можна уявити п'ятикомпонентною (п'ятивимірною векторною) величиною, що складається з компонентів:

1. фізичної;
2. сигнальної;
3. лінгвістичної;

4. семантичної;
5. прагматичної.

Перша компонента — фізична, тобто необхідна наявність фізичного джерела звуку (голосових зв’язок), фізичного середовища поширення звуку (повітря) і фізичного приймача (вуха).

Друга компонента — сигнальна: амплітудно і частотно модульовані коливання.

Третя компонента — лінгвістична: необхідно, щоб обидва співрозмовники знали хоча б одну спільну мову.

Четверта компонента — семантична, тобто в переданому повідомленні повинен бути присутнім змістовний опис об’єкта або впливу, щоб при отриманні повідомлення могли змінитися знання у того, хто приймає ці повідомлення

П’ята компонента — прагматична: необхідна наявність бажання (мотивації) передавати і приймати повідомлення.

*Інформаційна взаємодія відкритих систем*

Як приклад класифікації інформаційних взаємодій можна навести протокольні рівні в міжнародних стандартах взаємодії відкритих мереж. При взаємодії двох користувачів в комунікаційній мережі реалізується сукупність протоколів семи рівнів:

1. фізичного;
2. канального;
3. мережного;
4. транспортного;
5. сеансового;
6. представницького;
7. прикладного.

Перші три протокольних рівні визначають такі особливості роботи мережі зв’язку при обслуговуванні користувачів, як стандарт електричних сигналів в мережі, виявлення та виправлення помилок, маршрутизація в транспортній мережі і т. ін.

Наступні чотири рівні визначають такі стандарти взаємодії самих користувачів, як контроль за цілісністю повідомлення, відновлення без втрат сеансу взаємодії в разі переривання, представлення даних на дисплеях і друкуючих пристроях тощо.

*Класи взаємодії відкритих систем*

Спектр інформаційних взаємодій надзвичайно широкий. Можна умовно розділити досліджувані інформаційні взаємодії по об'єктах на три класи:

1- й клас — взаємодія штучних (технічних) систем;
2- й клас — взаємодія змішаних систем;
3- й клас — взаємодія природних (живих) систем.

До першого класу відносяться інформаційні взаємодії в технічних системах — від найпростіших регуляторів до глобальних комп'ютерних мереж.

До другого класу — інформаційні взаємодії типу «живий організм - штучний орган», «людина — машина», «живий дослідник — неживий об'єкт досліджень» і т. ін.

До третього класу належать інформаційні взаємодії, що діють в межах від молекулярно-генетичного рівня до рівня соціальних спільнот.

При такому різноманітті взаємодіючих об’єктів завдання опису законів інформаційної взаємодії надзвичайно складне, оскільки треба описати як обмін однобітовою інформацією типу «включено — виключено» в технічних системах, так і формування моралі в людських співтовариствах.

При описі кожного з цих рівнів доводиться спиратися на специфічну для відповідного рівня концепцію перетворювача інформації, свої мови опису, закономірності, що розробляються в рамках відповідних дисциплін (наук), які, тим самим, вивчають інформаційну взаємодію на даному рівні.

**Інформаційна інфраструктура**

**Інформаційна інфраструктура** [information infrastructure] — система організаційних структур і підсистем, що забезпечують функціонування засобів інформаційної взаємодії в інформаційному просторі.

Вона включає в себе: сукупність інформаційних центрів, підсистем, банків даних і знань, систем комунікацій, центрів управління, апаратно-програмних засобів і технологій, що забезпечують збирання, зберігання, оброблення і передавання інформації, а також доступ споживачів до інформаційних ресурсів.

**Глобальна інформаційна інфраструктура** — інформаційна інфраструктура світового (міждержавного) масштабу. Може створюватися на основі трансформації національних інформаційних інфраструктур при створенні глобального інформаційного суспільства з дотриманням наступних **принципів:**

— забезпечення справедливої конкуренції;

— заохочення приватних інвестицій;

— визначення й адаптація регулюючих механізмів;

— забезпечення відкритого доступу до мереж;

— створення умов для забезпечення універсального доступу до інформаційних послуг;

— забезпечення рівних можливостей для громадян;

- забезпечення різноманітності змісту, включаючи культурний і мовний.

Ці принципи застосовуються до глобальної інформаційної інфраструктури за допомогою:

- технічної можливості з’єднання й оперування різних комп'ютерних мереж;

- розвитку глобальних ринків для комп’ютерних мереж і телекомунікаційних та інформаційних послуг;

- забезпечення інформаційної безпеки особистості і даних;

- кооперації в галузі досліджень і розробок з створення нових інформаційних продуктів і послуг;

- моніторингу соціальних наслідків становлення інформаційного суспільства.

**Національна інформаційна інфраструктура** — інформаційна інфраструктура однієї держави. До її складу входить не тільки обладнання для передавання, зберігання, оброблення даних, голосу, образів, але й цілий широкий ряд пристроїв, включаючи камери, сканери, клавіатури, телефони, комп'ютери, компакт-диски, відео- і аудіострічки, кабелі, проводи, супутники, оптичні кабелі, лінії передач, мікрохвильові мережі, телевізори, монітори і т. ін.

Цінність національної інформаційної інфраструктури визначається такими її компонентами, як:

— інформація, яка може приймати вигляд наукових або лілових баз даних, звукових записів, бібліотечних архівів тощо;

— програмне забезпечення, яке дозволяє користувачам маніпулювати даними, одержувати доступ і переглядати великі масиви інформації:

— стандарти мереж і кодів передач, що полегшують встановлення взаємозв'язків між мережами і забезпечують захист інформації і надійність мереж;

— особистості, які створюють інформацію, програмні продукти, обладнання і т. ін.

*Інформаційна інфраструктура організації* — сукупність інформаційних ресурсів, інформаційних і комунікаційних систем і мереж, а також організаційної системи, що забезпечують формування і використання інформаційних ресурсів, створення і удосконалення інформаційних технологій і засобів їх забезпечення.

**Визначення кіберпростору**

Кіберпростір [cyberspace] — метафорична абстракція, що використовується в філософії та інформатиці і є віртуальною реальністю, яка представляє «ноосферу» («сферу розуму» відповідно до термінології В. І. Вернадського). Поняття вперше введене у вигляді слова «кіберпростір» (від кібернетика і простір) канадським письменником-фантастом Вільямом Гібсоном у 1982 році в його новелі «Burning Chrome», опублікованій у журналі «Omni», та було популяризовано у подальших творах автора, зокрема у романі «Neuromancer».

Кібернетика [cybernetics]— мистецтво керування) —

1) Наука про загальні закони управління і зв'язку в природі й суспільстві.

2) Прикладна інформатика в галузі створення і використання автоматичних або автоматизованих систем керування різної складності, від керування окремим об'єктом до найскладніших систем управління цілими галузями промисловості, банківськими системами, системами зв'язку і навіть співтовариствами людей.

**Віртуальна реальність** [Virtual Reality (VR)], штучна реальність — світ, створений технічними засобами (об'єкти та суб'єкти), який передається людині через його відчуття: зір, слух, нюх, дотик і інші. Віртуальна реальність імітує як вплив, так і реакції на вплив. Для створення переконливого комплексу відчуттів реальності комп'ютерний синтез властивостей і реакцій віртуальної реальності проводиться в реальному часі.

**Об'єкти віртуальної реальності** зазвичай ведуть себе близько до поведінки аналогічних об'єктів матеріальної реальності. Користувач може впливати на ці об'єкти в злагоді з реальними законами фізики (гравітація, властивості води, зіткнення з предметами, відображення і т. ін.). Однак часто в розважальних цілях користувачам віртуальних світів дозволяється більше, ніж можливо в реальному житті (наприклад: літати, створювати будь-які предмети і т. ін.).

У більш абстрактному сенсі віртуальну реальність можна розглядати як уявну реальність. До уявної реальності можна віднести релігійну і міфологічну містику. На сучасному етапі віртуальна реальність в значній мірі перетинається з кіберпростором.

Не слід також плутати віртуальну реальність з доповненою. їх корінна відмінність в тому, що віртуальна конструює новий штучний світ, а доповнена реальність лише вносить окремі штучні елементи в сприйняття світу реального.

**Доповнена реальність** [Augmented Reality (AR)] — «розширена реальність» — результат запровадження в поле сприйняття будь-яких сенсорних даних з метою доповнення відомостей про оточення і поліпшення сприйняття інформації.

**Інтернет [Internet]** — глобальна загальнодоступна комерційна мережа (всесвітнє об'єднання мереж), що об'єднує мільйони комп'ютерів по усьому світі. Життєдіяльність і розвиток Інтернету координує Товариство Інтернету [Internet Society (ISOC)].

Інтернет в основному складається з пристроїв семи видів: повторювачів, мостів, маршрутизаторів, комутаторів, шлюзів, хостів і вузлів. Більшість з них працює на фізичному, канальному і мережному рівнях моделі ISO/OSI.

Інтернет являє собою фізичну основу значної частини кіберпростору. Тому у вузькому сенсі кіберпростір часто розуміється як сукупність інформаційних ресурсів, доступних за допомогою глобальної комп'ютерної мережі Інтернет. Поняття кіберпростору активно використовується не тільки в комп'ютерних і філософських областях знань, айв продуктах масової культури.

Можна також сказати, що **кіберпростір — це простір для інформаційних об'єктів і подій.**

**Об'єкти в кіберпросторі:**

— сайт;
— web-сторінка;
— аккаунт на форумі;

— електронний лист;
— відеоролик.

**Події в кіберпросторі:**

— діалог в чаті;
— поява статті;
— дискусії на форумах і в блогах; поява і зникнення нових сайтів;
— хакерська атака на сайт.

Для всіх цих подій і об'єктів не можна вказати, до якої країни вони належать, і навіть на якому сервері відбуваються (знаходяться). Наприклад, більшість сайтів знаходиться на декількох серверах, хоча в кіберпросторі сприймається як єдиний об'єкт. Крім того, деякі об'єкти кіберпростору можуть не існувати фізично на серверах, а генеруватися «на льоту» при запиті користувача. Найчастіше фізична структура сайту на сервері принципово відрізняється від логічної структури, яка доступна відвідувачеві сайту через кіберпростір.

*Професійне визначення кіберпростору*

У різних країнах є свої визначення кіберпростору. У США в документі з національної стратегії щодо кібербезпеки від 2003 було зазначено, що «кіберпростір складається з сотень тисяч з'єднаних між собою комп'ютерів, серверів, маршрутизаторів, комутаторів і волоконно-оптичні кабелі, які дозволяють нашій критичної інфраструктури працювати. Таким чином. нормальне функціонування кіберпростору має важливе значення для нашої економіки і нашої національної безпеки» .

Згідно закону України «Про основні засади забезпечення кібербезпеки України» **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.

Звідси видно, що кіберпростір прямо пов'язаний з реальною географією, яка разом з політикою є основним елементом кібер геополітики.

По-перше, всі маршрути комунікації, сервера і технічні вузли, які пов'язані як з Інтернет, мають географічну локалізацію.

По-друге, кіберзони мають національну ідентифікацію в сенсі доменних зон, державного контролю і використовуваної мови.

По-третє, кіберпростір підкреслює фізичну географію особливим чином — датчики різних служб, навігаційні пристрої, технічні ґаджети і мобільні пристрої втілюють собою інтерактивну карту з перехресними потоками інформації, техніки і людей.

**Загальна структура кіберпростору**

Звичайно виділяють три рівні, що складають кіберпростір [48]:

— фізична структура;
— межа;

— соціальна структура.

Девід Кларк запропонував модель, в якій існує чотири рівні кіберпростору.

1. Фізичний рівень містить усі апаратні пристрої, які включають *мар- шрутизатори, комутатори*, носії і супутники, датчики та інші технічні з'єднувачі, як проводові, так і безпроводові. Фізична інфраструктура географічно розташована в «реальному просторі», і таким чином, є предметом різноманітних національних юрисдикцій.
2. Логічний рівень у цілому відноситься до коду, який включає в себе як програмне забезпечення, так і протоколи, які у ньому реалізуються.
3. Рівень контенту описує всю інформацію, яка створюється, береться, зберігається та обробляється у кіберпросторі. Інформація визначається як знання, що стосуються об'єктів, наприклад, факти, події, речі, процеси або ідеї.
4. Соціальний рівень складається з усіх людей, які використовують і формують характер кіберпростору. Це фактичний Інтернет людей і їх потенційні відносини. Він не стосується Інтернету апаратних засобів і програмного забезпечення. По суті, соціальний прошарок включає урядові організації, організації приватного сектору, громадянське суспільство і суб'єкти технічного співтовариства.

**Сполучені штати Америки. Визначення**

Вперше визначення кіберпростору було дано військовими експертами США у доктрині Комітету начальників штабів (КНШ) [Joint Chiefs of Staff (JCS)] 2006 року «Інформаційні операції».

У ній це поняття трактується як «сфера, в якій застосовуються різні радіоелектронні засоби (зв'язку, радіолокації, розвідки, навігації, автоматизації, управління і наведення), що використовують широкий діапазон електромагнітного спектра частот для прийому, передачі, обробки, зберігання, перетворення і обміну інформацією, і пов'язана з ними інформаційна інфраструктура збройних сил США».

У кінці того ж року, це формулювання було уточнена об'єднаним штабом КНШ в «Національній військовій стратегії ведення операцій в кібер-просторі». Відповідно до неї під кіберпростором розуміється «сфера, в якій радіоелектронні засоби та електромагнітний спектр використовуються для зберігання і перетворення даних, а також їх обміну за допомогою комп'ютерних мереж і відповідних інфраструктур».

Таке трактування зазначеної категорії дозволила командуванням ВПС, ВМС і сухопутних військ США, шо приступили до створення видових з'єднань і частин кібероперапій, чіткіше усвідомити поставлені їм завдання в області формування кібернетичних ресурсів. Адже кібер простір визначався як середовище, в якому необхідно широко використовувати не тільки відповідні засоби (комп'ютери з їх апаратно-програмними і мережними ресурсами), а й засоби радіоелектронної боротьби, інформаційних і психологічних операцій, а також зброю спрямованої енергії.

## 5.1.2. ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СФЕРА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

**Протиборство в кіберпросторі як складова інформаційного протиборства**

Найактивніше розробка концептуальних положень боротьби в кіберпросторі велася в ВПС США. Ще в лютому 2008 року міністром ВПС була видана директива про створення 24-ї повітряної армії (ведення бойових дій в кіберпросторі.

В одному з ключових доктринальних документів цього відомства, випущеному в 2010 році під назвою «Операції в кіберпросторі», термін «кіберпростір» конкретизований і сформульований як «глобальна сфера (домен) всередині інформаційного простору, що представляє собою взаємопов'язану сукупність інфраструктур і інформаційних технологій, включаючи Інтернет, телекомунікаційні мережі, комп'ютерні системи, вбудовані процесори та контролери».

Дане визначення вказує на те, що військове керівництво країни розглядає боротьбу в кіберпросторі як складову частину інформаційного протиборства, яке повинно вестися не тільки в чотирьох традиційних просторах — наземному, морському, повітряному і навколоземному космічному, а й у кіберпросторі.

**Сфера протиборства у кіберпросторі**

Виходячи з того, що інформаційний простір — це будь-яке середовище, в якому інформація створюється, через яке передається, приймається, в якому зберігається, обробляється і знищується, кіберпростір представляє електронне (включаючи фотоелектронні і т. ін.) середовище, в якому (через яке), інформація створюється, передається, приймається, зберігається, обробляється і знищується.

Сукупність людей, процесів (у тому числу керуючих) і системи, що складають кіберпростір представляють кіберінфраструктуру, а різні види обміну даними в кіберпросторі називаються кіберсервісами.

До сфери протиборства у кіберпросторі насамперед включають **критично важливий кіберпростір** [critical cyberspace] — підвид кіберпростору, до якого входять частина (елементи) кібернетичної інфраструктури і кібернетичних послуг, які необхідні для здійснення життєво важливих функцій підтримки, суспільної безпеки, економічної стабільності, національної безпеки, міжнародної стабільності (is cyber infrastructure and cyber services that are vital to preservation of public safety, economic stability, national security and international stability).

**Критично важлива кіберінфраструктура** [critical cyber infrastructure] - кіберінфраструктура, яка необхідна для здійснення життєво важливих функцій, підтримки суспільної безпеки, економічної стабільності, національної безпеки, міжнародної стабільності, а також для підтримки працездатності і функцій ефективного відновлення критично важливого кібернетичного простору (is the cyber infrastructure that is essential to vital

services for public safety, economic stability, national security, international stability and to the sustainability and restoration of critical cyberspace).

**Критично важливі кіберсервіси** [critical cyber services] — підвид кіберсервісів (послуг, служб), що представляють частину (елементи) кіберсервісів (послуг, служб), які необхідні для здійснення життєво важливих функцій підтримки суспільної безпеки, економічної стабільності, національної безпеки, міжнародної стабільності (are cyber services that are vital to preservation of public safety, economic stability, national security and international stability).

Будь-який індивідуальний об'єкт або суб'єкт, існуючий в кіберінфраструктурі називається кібероб'єктом [cyber entity]. Кібероб'єкт (кіберсуб'єкт), що має цінність, представляє собою кіберактив [cyber asset].

Організована діяльність у кіберпросторі щодо збирання та накопичення, підготовки, розповсюдження, обмеження в доступі, обробці інформації для досягнення поставлених цілих — це кібероперація [cyber operation], кіберактиви, організовані для проведення кібероперацій — кіберсили [cyber forces].

## 5.1.3. ПОНЯТТЯ КІБЕРБЕЗПЕКИ, ЗАХИСТУ ІНФОРМАЦІЇ ТА КІБЕРЗАХИСТУ

**Протиборство в інформаційній сфері**

Протиборство [confrontation, opposition, antagonism] — боротьба проти будь-чого, будь-кого, протидія.

**Боротьба** [struggle] — 1) Активне противенство, зіткнення між протилежними соціальними грудами, течіями в суспільстві і т. ін.. протистояння. 2) Діяльність, що має на меті подолати або знищити кого-небудь.

**Інформаційне протиборство** [information confrontation] — процес реалізації інформаційних впливів, спрямованих на досягнення мети державної політики в мирний і воєнний часи. Має місце у відносинах між державами незалежно від розвитку співробітництва між ними.

Інформаційне протиборство, використовується для розв'язання соціальних конфліктів різноманітного масштабу в інформаційній сфері та характеризується, з одній сторони, впливом на системи добування, оброблення, розповсюдження та зберігання інформації противника, а з іншої застосуванням заходів захисту своїх подібних систем від деструктивного та керуючого впливу.

Інформаційна сфера [information environment] **(**від грец. *ораїра* — куля) — це сфера діяльності суб'єктів, зв'язана із створенням, перетворенням і споживанням інформації. Інформаційна сфера умовно поділяється на три основні предметні частини (рис.1):

– створення і розповсюдження вихідної та похідної інформації:

– формування інформаційних ресурсів, підготовки інформаційних

продуктів, надання інформаційних послуг,

— споживання інформації та дві забезпечувальні предметні частини:

• створення і застосування інформаційних систем, інформаційних технологій і засобів їхнього забезпечення**:**

• створення і застосування засобів і механізмів інформаційної безпеки.


*РИС 1*. ХАРАКТЕРИСТИКА ІНФОРМАЦІЙНОЇ СФЕРИ

Інформаційне протиборство здійснюється між різноманітними видами соціальних суб'єктів (особистостей, суспільств, держав, наднаціональних утворень), проте цілий ряд таких конфліктних взаємодій має певні відносно стійкі ознаки, які у їхній сукупності утворюють окремі форми — інформаційна війна, інформаційний тероризм, інформаційна злочинність.

**Інформаційний вплив** [information impact] — 1) Організоване застосування сил і засобів інформаційної боротьби для вирішення завдань завоювання (підтримки) інформаційної переваги над противником. 2) Вплив, який здійснюється із застосуванням засобів інформаційної зброї, які дозволяють здійснювати з інформацією, що передається, обробляється, створюється, знищується і сприймається, задумані дії. Інформаційний вплив буде допустимим, якщо він грубо не порушує прийняті у більшості інформаційних систем в даному інформаційному просторі норми і правила поведінки (вихідні результати).

**Інформаційна боротьба** [information struggle] — 1) Боротьба з використанням спеціальних способів і засобів для впливу на інформаційну сферу (середовище) конфронтуючої сторони, а також для захисту власної інформаційної сфери в інтересах досягнення поставленої мети

## 5.1.4. ВИДИ ЗАХИСТУ ІНФОРМАЦІЇ

Напрями забезпечення безпеки інформації — це нормативно-правові категорії, орієнтовані на забезпечення комплексного захисту інформації від внутрішніх та зовнішніх загроз на державному рівні, на рівні підприємства або організації, на рівні окремої особистості.

З урахуванням практики, що склалася на теперішній час, виділяють наступні напрями захисту інформації:

- **правовий захист** — це спеціальні закони, інші нормативні акти, правила, процедури та заходи, що забезпечують захист інформації на правовій основі;
- **організаційний захист** — це регламентація виробничої діяльності та взаємовідносин виконавців на нормативно-правовій основі, яка виключає або послаблює нанесення будь-яких збитків виконавцям;
- **технічний захист** — це використання різноманітних технічних засобів, що перешкоджають нанесенню збитків.

Крім того, заходи захисту, орієнтовані на забезпечення безпеки інформації, можуть бути охарактеризовані цілим рядом параметрів, що відображають, окрім напрямів, орієнтацію на об'єкти захисту, характер загроз, способи дій, їх розповсюдження, охоплення та масштабність.

Так, за характером загроз заходи захисту орієнтовані на захист інформації від розголошення, витоку та несанкціонованого доступу. За способом дії їх можна поділити на попередження, виявлення, припинення та відновлення збитків або інших втрат. За охопленням заходи захисту можуть розповсюджуватися на територію, будівлю, приміщення, апаратуру або окремі елементи апаратури. Масштабність заходів захисту характеризується як об'єктовий, груповий або індивідуальний захист.

*Правовий захист*

Поняття права визначається як сукупність загальнообов'язкових правил і норм поведінки, які встановлені або санкціоновані державою, по відношенню до певних сфер життя та діяльності державних органів, підприємств (організацій) та населення (окремої особистості).

Правовий захист інформації як ресурсу признаний на міждержавному, державному рівні та визначається міждержавними договорами, конвенціями, деклараціями та реалізується патентами, авторським правом та ліцензіями на їхній захист. На державному рівні правовий захист регулюється державними та відомчими актами.

*Організаційний захист*

Організаційний захист — це регламентація виробничої діяльності та взаємовідносин виконавців на нормативній основі, що виключає або суттєво утруднює неправомірне оволодіння конфіденційною інформацією та прояву внутрішніх та зовнішніх загроз.

Організаційний захист забезпечує:

- організацію режиму, охорони, роботу з кадрами, з документами;
- використання технічних засобів безпеки та інформаційно-аналітичну діяльність із виявлення внутрішніх і зовнішніх загроз діяльності підприємства (організації).

Організаційні заходи відіграють суттєву роль у створенні надійного механізму захисту інформації, так як можливості несанкціонованого використання конфіденційних відомостей у значній мірі обумовлюються не те технічними аспектами, а зловмисними діями та недбалістю користувачів або персоналу. Впливу цих аспектів практично неможливо запобігти за допомогою технічних заходів. Для цього необхідна сукупність організаційно-правових і організаційно-технічних заходів, які вилучали би (або зводили до мінімуму) можливість виникнення небезпеки конфіденційності інформації.

*Технічний захист*

**Технічний захист** — це сукупність спеціальних органів, технічних засобів та заходів для їхнього використання в інтересах захисту конфіденційної інформації. Основне завдання технічного захисту — це попередження розголошення, витоку, несанкціонованого доступу та інших форм незаконного втручання в інформаційні ресурси.

Різноманітність цілей, завдань, об'єктів захисту та заходів, що проводяться. передбачають розгляд деякої системи класифікації засобів технічного захисту за видом, орієнтацією та іншими характеристиками.

Наприклад, засоби технічного захисту можна класифікувати за об'єктами впливу, характером заходів, способами реалізації, масштабом охоплення, класом засобів зловмисників, яким здійснюється протидія зі сторони служби безпеки.

За функціональним призначенням **засоби технічного захисту** поділяються на наступні групи: фізичні засоби захисту, апаратні засоби захисту, програмні засоби захисту, криптографічні засоби захисту.

**Фізичні засоби** включають різноманітні пристрої та споруди, які перешкоджають фізичному проникненню (або доступу) зловмисників на об'єкти захисту та до матеріальних носіїв конфіденційної інформації та здійснюють захист персоналу, матеріальних носіїв, фінансів та інформації від протиправних дій.

До **апаратних засобів** відносяться прилади, пристрої, та інші технічні рішення, які використовуються в інтересах захисту інформації. Основне завдання апаратних засобів — забезпечення стійкого захисту від розголошення, витоку і несанкціонованого доступу через технічні засоби забезпечення діяльності організації (підприємства).

**Програмні засоби** охоплюють спеціальні програми, програмні комплекси та системи захисту інформації в інформаційних системах різноманітного призначення та засобах обробки (збирання, нагромадження, зберігання, оброблення та передачі) даних.

**Криптографічні засоби** — це спеціальні математичні та алгоритмічні засоби захисту інформації, що передається системами та мережами зв'язку, зберігається та обробляється на ЕОМ із використанням різноманітних методів шифрування.

Апаратні методи та засоби захисту знайшли достатньо широке розповсюдження. Проте із-за того, що вони не мають достатньої гнучкості, часто втрачають свої захисні властивості при розкритті принципу їхньої дії і

в подальшому не можуть бути використані.

Програмні методи та засоби більш надійні, період їхнього гарантованого використання значно більший, ніж апаратних методів та засобів.

Криптографічні методи та засоби займають важливе місце і є надійним засобом забезпечення захисту інформації на тривалі періоди.

Очевидно, що такий поділ засобів захисту інформації достатньо умовний, так як на практиці дуже часто вони взаємодіють і реалізуються у вигляді програмно-апаратних засобів із широким використанням алгоритмів закриття інформації.

## 5.1.5. ПОНЯТТЯ КОНФІДЕНЦІЙНОСТІ, ЦІЛІСНОСТІ, ДОСТУПНОСТІ

Основні властивості інформації як предмета захисту **д**оступність інформації

Доступність інформації (даних) (availability of information] — де можливість використання інформації (даних), коли в цьому виникає необхідність. Доступність також характеризує працездатність інформаційної системи.

Інформація доступна, коли вона міститься на матеріальному носії. До носіїв інформації (даних) [data medium] відносяться матеріальні об’єкти, які забезпечують запис, зберігання і передавання інформації у просторі часі. Носіями інформації можуть бути:

- люди;
- матеріальні тіла (макрочастки);
- поля (випромінювання);
- елементарні частки (мікрочастки).

Так як за допомогою матеріальних засобів можна захищати тільки матеріальний об’єкт, то об’єктами захисту є матеріальні носії інформації. Розрізняють носії — джерела інформації, носії — переносники інформації та носії — одержувачі інформації.

**Цілісність інформації** [integrity of information] — це захищеність інформації від несанкціонованої зміни, забезпечення її точності та повноти.

Корисність інформації завжди конкретна. Нема цінної інформації взагалі. Інформація корисна або шкідлива для конкретного її користувача. Під користувачами звичайно розуміють як одну людину (процес), так і групу людей і навіть усе людство. Надзвичайно цінна для одних користувачів інформація може не представляти цінності для інших.

Для інформаційних систем як об’єктів захисту властиві наступні такі характеристики як конфіденційність, доступність та цілісність інформації (даних) в інформаційній системі .

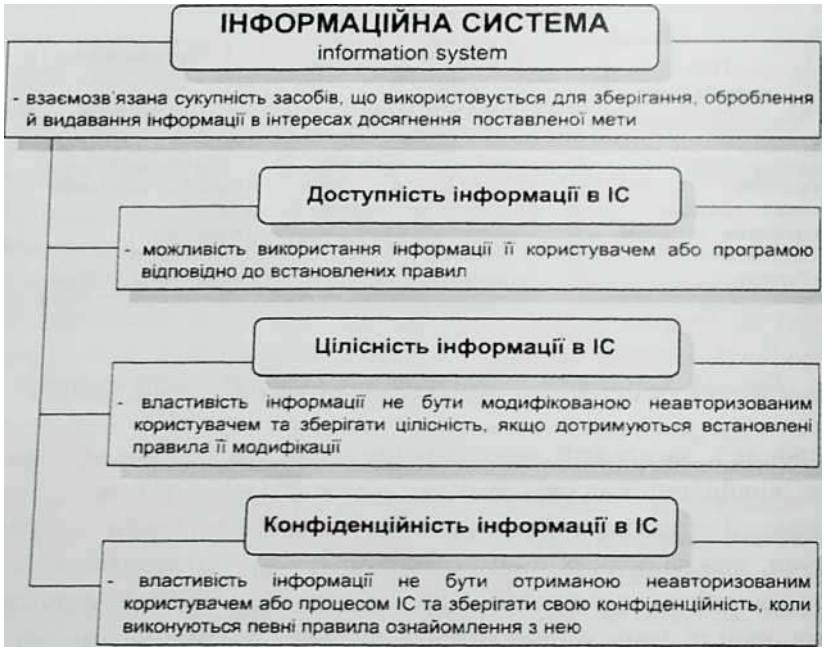


Рис. Інформаційна система як об’єкт захисту

Конфіденційність [confidentiality, privacy] (від лат. confidentia — довір’я) — це властивість не підлягати розголосові; довірчість, секретність, суто приватність, секретність.

Конфіденційність інформації (даних) в інформаційній системі - це властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і (або) процесом інформаційної системи. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею.

Доступність [availability] у загальному сенсі представляється як можливість проникнення куди-небудь.

Для інформаційної системи — це властивість ресурсу системи, яка полягає в тому, що користувач і (або) процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, і в той час, коли він йому необхідний.

Доступність даних [data confidentiality] в інформаційній системі — це властивість даних, що полягає у можливості їхнього читання користувачем або програмою. Визначається рядом факторів: можливістю працювати за терміналом, володінням паролем, знанням мови запитів і т. ін.

Цілісність [integrity] — це внутрішня єдність, зв’язаність усіх частин чого-небудь, єдине ціле.

В інформаційній системі — це стан даних або інформаційної системи, в якій дані та програми використовуються встановленим чином, що забезпечує:

– стійку роботу системи;

- автоматичне відновлення у випадку виявлення системою потенційної помилки;

– автоматичне використання альтернативних компонентів замість тих, що вийшли з ладу.

Для інформаційної системи можна розглядати такі поняття як цілісність даних, цілісність інформації, цілісність бази даних цілісність інформаційної системи і т. ін.

Цілісність даних [data integrity] в інформаційній системі — це стан, при якому дані, що зберігаються в системі, в точності відповідають даним у вихідних документах; властивість, що має відношення до набору даних і означає, що дані не можуть бути змінені або зруйновані без санкції на доступ. Цілісність даних вважається збереженою, якщо дані не спотворені і не зруйновані (стерті). Семантична цілісність даних [semantic data integrity] — це стан даних, коли вони зберігають свій інформаційний зміст та однозначність інтерпретації в умовах випадкових впливів.

Цілісність інформації [information integrity] — це властивість інформації, яка полягає в тому, що інформація не може бути модифікована не- авторизованим користувачем і (або) процесом. Інформація зберігає цілісність, якщо дотримуються встановлені правила її модифікації (видалення).

Цілісність бази даних [database integrity] — це стан бази даних, коли всі значення даних правильні в тому сенсі, що відображають стан реального світу (в межах заданих обмежень по точності та часовій узгодженості) і підпорядковуються правилам взаємної несулеречливості. Підтримка цілісності бази даних включає перевірку цілісності і відновлення з будь-якого неправильного стану, яке може бути виявлено; це входить у функції адміністратора бази даних.

**Цілісність системи** [system integrity] — **це властивість** системи, яка полягає в тому, що жоден її компонент не може бути усунений, модифікований або доданий з порушенням політики безпеки.

До **захищених інформаційних систем відносяться** інформаційні системи, які для певних умов експлуатації забезпечують безпеку (конфіденційність, цілісність) інформації, що функціонує в системі**,** та підтримує свою працездатність в умовах впливу на неї заданої множини загроз.

Для інформаційної системи властиві наступні види загроз: загрози порушення конфіденційності, загрози порушення цілісності, загрози порушення працездатності (доступності).

**Загрози порушення конфіденційності** спрямовані на розголошення інформації з обмеженим доступом.

**Загрози порушення працездатності (доступності)** спрямовані на створення ситуацій, коли в результаті навмисних дій понижується працездатність обчислювальної системи, або її ресурси стають недоступними.

**Загрози порушення цілісності** полягають у спотворенні або зміні неавторизованим користувачем інформації, що зберігається або передається. Цілісність інформації може бути порушена як зловмисником, так і в результаті об'єктивних впливів з боку середовища експлуатації системи.

## 5.1.6. ПРИНЦИПИ КІБЕРБЕЗПЕКИ

ЗАКОН УКРАЇНИ
Про основні засади забезпечення кібербезпеки України
(Відомості Верховної Ради (ВВР), 2017, № 45, ст.403)

*Стаття 7. Принципи забезпечення кібербезпеки*

1. Забезпечення кібербезпеки в Україні ґрунтується на принципах:

1) верховенства права, законності, поваги до прав людини і основоположних свобод та їх захисту в порядку, визначеному законом;

2) забезпечення національних інтересів України;

3) відкритості, доступності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі;

4) державно-приватної взаємодії, широкої співпраці з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проектів, навчання та підвищення кваліфікації кадрів у цій сфері;

5) пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам, реалізації невід'ємного права держави на самозахист відповідно до норм міжнародного права у разі вчинення агресивних дій у кіберпросторі;

6) пріоритетності запобіжних заходів;

7) невідворотності покарання за вчинення кіберзлочинів;

8) пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу;

9) міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в терористичних, воєнних, інших протиправних цілях;

10) забезпечення демократичного цивільного контролю за утвореними відповідно до законів України військовими формуваннями та правоохоронними органами, що провадять діяльність у сфері кібербезпеки.