**Тема 1.1. Інформація та інформаційна безпека**

**1. Зміст поняття інформація та її основні характеристики**

Інформація - це сукупність відомостей (даних), які сприймають із навколишнього середовища (вхідна інформація), видають у навколишнє середовище (вихідна інформація) або зберігають всередині певної системи.

Найбільш важливими властивостями інформації є:

* об'єктивність та суб'єктивність;
* повнота. Информацию можно назвать полной, если ее достаточно для понимания и принятия решений. Неполная информация может привести к ошибочному выводу или решению.
* достовірність ( Достовірність — суб'єктивна) - безоговорочная, почти абсолютная уверенность индивидуума либо группы людей, в честности и авторитете источника информации. Пример: до командования дошла достоверная информация, о готовности к наступлению групп противника.
* адекватність — это уровень соответствия образа, создаваемого с помощью информации, реальному объекту, процессу, явлению.
* доступність;
* актуальність;
* точність;
* цінність.

**2. Види інформації**

Основні види інформації розрізняють за формами її представлення, кодування та збереження.

Це:

* графічна,
* звукова,
* текстова,
* числова,
* відеоінформація.

**3. Інформаційні революції**  


**4. Безпека в інформаційному суспільстві**  
**Інформаці́йне суспі́льство** — теоретична концепція [постіндустріального суспільства](https://uk.wikipedia.org/wiki/%D0%9F%D0%BE%D1%81%D1%82%D1%96%D0%BD%D0%B4%D1%83%D1%81%D1%82%D1%80%D1%96%D0%B0%D0%BB%D1%8C%D0%BD%D0%B5_%D1%81%D1%83%D1%81%D0%BF%D1%96%D0%BB%D1%8C%D1%81%D1%82%D0%B2%D0%BE), історична фаза можливого еволюційного розвитку [цивілізації](https://uk.wikipedia.org/wiki/%D0%A6%D0%B8%D0%B2%D1%96%D0%BB%D1%96%D0%B7%D0%B0%D1%86%D1%96%D1%8F), в якій інформація і знання продукуються в єдиному інформаційному просторі. Головними продуктами виробництва інформаційного суспільства мають стати [інформація](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%8F) і [знання](https://uk.wikipedia.org/wiki/%D0%97%D0%BD%D0%B0%D0%BD%D0%BD%D1%8F). Характерними рисами теоретичного інформаційного суспільства, є:

* збільшення ролі інформації і знань в житті суспільства;
* зростання кількості людей, зайнятих [інформаційними технологіями](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%D1%96_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%97), комунікаціями і виробництвом інформаційних продуктів і послуг, зростання їх частки у валовому внутрішньому продукті;
* зростання інформатизації та ролі інформаційних технологій в суспільних та господарських відносинах;
* створення [глобального інформаційного простору](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%81%D1%84%D0%B5%D1%80%D0%B0), який забезпечує (а) ефективну інформаційну взаємодію [людей](https://uk.wikipedia.org/wiki/%D0%9B%D1%8E%D0%B4%D0%B8%D0%BD%D0%B0), (б) їх доступ до світових [інформаційних ресурсів](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%B8%D0%B9_%D1%80%D0%B5%D1%81%D1%83%D1%80%D1%81) і (в) задоволення їхніх потреб щодо інформаційних продуктів і послуг.

А дальше нужно рассказать, что безопасность это оч важно и т.д. тут больше отсебятины.

**5. Інформаційна безпека людини, суспільства, держави та міжнародного співтовариства**

ІНФОРМАЦІЙНА БЕЗПЕКА (ІБ) - стан захищеності особи, суспільства і держави, при якому досягається інформаційний розвиток (технічний, інтелектуальний, соціально-політичний, морально-етичний), за якого сторонні інформаційні впливи не завдають їм суттєвої шкоди.

Інформаційна безпека особистості - це стан людини, в якому його особистості не може бути завдано істотної шкоди шляхом здійснення впливу на навколишнє інформаційний простір.

Інформаційна безпека суспільства - це стан суспільства, в якому йому не може бути завдано істотної шкоди шляхом впливу на його інформаційну сферу. В її основі - безпека індивідуального, групового і масової свідомості громадян при наявності інформаційних загроз, до яких в першу чергу слід віднести інформаційно-психологічний вплив. Дія цих загроз може викликати психоемоційну і соціально-психологічну напруженість, спотворення моральних критеріїв і норм, морально-політичну дезорієнтацію і, як наслідок, неадекватна поведінка окремих осіб, груп і мас людей. В результаті таких дій можливі глибокі трансформації індивідуального, групового і масової свідомості, негативні зміни морально-політичного та соціально-психологічного клімату в суспільстві.

Інформаційна безпека держави - це стан держави, в якому йому не може бути завдано істотної шкоди шляхом здійснення впливу на його інформаційну сферу. Забезпечення інформаційної безпеки держави нерозривно пов'язано із забезпеченням національної безпеки.

**6. Розмежування інформаційної безпеки та захисту інформації.**інформаційна безпека - стан захищеності інформації та підтримує інфраструктури від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати неприйнятного збитку суб'єктам інформаційних відносин.

Захист інформації - комплекс заходів(правових, організаційних і технічних) і дій щодо запобігання загроз інформаційної безпеки та усунення їх наслідків в процесі збору, зберігання, обробки і передачі інформації в інформаційних системах.

Тобто інформаційна безпека - стан, а захист інформації - комплекс заходів для досягнення цього стану.

**Тема 1.2. Інформаційні права і свободи людини.**

**1. Поняття та види інформаційних прав людини**

Інформаційні права людини — це гарантовані державою можливості людини задовольняти її потреби в отриманні, використанні, поширенні, охороні і захисті необхідного для життєдіяльності обсягу інформації.

**У юридичній науці найбільшого поширення набула класифікація прав і свобод людини та громадянина за сферами діяльності держави і громадян (за сферами реалізації в суспільному житті). Зокрема за цим критерієм виокремлюють такі види прав і свобод людини та громадянина:**  
  
1) громадянські або особисті права й свободи   
2) політичні права і свободи  
3) економічні права і свободи   
4) соціальні права і свободи  
5) культурні права та свободи

Розглянемо основні види інформаційних правовідносин. У навчальній .літературі відсутня єдина точка зору на питання їх класифікації. Так, Б.А. Копилов виділяє відносини, що виникають:

* при здійсненні пошуку, отримання та споживання інформації, інформаційних ресурсів, інформаційних продуктів, інформаційних послуг;
* при виробництві, передачі та розповсюдженні інформації, інформаційних ресурсів, інформаційних продуктів, інформаційних послуг;
* при створенні та застосуванні інформаційних систем, їх мереж, засобів забезпечення;
* при створенні та застосуванні засобів та механізмів інформаційної безпеки.

1. Свобода особистого і сімейного життя (ст. 32: "...не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини");  
  
2. Таємниця листування, телефонних переговорів, телеграфної й іншої кореспонденції (ст. 31: "...винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо");  
  
3. Право громадянина не зазнавати втручання в його особисте та сімейне життя, шляхом збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, знайомитися в органах державної влади, органах місцевого самоврядування, установах та організаціях із відомостями про себе (ст. 32: це відноситься до відомостей, що "не є державною або іншою захищеною законом таємницею");  
  
4. Право громадянина направляти індивідуальні або колективні письмові звернення або особисто звертатися в органи державної влади, органи місцевого самоврядування та до посадових і службових осіб цих органів (ст. 40);  
  
5. Право кожного громадянина на сприятливе навколишнє середовище, достовірну інформацію про її стан (ст. 50: "...така інформація ніким не може бути засекречена");  
  
6. Право кожного на свободу творчості і право доступу до культурних цінностей (ст. 54: результати інтелектуальної, творчої діяльності громадянина "ніхто не може використовувати або поширювати їх без його згоди, за винятками, встановленими законом");  
  
7. Право кожного громадянина на одержання кваліфікованої правової допомоги (ст. 59: "...у випадках, передбачених законом, ця допомога надається безоплатно").

**2. Інформаційні права людини за Конституцією України**

Згідно зі ст. 34 Конституції України «кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб — на свій вибір».

В статті також зазначено: «здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя».

1. Свобода особистого і сімейного життя. Право громадянина не зазнавати втручання в його особисте та сімейне життя, шляхом збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, знайомитися в органах державної влади, органах місцевого самоврядування, установах та організаціях із відомостями про себе .(ст. 32 КУ: «…не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини»).

У ст. 302 ЦК законодавчо закріплено, що збирання, зберігання, використання і поширення інформації про особисте життя фізичної особи без її згоди не допускаються, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Після прийняття Закону України «Про захист персональних даних» стає актуальною проблема обігу та захисту персональних даних.

2. [Таємниця листування](https://uk.wikipedia.org/wiki/%D0%A2%D0%B0%D1%94%D0%BC%D0%BD%D0%B8%D1%86%D1%8F_%D0%BB%D0%B8%D1%81%D1%82%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F), телефонних розмов, телеграфної та іншої кореспонденції (ст. 31 КУ: «…винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо»).

3. Право громадянина направляти індивідуальні або колективні письмові звернення або особисто звертатися в органи державної влади, органи місцевого самоврядування та до посадових і службових осіб цих органів (ст. 40 КУ).

4. Право кожного громадянина на достовірну інформацію про стан [довкілля](https://uk.wikipedia.org/wiki/%D0%94%D0%BE%D0%B2%D0%BA%D1%96%D0%BB%D0%BB%D1%8F) (ст. 50 КУ: «…така інформація ніким не може бути засекречена»).

5. Право кожного на свободу творчості і право доступу до культурних цінностей (ст. 54 КУ: результати інтелектуальної, творчої діяльності громадянина «ніхто не може використовувати або поширювати їх без його згоди, за винятками, встановленими законом»).

**3. Право людини на захист персональних даних**

Визначення поняття персональні дані наводиться в абзаці восьмому статті 2 Закону, відповідно до якого персональними даними є відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Статтею 32 Конституції України проголошено право людини на невтручання в її особисте життя. Крім того, не допускається збирання, зберігання, використання поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

З метою конкретизації права людини, гарантованого статтею 32 Конституції України, та визначення механізмів його реалізації 1 червня 2010 року Верховною Радою України було прийнято Закон України «Про захист персональних даних» (далі – Закон), який набрав чинності з 1 січня 2011 року. Предметом правового регулювання Закону є правовідносини, пов’язані із захистом персональних даних під час їх обробки.

**4. Право на доступ до публічної інформації**

Частиною першою статті 1 Закону України «Про доступ до публічної інформації»визначено, що публічна інформація – відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, яка була отримана або створена у процесі виконання суб’єктами владних повноважень своїх обов’язків, передбачених чинним законодавством або яка знаходиться у володінні суб’єктів владних повноважень, інших розпорядників публічної інформації, визначених цимЗаконом.

Відповідно до статті 10 Закону України «Про доступ до публічної інформації» кожна особа має право:

1) знати у період збирання інформації, але до початку її використання, які відомості про неї та з якою метою збираються, як, ким і з якою метою вони використовуються, передаються чи поширюються, крім випадків, встановленихзаконом;

2) доступу до інформації про неї, яка збирається та зберігається;

3) вимагати виправлення неточної, неповної, застарілої інформації про себе, знищення інформації про себе, збирання, використання чи зберігання якої здійснюється з порушенням вимог закону;

4) на ознайомлення за рішенням суду з інформацією про інших осіб, якщо це необхідно для реалізації та захиступрав та законних інтересів;

5) на відшкодування шкоди у разі розкриття інформації про цю особу з порушенням вимог, визначених законом.

Відповідно до статті 19 Закону України «Про доступ до публічної інформації» запитувач має право звернутися до розпорядника інформації із запитом на інформацію незалежно від того, стосується ця інформація його особисто чи ні, без пояснення причини подання запиту.

**5. Цифрові права людини**

Цифрові права - права людини, що укладаються в праві людей на доступ, використання, створення та публікацію цифрових творів, доступ і використання комп'ютерів та інших електронних пристроїв, а також комунікаційних мереж, зокрема, до мережі Інтернет. Доступ до Інтернету визнається правом відповідно до законодавства ряду країн.

«цифрові права людини - це розширення і застосування універсальних прав людини до потреб суспільства, що базується на інформації ... Основні цифрові права людини включають **право доступу до електронної мережі, право вільно спілкуватися** і **висловлювати думки** в мережі, а також право на **непригодність приватної сфери** ». В 1997 році на кассельському художественном фестивале Documenta Group of Amsterdam Media Activists of De Waag вперше була представлена ​​Хартія комунікаційних прав людини (Народна комунікаційна хартія). В ній формулировались вимоги, що стосуються збереження суспільної публічної простору як суспільного достоїнства та захисту її від спроб з боку комерційних та поліцейських інтересів. З 1997-го року судно комунікаційних прав людини було серйозно доработан, і робота по їх захисту послідовно ведеться громадською ініціативою CRIS (Права зв'язку в інформаційному суспільстві).  
Поняття цифрового права нерозривно пов'язане з поняттям **цифрових послуг**. Якщо немає в необхідному обсязі цифрових послуг, то і не може виникнути цифрове право на їх використання. Водно час аналогових телефонів право на телефонну зв'язок відсутнє, так як суспільство не могло забезпечити телефонними лініями всіх бажаючих. Перехід до цифрової мобільної зв'язку давав можливість забезпечити всіх бажаючих мобільними телефонами. У кожного появилося право на цифрову телефонну зв'язок, але це право громадянина може втратити. При арест мобільні телефони вилучаються.  
  
Цифрові права громадянина можуть бути ущемлені державою (наприклад, правоохоронними органами), а також цифровими правами громадянина можуть бути ушкоджені провайдером, який оголосив про готовність надавати цифрові послуги, уклав договір, але не бажає його виконати. Атаковати цифрові права громадянина можуть різного роду мошенники. Одним із способів ущемлення цифрових громадянських прав людини є нав'язування йому абсолютно необов'язкових цифрових послуг (наприклад, спаму).  
  
Основна роль цифрового держави - це захист цифрових прав своїх громадян від наклепів на них вразливих, які намагаються дезинформувати суспільство або окремого людини [джерело не вказано 742 дня].

**Тема 1.3. Загрози інформаційній безпеці людини**

**1. Поняття загроз інформаційній безпеці людини**

Загрози інформаційній безпеці людини – це сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості. Чинне законодавство визначає як життєво важливі інтереси особи в інформаційній сфері України наступні: 1) забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; 2) недопущення несанкціонованого втручання у зміст, процеси обробки, передачі та використання персональних даних; 3) захищеність від негативного інформаційно-психологічного впливу

**2. Вплив інформації на свідомість та поведінку людини.**

В процесі функціонування засоби масової інформації здійснюють двобічний зв'язок між комунікатором та реципієнтом

ЗМІ не лише виконують інформативну функцію (хоча вона має бути основною), але пропагують ідеї, погляди, вчення, політичні програми і беруть, таким чином, участь у соціальному управлінні. Шляхом формування громадської думки, вироблення певних установок, вони спонукають людину до тих чи інших вчинків

В процесі динамічної взаємодії та різноплановості й багатоповторюваності цієї взаємодії людина втрачає можливість (та й потребу) бути безпосереднім свідком.

Тому не дивною є думка про те, що ЗМІ здійснюють вплив на суспільство, його розвиток. Особливістю масово-інформаційних процесів останнього часу є їхня "демасифікація" - можливість вибору для індивіда тієї інформації, яку він сам хоче отримати, а не яку йому нав'язують ззовні, хоча це й пов'язано з певними труднощами технічного й політичного плану.

**Важливий вплив на психологію здійснює музичний супровід** до картинки та кольорова гама, бо кожний колір налаштовує на відповідну хвилю поведінки, реакції - він фактично створює настрій. Таким чином, можна загострити або пом'якшити інформацію, що надається. Виходячи з каналу сприйняття, розрізняються різні типи поведінки.

Психологічно люди готові краще сприймати зовнішньо привабливий образ й до того ж максимально наближений до їх умов існування - так він стає зрозумілішим і немов "ріднішим". Подібні замовлення досить часто виконуються ЗМІ як для влади, так і для спецслужб й бізнесових кіл, які часто стоять за ЗМІ.

На відміну від преси та інших друкованих видів ЗМІ, де інформація подається послідовно, телебачення робить це фрагментарно, тобто подрібнює інформацію, створюючи таким чином ілюзорність її оперативності та різноманітності.

**Серед інших прийомів психологічного впливу ЗМІ застосовують:**

* прийоми лінгвістичного маніпулювання (слова-синоніми, що передають різні відтінки, а тому й формують різне ставлення);
* викривлення масштабів подій та часу;
* звернення до негативних рівнів свідомості;
* "метод Геббельса".

**Прийоми, притаманні TV:**

* ракурс,
* освітлення,
* монтаж кадрів,
* час;
* посилання на сфабриковані вияви громадської думки;
* "ефект вагону з оркестром";
* спираль замовчування і т. ін.

**3. Загрози інформаційній безпеці людини на ранніх етапах соціалізації**

Інформаційна культура особистості формується в процесі соціалізації, як і інші – правова, економічна, екологічна тощо. На свідомому та підсвідомому рівнях відбувається засвоєння певних соціальних ролей та поведінкових моделей. В подальшому доросла людина повинна самостійно розвиватись і переживати становлення як особистість в суспільстві. Тому в особливий спосіб акцентуємо увагу на окремих загрозах, які особливо актуальні на початкових етапах соціалізації.

Відбувається помітна **уніфікація масової свідомості**, оскільки люди “споживають” одні й ті ж інформаційні продукти глобального характеру (новини, реклама, художні твори і т.д.), йде масова пропаганда способу життя, притаманного цивілізації технологічно розвинених країн.

Значна увага приділяється загрозам, що виникають у зв’язку з інформацією, яка становить **загрозу морально-психічному здоров’ю дітей та підлітків**. Еротика користується великою популярністю у всіх сферах індустрії розваг, в т.ч. в Інтернеті і в мобільному контенті.

**Віртуалізація реальності**. Поширення масової культури, неминучість зіткнення з віртуальною реальністю, в якій важко розрізнити ілюзію і дійсність, створюють не лише психологічні і культурні проблеми, але й правові. Створюючи свій образ у віртуальному просторі, людина втрачає адекватне сприйняття реального світу, в тому числі правової дійсності

**4. Інформаційна дискримінація**Інформаційна дискримінація - умисне приховування інформації одного суб'єкта економічних відносин від іншого, з метою отримання власної вигоди.

Спочатку проблема цифрової нерівності сприймалася як суто американська й обговорювалася лише в США. Однак згодом вона стала осмислюватися як глобальна. На міжнародному рівні питання інформаційної нерівності вперше було порушене в підписаній улітку 2000 року лідерами країн “вісімки” Окінавській хартії глобального інформаційного суспільства. Згідно з цим документом було утворено міжнародну експертну раду Dіgіtal Opportunіty Task Force, що виробила план дій, представлений лідерам країн “вісімки” на зустрічі в Генуї влітку 2001 року

**Економічні ресурси** є одним із найважливіших чинників формування світових розривів. Економічно багаті країни мають більші ресурси для втілення технологічних новацій та залучення до них мас.

**Вікові розриви** пов’язані з прагненням і відкритістю молоді до інновацій, тоді як люди середнього та старшого віку схильні до стабільності й певної статики. Все залежить від створених можливостей і мотивації.

**Гендерні проблеми** виникають у суспільствах, в яких жінка через релігійні чи інші умовності розглядається як неповноправний суб’єкт громадського життя.

Однією з суттєвих нерівностей, які перешкоджають реалізації якісного мережевого спілкування, є **мовна диспропорція**, сформована на основі домінування англійської мови як головної мови Інтернету та програмного і технічного супроводу комп’ютерних та телекомунікаційних засобів.

**Люди з обмеженими фізичними даними** часто не мають можливості спілкуватися в Інтернеті, оскільки не всі комп’ютери налаштовані під потреби інвалідів зору чи слуху, і лише невеликий відсоток сайтів обладнаний програмами звукового супроводу текстового чи графічного матеріалів.

**5. Інформаційний вибух і інформаційне перевантаження. Інформційні адикції  
Інформаційний вибух** — постійне збільшення швидкості і обсягів [публікацій](https://uk.wikipedia.org/wiki/%D0%9F%D1%83%D0%B1%D0%BB%D1%96%D0%BA%D0%B0%D1%86%D1%96%D1%8F) (обсягу [інформації](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%8F)) в масштабах [планети](https://uk.wikipedia.org/wiki/%D0%9F%D0%BB%D0%B0%D0%BD%D0%B5%D1%82%D0%B0).

За статистикою, обсяг цифрової інформації подвоюється кожні вісімнадцять місяців.  
**Інформаційне перевантаження** - термін, що описує труднощі розуміння проблеми і прийняття рішень, причиною якої є надлишок інформації.

**Адди́кция** ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) addiction — зависимость, пагубная привычка, привыкание), в широком смысле, — ощущаемая [человеком](https://ru.wikipedia.org/wiki/%D0%A7%D0%B5%D0%BB%D0%BE%D0%B2%D0%B5%D0%BA) навязчивая потребность в определённой деятельности.

Наваяйте то-то про интернет заваисимость

**6. Маніпулювання свідомістю - сутність та види маніпуляції.**Маніпуляція свідомістю - це своєрідне панування над духовним станом людей, управління шляхом нав'язування людям ідей, установок, мотивів, стереотипів поведінки, вигідних суб'єкту впливу.

Дозування інформації. Повідомляється тільки частина відомостей, а решта ретельно приховуються. Це призводить до того, що картина реальності спотворюється в ту чи іншу сторону, або взагалі стає незрозумілою.

Велика брехня. Улюблений прийом міністра пропаганди нацистської Німеччини Й. Геббельса. Він стверджував, що чим нахабніше і неправдоподібніше брехня, тим швидше в неї повірять, головне - подавати її максимально серйозно.

Затягування часу. Цей спосіб зводиться до того, щоб під різними приводами відтягувати оприлюднення дійсно важливих відомостей до того моменту, коли буде вже пізно щось змінити.

Поворотний удар. Суть цього способу в тому, що вигадану (природно, вигідну для себе) версію тих чи інших подій через підставних осіб поширюють в органах ЗМІ, нейтральних по відношенню до обох конфліктуючих сторін. Преса противника зазвичай повторює цю версію, бо вона вважається більш "об'єктивної", ніж думки прямих учасників конфлікту.

Своєчасна брехня. Спосіб полягає в повідомленні абсолютно брехливою, але надзвичайно очікуваної в даний момент ("гарячої") інформації.

Є й інші способи маніпулювання, немає сенсу розглядати їх усі без винятку.

**7. Сутність та прояви інформаційного насильства**

Інформаційне насильство можна очевидним чином розділити на три основних прояви:

* До першого з них відноситься отримання інформації без згоди її власника, т. Е. Передача інформації без згоди передавального. Це, перш за все, всілякий шпигунство, прослуховування каналів зв'язку, перлюстрація поштової кореспонденції, радіоперехоплення тощо.
* Другий вид інформаційного насильства - це передача інформації без згоди одержувача. До цього виду відносяться спам, словесні образи, зловмисна дезінформація і т.п. Разом з тим, до даного виду інформаційного насильства автор пропонує віднести: велику частину існуючої реклами (як мінімум, будь-яку рекламу з використанням персональних каналів зв'язку, а також зовнішню рекламу і т.п.,
* У третій, і останній вид інформаційного насильства автор виділяє втручання третіх осіб у вільний інформаційний

**Тема 1.4. Свобода інформації як інститут міжнародного інформаційного права**

**1. Філософсько-правовий зміст свободи інформації.**непонятно где должна находиться граница между конфеденциальной информацией и свободной информацией ( написать несколько предложений об этом).

**Свобода інформації** — поняття, що використовується для позначення групи прав і свобод, включаючи свободу вираження переконань (свобода слова), вільне функціонування засобів масової інформації (свобода друку), право суспільства на отримання від державних служб інформації, що має суспільне значення, свободу поширення інформації будь-яким законним способом[[1]](https://uk.wikipedia.org/wiki/%D0%A1%D0%B2%D0%BE%D0%B1%D0%BE%D0%B4%D0%B0_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97#cite_note-dic_economic_law-1).

Свобода шукати, одержувати та поширювати інформацію є одним з найважливіших політичних та особистих прав людини та включена в Загальну декларацію прав людини (стаття 19). Свобода слова, розширенням якої є свобода інформації, — це фундаментальне право людини, визнане в міжнародному праві.

Свобода інформації, як свобода вираження своїх думок, не залежить від носія та способу передачі інформації: усно, письмово, друковано, через Інтернет або у формі художньої творчості. Таким чином, правова охорона цієї свободи поширюється як на зміст інформації, так і на засоби її висловлювання[[2]](https://uk.wikipedia.org/wiki/%D0%A1%D0%B2%D0%BE%D0%B1%D0%BE%D0%B4%D0%B0_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97#cite_note-2). Свобода інформації може бути пов'язана з [приватністю](https://uk.wikipedia.org/w/index.php?title=%D0%97%D0%B0%D1%85%D0%B8%D1%81%D1%82_%D0%BF%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D1%85_%D0%B4%D0%B0%D0%BD%D0%B8%D1%85&action=edit&redlink=1) в контексті [Інтернету](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82) та сучасних [інформаційних технологій](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%D1%96_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%97)[[3]](https://uk.wikipedia.org/wiki/%D0%A1%D0%B2%D0%BE%D0%B1%D0%BE%D0%B4%D0%B0_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97#cite_note-autogenerated2-3)[[4]](https://uk.wikipedia.org/wiki/%D0%A1%D0%B2%D0%BE%D0%B1%D0%BE%D0%B4%D0%B0_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97#cite_note-4)

Разом з тим, свобода інформації може бути обмежена, як для дотримання інших прав особистості ([таємниця зв'язку](https://uk.wikipedia.org/wiki/%D0%A2%D0%B0%D1%94%D0%BC%D0%BD%D0%B8%D1%86%D1%8F_%D0%B7%D0%B2%27%D1%8F%D0%B7%D0%BA%D1%83), захист від [втручання в особисте та сімейне життя](https://uk.wikipedia.org/wiki/%D0%97%D0%B0%D1%85%D0%B8%D1%81%D1%82_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97)), так і для захисту інтересів суспільства (обмеження в період дії надзвичайного або воєнного стану)[[1]](https://uk.wikipedia.org/wiki/%D0%A1%D0%B2%D0%BE%D0%B1%D0%BE%D0%B4%D0%B0_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97#cite_note-dic_economic_law-1).

**2. Право на доступ до інформації.**Право на доступ до інформації — гарантоване статтею 34 Конституції України, а саме:  
- право кожного на свободу думки і слова, на вільне вираження своїх поглядів і переконань;  
- право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб на свій вибір.

**3. Обмеження свободи інформації: підстави та критерії.**Право на доступ до інформації може бути обмежене законом:

* в інтересах національної безпеки,
* в інтересах територіальної цілісності
* в інтересах громадського порядку
* з метою запобігання заворушенням чи злочинам,
* для охорони здоров'я населення,
* для захисту репутації або прав інших людей,
* для запобігання розголошенню інформації, одержаної конфіденційно,
* для підтримання авторитету і неупередженості правосуддя.

**4. Поняття та види незаконної інформації**В самом общем смысле к «незаконной» принято относить информацию, распространение которой запрещено рядом правовых норм, как то: детская порнография, призывы к терроризму и насилию, сегрегация, разжигание конфликтов на религиозной или этнической почве, равно как и недостоверная реклама или распространение порочащих сведений, в том числе и о государственных лидерах.

**Тема 1.5. Трансформаційні процеси в системах забезпечення національної та міжнародної безпеки (інформаційні війни )**

**1. Міжнародно-правове регулювання інформаційної безпеки**

Глобалізація сучасного інформаційного середовища призводить до послаблення інформаційного суверенітету держави, а рівень розвитку та безпека інформаційного середовища впливають на стан політичної, економічної, військової та інших складових безпеки кожної країни. Саме тому одним з напрямів міжнародної діяльності в інформаційній сфері є формування та розвиток системи заходів гарантування безпеки міждержавного обігу інформації, а найважливішим засобом забезпечення інформаційної безпеки виступає право. Основним завданням суб’єктів міжнародних відносин є розробка та удосконалення сучасної системи правової охорони та захисту інформації, що викликано розширенням міжнародних інформаційних зв’язків.

Основні засади міжнародної інформаційної безпеки закладені в Статуті ООН, серед цілей якої виділяються підтримка міжнародного миру та безпеки, повагу до прав людини та основних свобод для всіх незалежно від раси, статі, мови, віросповідання.

До вирішення проблем міжнародної інформаційної безпеки долучилося ряд інших впливових міжнародних організацій, які включили у сферу своєї нормотворчої діяльності питання правової охорони та захисту інформації. Ці питання включені до

* Договору про принципи діяльності держав по дослідженню і використанню космічного простору, включаючи Місяць та інші небесні тіла, 1967 р.;
* Конвенції по морському праву 1982 р.;
* Договору про нерозповсюдження ядерної зброї від 1 липня 1968 р.;
* Договору про обмеження систем ПРО від 26 травня 1972 р.;
* Конвенцію про заборону хімічної зброї, яка набула чинності 29 квітня 1997 р.;
* Конвенцію про заборону біологічної зброї, що набула чинності 26 березня 1975 р.;
* Конвенцію про заборону застосування, накопичення запасів, виробництва і передачі протипіхотних мін і про їх знищення від 18 вересня 1997 р. тощо.

Норми, що містяться в таких міжнародних актах мають універсальний характер, оскільки урегульовують не тільки відносини певної сфери, але опосередковано відносини, пов’язані зправами та свободами людини в інформаційній сфері та відносини у сфері інформаційної безпеки.

**2. Міжнародно-правовий режим критичної інформаційної інфраструктури**

Критичні інфраструктури - це системи, що мають найбільш важливе значення в захисті людського життя, забезпеченні економічної стабільності та національної безпеки. Незважаючи на те, що термін «захист критичних інфраструктур» не використовується у Конвенціях, у них визнається безпека людини, зокрема цивільного населення. Велике значення в праві збройних конфліктів надається захисту цивільних об'єктів - «цивільні об'єкти не повинні бути об'єктом нападу або репресалій».

До критичної інфраструктури нажелать система доменних імен Інтернету, комунікаційні супутники, міжконтинентальні кабелі і маршрутизатори та ін.

Конвенції виключають такого роду об'єкти з числа можливих об'єктів атаки, а також гарантує їм захист і обережне поводження. У разі припинення дії такого статусу цивільних об'єктів, атакуюча сторона зобов'язується зробити належне попередження.  
  
Серед критичних інформаційних інфраструктур можна виокремити лише незначну кількість систем, що використовуються виключно в цивільних цілях, що звужує можливість застосування норм гуманітарного права. Цивільні інформаційні ресурси і системи не мають відмітних знаків, що потенційно підвищує їх вразливість і знижує ступінь захисту.

**3. Концепція кібермиру**П'ять принципів кібермиру, сформульованих Генеральним секретарем МСЭ паном Хамадуном Турі, визначають конкретні дії та зобов'язання, які забезпечать мир і стабільність в кіберпросторі. Ці принципи свідчать, що:  
1. Кожен уряд повинен узяти на себе зобов'язання дати своєму народу доступ до засобів зв'язку.  
2. Кожен уряд візьме на себе зобов'язання захищати своїх людей в кіберпросторі.  
3. Кожна країна візьме на себе зобов'язання не укривати терористів/злочинців на своїх територіях.  
4. Кожна країна повинна взяти на себе зобов'язання не застосовувати першою кібернапади по відношенню до інших країн.  
5. Кожна країна повинна узяти на себе зобов'язання взаємодіяти з іншими країнами у рамках міжнародної співпраці для забезпечення миру в кіберпросторі.

**4. Сучасні види воєн (інформаційні, ідеологічні, економічні, гібридні тощо)**

**Інформаці́йна війна́** — використання і управління [інформацією](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%8F) з метою набуття конкурентоздатної переваги над супротивником.

Інформаційна війна може включати в себе

* збір тактичної інформації,
* забезпечення [безпеки](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) власних [інформаційних ресурсів](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%B8%D0%B9_%D1%80%D0%B5%D1%81%D1%83%D1%80%D1%81),
* поширення [пропаганди](https://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%BF%D0%B0%D0%B3%D0%B0%D0%BD%D0%B4%D0%B0) або [дезінформації](https://uk.wikipedia.org/wiki/%D0%94%D0%B5%D0%B7%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%8F), щоб деморалізувати військо та населення ворога,
* підрив якості інформації супротивника і попередження можливості збору інформації супротивником.

Мета інформаційної війни — послабити моральні і матеріальні сили супротивника або конкурента та посилити власні. Вона передбачає заходи пропагандистського впливу на свідомість людини в ідеологічній та емоційній галузях. Очевидно, що інформаційна війна — складова частина ідеологічної боротьби. Вони не призводять безпосередньо до кровопролиття, руйнувань, при їх веденні немає жертв, ніхто не позбавляється їжі, даху над головою. І це породжує небезпечну безпечність у ставленні до них. Тим часом, руйнування, яких завдають інформаційні війни у суспільній психології, психології особи, за масштабами і за значенням цілком співмірні, а часом і перевищують наслідки збройних воєн.

**Психологі́чна війна́ —** сукупність різних форм, [методів](https://uk.wikipedia.org/wiki/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4) і засобів впливу на людину з ціллю зміни в бажаному напрямку її [психологічних](https://uk.wikipedia.org/wiki/%D0%9F%D1%81%D0%B8%D1%85%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%8F) характеристик (поглядів, думок, цінністних орієнтацій, настроїв, установок, мотивів, стереотипів поведінки), а також групових норм, масових настроїв, [суспільної свідомості](https://uk.wikipedia.org/wiki/%D0%A1%D1%83%D1%81%D0%BF%D1%96%D0%BB%D1%8C%D0%BD%D0%B0_%D1%81%D0%B2%D1%96%D0%B4%D0%BE%D0%BC%D1%96%D1%81%D1%82%D1%8C) в цілому.

**Мереже́ва війна́** — форма ведення конфліктів, коли її учасники застосовують мережеві форми організації, [доктрини](https://uk.wikipedia.org/wiki/%D0%94%D0%BE%D0%BA%D1%82%D1%80%D0%B8%D0%BD%D0%B0), [стратегії](https://uk.wikipedia.org/wiki/%D0%A1%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D1%96%D1%8F) та технології, пристосовані до сучасної інформаційної доби. Звичайними учасниками таких мереж можуть бути [терористи](https://uk.wikipedia.org/wiki/%D0%A2%D0%B5%D1%80%D0%BE%D1%80%D0%B8%D0%B7%D0%BC), кримінальні угруповання, [громадські організації](https://uk.wikipedia.org/wiki/%D0%93%D1%80%D0%BE%D0%BC%D0%B0%D0%B4%D1%81%D1%8C%D0%BA%D0%B8%D0%B9_%D0%B4%D1%96%D1%8F%D1%87) та [соціальні рухи](https://uk.wikipedia.org/wiki/%D0%A0%D1%83%D1%85_%D1%81%D0%BE%D1%86%D1%96%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9), які використовують [децентралізацію](https://uk.wikipedia.org/wiki/%D0%94%D0%B5%D1%86%D0%B5%D0%BD%D1%82%D1%80%D0%B0%D0%BB%D1%96%D0%B7%D0%B0%D1%86%D1%96%D1%8F) та є гнучкими [мережевеми соціальними структурами](https://uk.wikipedia.org/wiki/%D0%A1%D0%BE%D1%86%D1%96%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B0).

ІТ

**Кібервійна́** — [комп'ютерне](https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80) протистояння у просторі [Інтернету](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82).

Спрямована передусім на дестабілізацію [комп'ютерних систем](https://uk.wikipedia.org/w/index.php?title=%D0%9A%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0_%D1%81%D0%B8%D1%82%D0%B5%D0%BC%D0%B0&action=edit&redlink=1) і доступу до інтернету державних установ, фінансових та ділових центрів і створення безладу та хаосу в житті країн, які покладаються на інтернет у повсякденному житті. Міждержавні стосунки і політичне протистояння часто знаходить продовження в інтернеті у вигляді кібервійни: [вандалізмі](https://uk.wikipedia.org/wiki/%D0%92%D0%B0%D0%BD%D0%B4%D0%B0%D0%BB%D1%96%D0%B7%D0%BC),[пропаганді](https://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%BF%D0%B0%D0%B3%D0%B0%D0%BD%D0%B4%D0%B0), [шпигунстві](https://uk.wikipedia.org/wiki/%D0%A8%D0%BF%D0%B8%D0%B3%D1%83%D0%BD%D1%81%D1%82%D0%B2%D0%BE), та безпосередніх атаках на комп'ютерні системи та [сервери](https://uk.wikipedia.org/wiki/%D0%A1%D0%B5%D1%80%D0%B2%D0%B5%D1%80).

**Економічна війна** — економічна стратегія, заснована на використанні заходів економічного характеру (наприклад, економічної блокади, торговельних обмежень тощо), направлених на ослаблення економіки іншої держави або блоку держав. Економічна війна може бути складовою економічного протистояння або складовою [гібридної війни](https://uk.wikipedia.org/wiki/%D0%93%D1%96%D0%B1%D1%80%D0%B8%D0%B4%D0%BD%D0%B0_%D0%B2%D1%96%D0%B9%D0%BD%D0%B0), класична війна звичайно передбачає повне припинення будь яких економічних відносин між країнам-ворогами.

**Гібридна війна** — [війна](https://uk.wikipedia.org/wiki/%D0%92%D1%96%D0%B9%D0%BD%D0%B0), основним інструментом якої є створення державою-агресором в державі, обраній для агресії, внутрішніх протиріч та конфліктів з подальшим їх використанням для досягнення політичних цілей агресії, які звичайно досягаються звичайною війною.

**Тема 2.1. Інформаційні ресурси.**

**1. Поняття «інформаційний ресурс».**

Загальне визначення інформаційного ресурсу міститься у ст. 1 Закону України “Про Національну програму інформатизації”, де інформаційні ресурси визначаються як “**сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо)**”.

У більш конкретному вигляді під інформаційними ресурсами розуміють організовану сукупність інформації, інформаційних продуктів та інформаційних технологій, які призначені для інформаційного забезпечення життєдіяльності людини, суспільства та держави. Тому, книги (найперші інформаційні ресурси), музеї, бібліотеки, архіви тощо – все це інформаційні ресурси.

**2. Законодавче визначення типів та видів інформаційних ресурсів.**

На законодавчому рівні України визначаються тільки інформаційні ресурси науково-технічної інформації та інформаційні ресурси спільного користування.

Згідно зі ст. 1 Закону України “Про науково-технічну інформацію”:

- під інформаційними ресурсами науково-технічної інформації розуміється систематизоване зібрання науково-технічної літератури і документації, зафіксоване на паперових чи інших носіях;

- під інформаційними ресурсами спільного користування розуміється сукупність інформаційних ресурсів державних органів науково-технічної інформації, наукових та науково-технічних бібліотек, центрів, фірм, організацій, які займаються науково-технічною діяльністю і з власниками яких укладено договори про їх спільне використання.

**3. Законодавче забезпечення доступу до інформаційних ресурсів.**

**4. Законодавче обмеження доступу до інформаційних ресурсів**

**Тема 2.2. Інформаційний та кіберпростір**

**1. Інформаційний простір**

Під **інформаційним простором** ми розуміємо, перш за все, територію розповсюдження інформації за допомогою конкретних компонентів національної системи інформації за допомогою інформації і зв’язку, діяльність якої має гарантоване правове забезпеченняУ формуванні українського національного інформаційного простору, крім традиційних ЗМІ, сьогодні активну роль відіграють новітні електронні ЗМІ, серед яких, на думку сучасних дослідників, найважливішими є такі.

1. **Кабельне телебачення.** Кабельне телебачення розраховане в основному на поширення розважальних програм, але може мати й суспільно-політичні за характером передачі.

2. **Відеомагнітофони** - апарати, призначені для записування та відтворення аудіовізуальних програм та інших журналістських матеріалів. Інформація для них поширюється на касетах і має переважно культурно-розважальний характер, що не виключає поширення через цей спосіб ЗМІ всіх інших типів інформації. Відеомагнітофони широко використовуються для реклами.

3. **Телеконференції** - встановлення зв'язку за допомогою супутникової техніки між двома точками землі незалежно від відстані та регіону з метою спілкування між групами людей, участі їх в обговоренні важливих суспільних проблем тощо.

**4. Електронна пошта (e-mail)** - спосіб передачі кореспонденції між двома віддаленими точками негайно за допомогою міжнародної системи комп'ютерного зв'язку.

5. Електронні банки даних - це великі комп'ютери, у яких нагромаджують і зберігають найрізноманітнішу інформацію, що доступна для підключених до них через систему ЕОМ абонентів.

6. **Відеогазети.** У цьому випадку газета виготовляється, але не віддруковується, а лишається в комп'ютері і стає доступною підключеним до нього абонентам, які зчитують її з екрана, а потрібні статті можуть самі віддрукувати на принтері. Усе більше поширюється практика розміщення електронного варіанту газети чи журналу в системі Інтернет.

7. Мессенджери. Миттєвий обмін повідомленнями

На особливе місце в сучасному світовому інформаційному просторі висунулася комп'ютерна мережа Інтернет. Власне, кілька вже розглянутих новітніх засобів масової інформації (телеконференції, електронна пошта, відеогазети) діють лише завдяки налагодженій системі світового комп'ютерного зв'язку. Це спонукає говорити про Інтернет окремо, вбачаючи в ньому новий тип журналізму в цілому.

**Інтернет - найбільша в світі комп'ютерна мережа,** утворена з мстою нагромадження, обміну і швидкісного поширення інформації.

**До складу світової системи Інтернет** входять національні мережі багатьох країн світу, регіональні, локальні мережі та персональні комп'ютери приватних користувачів.

**Інформаційне суспільство несе в собі й загрозу людству:** ану ж глобальна інформаційна система опиниться в руках невеликої групи людей, що переслідують свої, далеко не гуманні цілі. Перед людством стоїть завдання - впоратися з цією проблемою за допомогою Колективного Розуму.

**Головне завдання Колективного Розуму - об'єднання людства за допомогою інформаційного обміну в одну загальнолюдську спільноту.** Найважливішу роль у цьому повинна відіграти й уже зараз відіграє журналістика. Колективний Розум призведе до якісної зміни соціальної структури суспільства, системи звичаїв, а найбільш істотне - перетворить "четверту владу" на складову Колективного Розуму, на найважливіший механізм самоорганізації суспільства, що спрямовує його розвиток на формування нового гомеостазу.

**2. Кіберпростір**

Кіберпростір — інтерактивне інформаційне середовище, яке функціонує за допомогою комп'ютерних систем.

Кіберпростір характеризується трьома основними ознаками:

* це інформаційний простір;
* він є комунікативним середовищем;
* утворюється за допомогою технічних (комп'ютерних) систем.

Кіберпростір можна розглядати як локальне середовище, у випадку функціонування засобу комп'ютерної техніки, який не підключено до мережі, та як розосереджене середовище, яке виникає в разі підключення засобу комп'ютерної техніки до локальної глобальної мережі передачі даних (Інтернет)

**3. Особливості правового регулювання інформаційного простору**

Термін "єдиний інформаційний простір" по-різному вживається в нормативних правових актах і науковій літературі.

**З точки зору інформаційної безпеки**: словник термінів і визначень у галузі інформаційної безпеки визначив інформаційний простір як сукупність інформації та інформаційної інфраструктури; сферу діяльності, пов’язану із створенням, перетворенням і використанням інформації, включаючи індивідуальне і суспільне створення, інформаційно-телекомунікаційну інфраструктуру і власну інформацію.

Рішення про розроблення проекту Концепції формування інформаційного простору Співдружності Незалежних Держав, яке підписав Уряд України 03.11.1995 р., встановило формування єдиного інформаційного простору головною метою здійснення державної політики у галузі інформатизації.

Формування та розвиток єдиного інформаційного простору України передбачає насамперед забезпечення оперативного доступу до наявних інформаційних ресурсів і проведення робіт з їх включення в єдиний інформаційний простір, що було реалізовано у Законі України “Про Національну програму інформатизації”.

Згідно з Законом України “Про Концепцію Національної програми інформатизації”, основу інформаційного простору органів державної влади повинні становити інформаційно-телекомунікаційні системи, здатні забезпечити інформаційну підтримку прийняття рішень і у сфері управління економікою, і в галузі безпеки особистості, суспільства, держави.

Реалізація цієї Концепції дала змогу, зокрема, правоохоронним органам розпочати інтеграцію своїх інформаційних систем з інформаційними системами інших державних структур. Одним із завдань Концепції є забезпечення відкритості у діяльності органів державної влади та загальнодоступності державних інформаційних ресурсів, створення умов для ефективної взаємодії між органами державної влади та громадянами на основі використання інформаційних та комунікаційних технологій.

Базовим у сфері формування єдиного інформаційного простору України є Закон “Про захист інформації в інформаційно-телекомунікаційних системах”. В ст. 1 закону закріплений основний понятійний апарат в інформаційній сфері: виток інформації, володілець інформації, власник системи, доступ до інформації в системі, захист інформації в системі, знищення інформації в системі, інформаційна (автоматизована) система, комплексна система захисту інформації, користувач інформації в системі, криптографічний захист інформації.

**4. Особливості правового регулювання кіберпростору**

Правове регулювання кіберпростору - це цілеспрямований вплив на процеси у цифровому середовищі мережі Інтернет правовими засобами з метою їх впорядкування та розвитку. Це також плив на поведінку суб’єктів права за допомогою норм права, що забезпечує їх нормальну роботу.

Інтернет формує особливу інформаційну сферу (Інтернет-сферу), пов’язану з оборотом цифрової інформації. Таким чином, *Інтернет-відносини* – це суспільні відносини, що пов’язані з соціально-правовим регулюванням віртуального простору, тобто з регулюванням цього простору за допомогою норм права, моралі, етики та інших засобів.

«Інтернет» як сукупність інформаційних ресурсів непідконтрольний якійсь конкретній особі держави або міжнародній організації.

* По-перше, кожен провайдер має можливість контролювати інформацію, яка передається в мережу або виходить з мережі при користуванні його послугами. У цьому сенсі кожен провайдер має потенційну можливість встановлювати певні стандарти користування мережею для своїх клієнтів [24, c. 80].
* По-друге, держава має можливість регулювати і контролювати діяльність провайдерів, що надають послуги на його території, за допомогою різних юридичних інститутів.
* По-третє, режим інформаційного обміну з використанням мережі Інтернет може бути предметом міжнародно-правового регулювання.

**Тема 2.3. Правове забезпечення інформаційної безпеки за законодавством України**

**1. Інформаційна безпека держави**

**Інформаційна безпека держави** — це стан її захищеності, при якому спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів, комп'ютерні злочини та інший деструктивний інформаційний вплив не завдає суттєвої шкоди національним інтересам.

Виокремлюють три рівня забезпечення інформаційної безпеки:

* рівень особи (формування раціонального, критичного мислення на основі принципів свободи вибору);
* суспільний рівень (формування якісного інформаційно-аналітичного простору, плюралізм, багатоканальність отримання інформації, незалежні потужні ЗМІ, які належать вітчизняним власникам);
* державний рівень (інформаційно-аналітичне забезпечення діяльності державних органів, інформаційне забезпечення внутрішньої і зовнішньої політики на міждержавному рівні, система захисту інформації з обмеженим доступом, протидія правопорушенням в інформаційній сфері, комп’ютерним злочинам)

**2. Об’єкти інформаційної безпеки держави**

**Об'єктами інформаційної безпеки України є:**

* людина і громадянин - їхні конституційні права і свободи, фізичне та психологічне здоров'я, захищеність від негативного впливу інформаційних технологій та інформації;
* суспільство і держава - захищеність їх законних інтересів в інформаційній сфері;
* інформаційні ресурси та інформаційна інфраструктура - їх цілісність, доступність та захищеність.

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

**3. Суб’єкти інформаційної безпеки держави**

До суб'єктів інформаційної безпеки відносяться:

* держава, що здійснює свої функції через відповідні органи;
* громадяни,
* суспільні або інші організації і об'єднання, що володіють повноваженнями по забезпеченню інформаційної безпеки у відповідності до законодавства.

**Тема 2.4. Правове регулювання Інтернету**

**1. Основні етапи виникнення та розвитку Інтернету.**

Історія INTERNET починається з 1969 року, коли Міністерством Оборони США було ініційовано створення першої локальної мережі під назвою ARPANET (адміністрування передових дослідницьких проектів). Метою цих досліджень було вивчення можливостей об’єднання ресурсів багатьох комп’ютерів в єдиній системі. Спочатку мережа складалась з чотирьох комп’ютерів (трьох в Каліфорнії та одного в Юті).

Створення ARPANET було експериментом уряду США в галузях мереж комутацій пакетів. ARPA, (Department of Defense (DOD) Advanced Research Projects Agency - Агенство Перспективних досліджень Міністерства оборони США), який пізніше став називатися DARPA (Defense Advanced Research Projects Agency), об’єднало дослідників, надавши їм можливість колективно використовувати апаратні і програмні ресурси, бази даних, та іншу інформацію. Через деякий час до ARPANET були підключені інші експериментальні мережі: PRNET (packet radio) і SATNET (packet satellite). Об’єднання мереж було реалізовано з використанням розробленої спеціально для цієї мети технології міжмережної взаємодії TCP/IP, фінансованої DARPA.

Ця мережа з’єднувала науковців, задіяних у військовій тематиці, з окремими комп’ютерними центрами. В 1986р. Міністерство оборони розділило цю систему на дві підсистеми – військову і цивільну (ARPANET і MILNET ) у зв’язку з проханням науковців США, але з’єднання, зроблене між мережами, дозволило їм взаємодіяти між собою.

Це перше міжмережне з’єднання було названо DARPA Internet, пізніше перше слово було опущено і нове міжмережне з’єднання почали називати INTERNET. Велике значення для розвитку ARPAnet мала поява Ethernet технології - технології локальних мереж. Це дозволило підключати до ARPANET не тільки окремі комп’ютери, але і локальні та корпоративні мережі великих організацій. На початковій стадії розвитку доступ до ARPANET обмежувався військовими та організаціями, які працювали за контрактом з військовими, університетами, що виконували військові замовлення. В кінці 1970-х років була створена нова глобальна мережа, яка обслуговувала університетські колективи і частково комерційні організації: UUCP, мережу комп’ютерів, працюючих під керівництвом операційної системи UNIX і USENET - всесвітню мережу телеконференцій.

**2. Основні поняття та ознаки Інтернету.**

На основі зазначеного вище тлумачення сутності поняття "Інтернет” можна визначити основні підходи до правових аспектів цього явища:

*Інтернет в цілому не с суб’єктом права.* Це є сукупність інформа­ційного обладнання та інформаційних ресурсів. Але він не є ні міжна­родною організацією, ні юридичною особою, ні будь-якою іншою ор­ганізованою структурою, яка може вступати в правовідносини.

*Інтернет у цілому не с об'єктом права.* В Інтернет немає єдино­го конкретного власника, як і немає такого суб'єкта, який би управ­ляв або контролював досить значну частину цієї мережі. Понад те, че­рез технічні особливості жодна складова Інтернет не є критичною для функціонування всієї системи.

До основних *ознак мережі Інтернет* можна віднести такі:

1. Інтернет як технологічна система, що забезпечує обмін інформацією між комп’ютерами є різновидом мережі електрозв’язку – телекомунікаційної мережі;
2. Інтернет як система інформаційного зв’язку регулює суспільні відносини з приводу обміну даними;
3. глобальний, екстериторіальний, міжнародний характер Інтернету;
4. Інтернет відкритий для використання всіма фізичними та юридичними особами, тобто є мережею зв’язку загального користування;
5. мережа Інтернет призначена для передачі (обміну) електронних даних.-+

Необхідно зазначити, що серед фахівців (насамперед в технічній сфері) існує вкрай негативне ставлення до самої ідеї правового регулювання відносин, що виникають в Інтернет – середовищі. У мережі навіть була поширена «Декларація незалежності кіберпростору» (автор – Джон Барлоу) [27], в якій проголошувалося право на свободу Інтернет – простору та принцип невтручання держав у регулювання Інтернет – відносин.

**3. Структура інтернету. Darknet i Deepweb**

Даркнет — оверлейна мережа, доступ до якої можливий лише через певне програмне забезпечення, налаштування чи авторизацію, часто з використанням нестандартних комунікаційних протоколів та портів. Типовими мережами такого типу є friend-to-friend мережі (зазвичай використовуються для спільного користування файлами та peer-to-peer з'єднання) та приватних мереж на кшталт Tor.

Загалом даркнети може бути використано з багатьох причин на кшталт:

1. для кращого захисту права громадян на приватне життя від точкового та масового спостереження
2. для захисту дисидентів від політичної розправи
3. написання доносів та витік новин
4. інформаційні злочини (хакерство, пошкодження файлів тощо)
5. Продаж заборонених товарів на ринках даркнетів
6. Спільне користування файлами (Варез, особисті та конфіденційні файли, порнографія, нелегальне та контрабандне програмне забезпечення тощо).

Глибинна мережа, невидима мережа чи прихована мережа – це частка всесвітньої мережі інтернет, вміст якої за жодних обставин не індексують стандартні пошукові онлайн-системи. Глибинна мережа є протилежним явищем до поверхневої мережі.

Серед поширених застосувань глибинної мережі є такі, як онлайн-листування, інтернет-банкінг, а також платні послуги на кшталт відео на вимогу, доступ до яких здійснюється через так звану платну стіну (Paywall), та багато іншого.

Інформатик Майк Бергман започаткував цей термін у 2000 році як термін пошукового індексування.

Методи запобігання індексування веб-сторінок можна розбити на такі категорії:

1. Контекстна мережа.
2. Динамічний контент.
3. Вміст з обмеженим доступом.
4. Не-HTML/текстовий вміс.
5. Приватна мережа.
6. Скриптований контент.
7. Програмне забезпечення.
8. Незв'язаний вміст.
9. Мережеві архіви.

**4. ІКАНН, МСЕ та інші органи управління інтернетом**

**ІКАНН -** Інтернет корпорація з присвоєння імен та номерів міжнародна некомерційна організація, створена восени 1998 за участю уряду США для регулювання питань, пов'язаних з доменними іменами, [IP-адресами](https://uk.wikipedia.org/wiki/IP-%D0%B0%D0%B4%D1%80%D0%B5%D1%81%D0%B0) і іншими аспектами функціонування Інтернету.

Діяльність ICANN істотно змінила вигляд Інтернету. До 1998 реєстрацією імен в доменах загального користування займалася тільки одна компанія. Подібний монополізм обумовлював високу вартість реєстрації — кожен домен в зонах [.com](https://uk.wikipedia.org/wiki/.com), [.net](https://uk.wikipedia.org/wiki/.net)і [.org](https://uk.wikipedia.org/wiki/.org) щороку обходився його власнику в $50. Це, у свою чергу, було однією з причин, які перешкоджали зростанню кількості зареєстрованих доменних імен: у 1998 році у світі їх налічувалося всього три мільйони.

**МСЕ -** Міжнаро́дний сою́з електрозв'язку (МСЕ) ([англ.](https://uk.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0) *International Telecommunication Union, ITU*) — міжнародна організація, що визначає стандарти (точніше, за термінологією МСЕ — Рекомендації, [англ.](https://uk.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0) *Recommendations*) в галузі телекомунікацій та [радіо](https://uk.wikipedia.org/wiki/%D0%A0%D0%B0%D0%B4%D1%96%D0%BE). Це, імовірно, найстарша з нині існуючих міжнародних організацій, вона була заснована в [Парижі](https://uk.wikipedia.org/wiki/%D0%9F%D0%B0%D1%80%D0%B8%D0%B6) ще [17 травня](https://uk.wikipedia.org/wiki/17_%D1%82%D1%80%D0%B0%D0%B2%D0%BD%D1%8F) [1865](https://uk.wikipedia.org/wiki/1865) року під назвою «Міжнародний телеграфний союз» ([фр.](https://uk.wikipedia.org/wiki/%D0%A4%D1%80%D0%B0%D0%BD%D1%86%D1%83%D0%B7%D1%8C%D0%BA%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0) *Union internationale du telegraphe*). В основному МСЕ займається розподілом радіочастот, міжнародною телефонною організацією та організацією радіозв'язку, стандартизацією телекомунікаційного обладнання. Зараз МСЕ офіційно є спеціалізованим агентством [ООН](https://uk.wikipedia.org/wiki/%D0%9E%D0%9E%D0%9D) і має штаб-квартиру в [Женеві](https://uk.wikipedia.org/wiki/%D0%96%D0%B5%D0%BD%D0%B5%D0%B2%D0%B0) ([Швейцарія](https://uk.wikipedia.org/wiki/%D0%A8%D0%B2%D0%B5%D0%B9%D1%86%D0%B0%D1%80%D1%96%D1%8F)) поруч з Палацом Націй (Європейське відділення ООН).

**ISOC**  (англ. Internet Society) — Інтернет Суспільство, професійна організація фахівців, яка формує політику і практику Інтернету і здійснює спостереження за іншими організаціями, пов'язаними з питаннями мережевої політики. Своєю місією ISOC вважає «забезпечення відкритого розвитку, еволюції і використання Інтернету на благо людей у всьому світі». ISOC займається не тільки стандартизацією Інтернету, але і питаннями освіти в країнах, що розвиваються, професійної підготовки фахівців, управління і координації різних проектів, так або інакше пов'язаних з Інтернетом.

**5. Мережевий нейтралітет**

Мережевий нейтралітет (англ. *Network neutrality*, NN) — принцип, відповідно до якого провайдери телекомунікаційних послуг не віддають переваги одному цільовому призначенню перед іншим, або одним класам додатків (наприклад World Wide Web) перед іншими (наприклад, онлайн-ігри або IP-телефонія). Хоча сам цей термін новий, його фундаментальна ідея бере початок в епоху винаходу телеграфу в середині XIX століття. Телеграми доставлялися 'однаково', на рівних умовах, без спроб розрізняти їх зміст і регулювати їх приналежність до того чи іншого технічного способу доставки. Така мережа «від початку до кінця нейтральна».

**Тема 2.5 Е-демократія**

**1. Електронна демократія та її складові**

Електронна демократія (е-демократія) – форма суспільних відносин, за якої громадяни та організації залучаються до державотворення та державного управління, а також до місцевого самоуправління шляхом широкого застосування інформаційно-комунікаційних технологій.[[1]](https://uk.wikipedia.org/wiki/%D0%95%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0_%D0%B4%D0%B5%D0%BC%D0%BE%D0%BA%D1%80%D0%B0%D1%82%D1%96%D1%8F#cite_note-1)

Українське законодавство визначає електронну демократію як форму суспільних відносин, за якої громадяни та інститути громадянського суспільства залучаються до [державотворення](https://uk.wikipedia.org/wiki/%D0%94%D0%B5%D1%80%D0%B6%D0%B0%D0%B2%D0%BE%D1%82%D0%B2%D0%BE%D1%80%D0%B5%D0%BD%D0%BD%D1%8F) та державного управління, до місцевого самоврядування шляхом широкого застосування інформаційно-комунікаційних технологій в демократичних процесах, з метою:

* посилити участь, ініціативність та залучення громадян на всіх рівнях до публічного життя;
* поліпшити прозорість процесу прийняття рішень, підзвітність демократичних інститутів;
* поліпшити реакцію суб’єктів владних повноважень на звернення громадян;
* сприяти публічним дискусіям та привертати увагу громадян до процесу прийняття рішень.[2]

*Складові е-демократії:* електронний парламент, електронне законодавство, електронний суд, електронне посередництво, електронні вибори, електронний референдум, електронне голосування, електронні петиції, електронні кампанії, електронні опитування тощо

**2. Правове регулювання е-демократії у світі та в Україні**

**“Про схвалення Концепції розвитку електронної демократії в Україні та плану заходів щодо її реалізації”**

**3. Цифрова диктатура**

Імідж цифрової диктатури дуже сильно закріпився за Китаєм

Після приходу до влади Сі Цзіньпіна Держрада КНР в 2014 році опублікувала новий документ - "Програму створення системи соціального кредиту (2014-2020)".

З програми слідує, що до 2020 року не тільки кожна компанія, але і кожен житель материкового Китаю буде відслідковуватися і оцінюватися цією системою в режимі реального часу. Рейтинг довіри фізосіб буде прив'язаний до внутрішнього паспорту. Рейтинги будуть публікуватися в централізованій базі даних в інтернеті у вільному доступі.

Інститут політичних досліджень Asan (Республіка Корея) назвав систему соціального кредиту "кошмаром Джорджа Оруелла". Час покаже, чи перетвориться система соціального кредиту в небачену раніше цифрову диктатуру XXI століття, всевидющого Великого брата, який невсипно стежить за тобою. Неясно також, чи буде існувати якийсь контроль і обмеження для самого Великого брата. Поки ж цілком резонним для жителів Китаю здається рада Оруелла з "1984": якщо хочеш зберегти секрет, треба приховувати йогоі від себе.

**4. Загрози демократичним процессам, що повязані з використанням інформаційних впливів та ІТ**Однією з таких загроз є **постправда** - обставини, за яких суспільна думка ігнорує об'єктивні факти на користь звернень до емоцій та особистих переконань.

Визначною рисою політики постправди є те, що тези, які впливають на суспільну думку, повторюються навіть після того, як вони були спростовані з наведенням доказів.

Прикладами є:

1. Кампанія організації Vote Leave перед проведенням референдума про вихід Великобританії з ЄС.

До дня проведення референдума робились численні заяви про те, що перебування в ЄС коштує 350 мільйонів фунтів на тиждень, хоча неодноразово було наведено документальні докази того, що наведена сума набагато перевищує дійсність. Кампанія зазнала успіху.

2. Президентська кампанія Мітта Ромні 2012 року, в ході якої він обіцяв відмінити скорочення витрат на оборону, хоча насправді витрати на оборону під час президентства Обами тільки виросли.

3. Президентська кампанія Дональда Трампа, який неодноразово робив провокативні та шокуючі заяви про імігрантів, Іслам, своїх конкурентів та ін. Більшу частину цих заяв було спростовано з наведенням доказів, проте згідно опитувань, Трампа вважали більше заслуговючим на довіру, ніж його опонента.

**Тема 2.6. Безпека в ІТ-праві**

**1. ІТ-право в Україні**

**2. Трудові відносини в ІТ-галузі**В угодах в IT-секторі кадри відіграють вирішальне значення, саме тому інвестори часто вирішують придбавати саме компанію, а не, скажімо, її активи. І саме тому дотримання правил трудового законодавства під час працевлаштування співробітників і надалі є таким значимим, а помилки потенційних продавців у веденні кадрової політики коштують так дорого.  
  
Типовою схемою ведення бізнесу в IT-сфері є співпраця з ФОП, що перебувають на спрощеній системі оподаткування, а не з працевлаштованими спеціалістами. Вигідність такої схеми, яку через неабияку популярність нарекли "внутрішнім українським офшором", важко не помітити, адже замість усіх податків і соціальних відрахувань, що підлягають сплаті роботодавцем від розміру заробітної плати (18 % – ПДФО, 1,5 % – військовий збір, 22 % – ЄСВ), у випадку із ФОП необхідно сплатити лише 5 % від обороту та 22 % ЄСВ, але від мінімальної зарплати (704 грн у 2017 році).  
  
Проте використання такої системи, якщо відносини з ФОП фактично носять характер трудових, є неправомірним, а тому ризикованим для інвестора. Якщо тіньове працевлаштування буде виявлено, то контролюючі органи можуть донарахувати роботодавцю суми податкових зобов'язань. Крім того, зважаючи на те, що людський капітал є найважливішим ресурсом IT-компанії, покупцю незрозуміло, яким чином утримати всіх ФОП після переходу права власності на корпоративні права в компанії та як убезпечити себе від того, що попередній власник переманить більшість ключових працівників. Рекомендуємо IT-компаніям, які готуються до продажу, укласти трудові договори щонайменше з ключовими працівниками та будувати з ними стосунки в межах трудових відносин.  
  
Виплата "сірих" або "чорних" заробітних плат, працевлаштування працівників без укладення трудового договору, помилки в оформленні кадрової документації також посідають почесні місця серед найпоширеніших порушень роботодавців – українських IT-компаній. До кінця 2017 року в Україні діє мораторій на проведення перевірок підприємств контролюючими органами, а отже перевірки буде ініційовано переважно за наявності скарг третіх осіб. Проте значне підвищення санкцій за такі порушення аж до 320000 гривень з початку 2017 року змушує інвесторів пильніше перевіряти цільові ІТ-компанії й оцінювати потенційні фінансові ризики вищими сумами.

**3. Авторські права на комп’ютерну програму, реєстрація торгових марок та патентів** У нашій країні державна реєстрація авторських прав є стандартною процедурою й проводиться у відповідності до Закону України «Про авторське право і суміжні права» № 3792-12 (далі – Закон), постанови КМУ «Про державну реєстрацію авторського права і договорів, які стосуються права автора на твір» № 1756 від 27.12.2001 р (далі – Порядок). Також під час проведення процедури реєстрації необхідно взяти до уваги те, що при регулюванні деяких положень авторського права Цивільним кодексом (далі – ЦК) та Законом спостерігаються деякі розбіжності через те, що останній був прийнятий пізніше. Все вищенаведене законодвство має застосовуватися з врахуванням угоди про асоціацію між Україною та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами.

З метою захисту будь-якого продукту (комп’ютерна програма, база даних, сайт та ін.) від незаконного привласнення, можна вжити таких дієвих заходів:

1. захистити авторським правом вихідний код програми;
2. захистити алгоритми, які використані у програмі;
3. помістити під охорону закону назву програмного продукту.

Охорона комп’ютерної програми або іншого ідентичного суб’єкту авторським правом відбувається на зразок літературного твору. Авторське право на зазначені продукти виникає у момент їх створення та не вимагає обов’язкової реєстрації.

Відповідно до Закону, комп’ютерна програма – це сукупність інструкцій, які складені у вигляді слів, чисел, певних схем, кодів та інших знаків, які можуть зчитуватися комп’ютером з метою його запуску та досягнення поставленої мети чи результату.

**4. Комерційна таємниця в ІТ-галузі. Угоди про не конкуренцію та про нерозголошення** Неконкуренція тісно пов’язана і з конфіденційністю, зокрема з комерційною таємницею, адже часто працівники, йдучи з фірми, “виносять” з собою інформацію, яку вони застосовували під час своєї роботи. Завжди є ризик, що у результаті “цінний кадр” з “цінною інформацією”, розуміючи можливість самостійно виробляти і продавати продукцію, використовує всі напрацювання компанії і організовує свій бізнес або ж переходить з готовими проектами в інші фірми.

На жаль, в Україні, на відміну від практики розвинених країн світу, зобов’язання про неконкуренцію фактично не мають жодної юридичної сили. Більше того, це стосується як трудових відносин з працівником, так і осіб, що працюють на основі цивільно-правових договорів.

Зрозуміло, що повна заборона займатися тим чи іншим видом діяльності чи виконувати певну роботу не можлива інакше, як на підставі закону та за рішенням суду. Конституція України гарантує кожному право на підприємницьку діяльність, яка не заборонена законом. Відповідно до

ст. 27 Цивільного кодексу України, правочин, що обмежує можливість фізичної особи мати не заборонені законом цивільні права та обов’язки, є нікчемним.

Стаття 5–1 Кодексу законів України про працю встановлює, що держава гарантує працездатним громадянам, які постійно проживають на території України, вільний вибір виду діяльності.

Компанії різними способами намагаються прописати в договорах зобов’язання щодо неконкуренції. Часто на зразок договорів іноземних компаній використовують формулювання щодо “заборони займатися діяльністю, аналогічною до діяльності Компанії, або брати участь у проектах, аналогічних до

проектів Компанії, самостійно чи разом з іншими особами, на певний строк”.

Такі положення обґрунтовують, як правило, принципом свободи договору. Так, ст. 627 Цивільного кодексу України закріплює, що сторони є вільні в укладенні договору, виборі контрагента та визначенні умов Договору з урахуванням вимог ЦК, інших актів цивільного законодавства, звичаїв ділового обороту, вимог розумності та справедливості.

**5. Електронна комерція.** Електронна комерція — це сфера цифрової економіки, що включає всі фінансові та торгові транзакції, які проводяться за допомогою комп'ютерних мереж, та бізнес-процеси, пов'язані з проведенням цих транзакцій.

До електронної комерції відносять електронний обмін інформацією (англ. Electronis Data Interchange, EDI), електронний рух капіталу (англ. Electronic Funds Transfer, EFT), електронну торгівлю (англ. E-Trade), електронні гроші (E-Cash), електронний маркетинг (англ. E-Marketing), електронний банкінг (англ. E-Banking), електронні страхові послуги (англ. E-Insurance) тощо.

B2B електронна комерція — це електронна комерція між компаніями. Це тип електронної комерції, що має справу з відносинами між видами комерційної діяльності. Приблизно 80% електронної комерції належать до цього типу, і більшість експертів пророкує, що B2B електронна комерція продовжить поширюватися швидше ніж B2C.

Електронна комерція бізнес-до-користувача, або торгівля між компаніями й споживачами, включає збирання інформації клієнтами; купівлю фізичних речей чи інформаційних/електронних товарів; і, для інформаційних товарів, одержування товару (програми, електронної книги) по електронній мережі. Це друга по величині й найперша форма електронної комерції.

Електронна комерція споживач-до-споживача або C2C — торгівля між приватними індивідуумами або споживачами. Цей тип електронної комерції характеризований ростом електронних ринків і мережних аукціонів, особливо у вертикальних галузях промисловості. С2С можливо має найбільший потенціал для того, щоб розвивати нові ринки. Цей тип електронної комерції входить принаймні в три форми:

1. аукціони на кшталт eBay, що дозволяє інтерактивно пропонувати ціну в реальному масштабі часу;
2. однорангові системи, типу моделі Napster (протокол спільного використання файлів між користувачами в системах типу IRC) і пізніші моделі обміну грошей;
3. оголошення тематичних категорій у портальних сайтах типу Тематичних категорій Excite і eWanted (діалоговий, мережний ринок, де покупці і продавці можуть вести переговори).

Мобільна торгівля — закупівля й продаж товарів і послуг через бездротову технологію, тобто, кишенькові пристрої типу мобільних телефонів і особистих цифрових помічників.

**6. Спростування недостовірної інформації та відповідальність за її поширення**

Після того, як в 2001 році в Україні зникла кримінальна відповідальність за наклеп, справи про поширення недостовірної інформації (реальне або гадане) розглядають фактично тільки у порядку цивільного судочинства. Специфіка діяльності засобів масової інформації спричинила виникнення низки особливостей їх юридичної відповідальності за поширення недостовірної інформації. Адже поширення інформації це не стільки право ЗМІ, скільки їх основна функція, яку більшість журналістів розглядають як власний обов’язок.

Однією з найхарактерніших особливостей розгляду справ про спростування недостовірної інформації, захист честі, гідності або ділової репутації є коло суб’єктів, які можуть виступати в якості відповідачів по таких справах, тобто тих осіб, на яких позивач хоче покласти відповідальність за поширення інформації. Цивільний кодекс не містить вказівки на можливість притягнення у справах про спростування інформації у якості відповідача іншої особи, крім самого засобу масової інформації (тобто редакції, якщо вона є юридичною особою, засновника ЗМІ). Навпаки, стаття 1172 ЦКУ покладає обов’язок відшкодовувати шкоду, завдану працівником при виконанні трудових (службових) обов’язків або підрядником при виконанні договору підряду, саме на юридичну чи фізичну особу, для якої здійснювалося виконання відповідної роботи. А частина 4 статті 277 цього ж Кодексу встановлює, що поширювачем інформації, яку подає посадова чи службова особа при виконанні своїх посадових/службових обов'язків, вважається юридична особа, у якій вона працює.

**Тема 2.7. Особливості юридичної відповідальності в інформаційній галузі.**

**1. Правопорушення в інформаційній галузі.**

Правонарушения в информационной сфере делятся на проступки (деликты) и преступления. Под правонарушением обычно понимается противоправное виновное нарушение субъектом действующей нормы информационного права, в результате чего наносится существенный вред интересам личности, государства, общества в информационной сфере. Все правонарушения выступают в качестве юридических фактов, причем эти действия или бездействие субъектов могут повлечь для последних неблагоприятные последствия личного, организационного, имущественного характера, вытекающие из санкции нарушенной информационно-правовой нормы в определенном регламентированном порядке.

Наиболее распространенными правонарушениями в информационной сфере являются проступки, имеющие следующие особенности:

— они отличаются незначительной опасностью (вред для общества);

— совершаются в различных областях информационной деятельности;

— направлены на различные объекты и имеют разные юридические последствия.

Проступки подразделяются на дисциплинарные, административные и деликты.

**2. Адміністративно-правові санкції за порушення інформаційного законодавства.**Адміністративна відповідальність — вид юридичної відповідальності громадян і службових осіб за вчинені ними адміністративні правопорушення.  
  
Адміністративно-правовими правопорушеннями визначені, наприклад:  
1) відмова у наданні інформації;  
- несвоєчасне або неповне надання інформації:  
- надання інформації, що не відповідає дійсності, у разі, коли така інформація підлягає наданню на запит громадянина чи юридичної особи відповідно до законів України.  
Посадові особи, які скоїли таке адміністративне правопорушення, притягуються до відповідальності у вигляді штрафу у розмірі від п'ятнадцяти до двадцяти п'яти неоподатковуваних мінімумів доходів громадян.

Повторне протягом року вчинення порушення особою, яка притягалася до адміністративної відповідальності, тягне за собою накладення штрафу на посадових осіб від двадцяти п'яти до п'ятдесяти неоподатковуваних мінімумів доходів громадян;  
2) відмова у наданні за інформаційними запитами повної та достовірної інформації або несвоєчасне її надання.  
У такому випадку на службових та посадових осіб накладається штраф від трьох до десяти неоподатковуваних мінімумів доходів громадян.  
3) Адміністративним правопорушенням визнається також недбале зберігання, псування, знищення, приховування, незаконна передача іншій особі документів Національного архівного фонду або документів, що підлягають внесенню до нього, незаконний доступ до зазначених документів.  
Попередження або накладення штрафу на громадян від трьох до семи неоподатковуваних мінімумів доходів громадян і попередження або накладення штрафу на посадових осіб -від п'яти до десяти неоподатковуваних мінімумів доходів громадян.

4) Порушення законодавства про друковані засоби масової інформації:  
- виготовлення, видання або розповсюдження продукції друкованого засобу масової інформації після припинення діяльності такого ЗМІ;  
- ухилення від перереєстрації друкованого ЗМІ у передбаченому законом порядку чи від повідомлення реєструючому органу про зміну виду видання, юридичної адреси засновника (співзасновників), місця розташування редакції.  
Такі дії тягнуть за собою накладення штрафу від десяти до тридцяти неоподатковуваних мінімумів доходів громадян.

5) Адміністративна відповідальність передбачена і за порушення законодавства про державну таємницю. Такими правопорушеннями є:  
- недодержання встановленого законодавством порядку пере-дання державної таємниці іншій державі чи міжнародній організації;  
- засекречування інформації: про стан довкілля, якість харчо» вих продуктів і предметів побуту; про аварії, катастрофи, небезпечні природні явища та надзвичайні події, які сталися або можуть статися та загрожують безпеці громадян;  
- про факти порушення прав і свобод людини і громадянина:  
- итд

Названі правопорушення тягнуть за собою накладення штрафу на громадян від одного до трьох і на посадових осіб - від трьох до десяти неоподатковуваних мінімумів доходів громадян. Повторне протягом року вчинення порушення тягне за собою накладення штрафу на громадян від трьох до восьми і на посадових осіб - від п'яти до п'ятнадцяти неоподатковуваних мінімумів доходів громадян.  
6) Порушення порядку обліку, зберігання і використання документів та інших носіїв інформації, що містять конфіденційну інформацію, яка є власністю держави, що призвело до розголошення такої інформації.  
Накладення штрафу на громадян від одного до двох і на посадових осіб - від трьох до восьми неоподатковуваних мінімумів доходів громадян. Повторне протягом року вчинення порушення тягне за собою накладення штрафу на громадян від двох до семи і на посадових осіб - від восьми до тринадцяти неоподатковуваних мінімумів доходів громадян.  
7) Здійснення незаконного доступу до інформації яка зберігається, обробляється чи передається в інформаційно-комунікаційних (автоматизованих) системах.  
Накладення штрафу від п'яти до десяти неоподатковуваних мінімумів доходів громадян із конфіскацією засобів, що використовувалися для незаконного доступу, або без такої. Повторно тягне за собою штраф від десяти до двадцяти неоподатковуваних мінімумів доходів громадян з конфіскацією засобів, що використовувалися для незаконного доступу.  
8) За заклики або агітацію за бойкотування референдуму, перешкоджання членам ініціативної групи у збиранні підписів громадян під вимогою про проведення референдуму, а так само будь-яка агітація в день проведення референдуму передбачає накладення штрафу від трьох до шести неоподатковуваних мінімумів доходів громадян.

**3. Засоби цивільно-правової відповідальності за правопорушення в інформаційній галузі.**

Цивільно-правова відповідальність – важливий самостійний вид відповідальності у праві, один з невід’ємних компонентів інституту юридичної відповідальності. В інформаційній сфері, якій властиві синергетичні форми, така відповідальність на приватноправових засадах має забезпечувати захист і відновлення фундаментальних для сучасного суспільства інформаційних прав як майновими, так і спеціальними немайновими засобами.

В Україні перспективи цивільно-правової відповідальності за інформаційні правопорушення зумовлені багатьма різноплановими факторами, зокрема: підвищенням рівня правової та інформаційної культури, еволюцією наукових уявлень щодо правової природи інформаційних явищ, розвитком інформаційного права і законодавства, удосконаленням діяльності судової системи тощо.

Цивільно-правова відповідальність виконує всі функції притаманні інституту юридичної відповідальності, зокрема й карні, проте її пріоритетним завданням є повернення становища потерпілого до того, яким воно було на момент вчинення правопорушення, а у разі неможливості – компенсація потерпілому втрат, спричинених правопорушенням, передусім у майновій формі. Однак усунення порушень інформаційних прав, зумовлених недостовірністю поширеної інформації, які часто призводять до шкоди «позитивному іміджу» особи в суспільстві, поряд з компенсаційними майновими засобами вимагає додаткових механізмів немайнового поновлення особистих немайнових прав в межах відносин цивільно-правової відповідальності. Таким механізмом є спростування недостовірної інформації та заборона поширення інформації, якою порушуються особисті немайнові права (ст. 277, ст. 288 ЦКУ).

**4. Кримінально-правові санкції за порушення інформаційного законодавства.**Кримінальна відповідальність - вид юридичної відповідальності, який застосовується за скоєння злочинів в інформаційній галузі, вичерпний перелік яких встановлений у Кримінальному кодексі України.  
  
У сфері охорони державної таємниці кримінальна відповідальність настає:  
- за розголошення відомостей, що становлять державну таємницю особою, якій ці відомості були довірені або стали відомі у зв'язку з виконанням службових обов'язків, за відсутності ознак державної зради або шпигунства.

Карається позбавленням волі на строк від 2х до 5 років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого. Те саме діяння, якщо воно спричинило тяжкі наслідки, карається позбавленням волі на строк від п'яти до восьми років;  
- за втрату документів або інших матеріальних носіїв секретної інформації, що містять державну таємницю, а також предметів, відомості які становлять державну таємницю.  
Карається позбавленням волі на строк до 3х років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до 3х років або без такого. Те саме діяння, якщо воно спричинило тяжкі наслідки, карається позбавленням волі на строк від двох до п'яти років.  
Правопорушеннями також визнаються:  
- передача або збирання з метою передачі іноземним підприємствам, установам, організаціям або їхнім представникам економічних науково-технічних або інших відомостей, що становлять конфіденційну інформацію, яка є власністю держави, особою, якій ці відомості були довірено або стали відомі у зв'язку з виконанням службових обов'язків, за відсутності ознак державної зради або шпигунства.  
Злочин карається обмеженням волі на строк до трьох років або позбавленням волі на строк від двох до п'яти років із позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого  
- розголошення службовою особою лікувального закладу, допоміжним працівником, який самочинно здобув інформацію, або медичним працівником відомостей про проведення медичного огляду особи на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби, що є небезпечною для життя людини  
Такі дії караються штрафом від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян або громадськими роботами на строк до двохсот сорока годин, або виправними роботами на строк до двох років, або обмеженням волі на строк до трьох років із позбавленням права обіймати посади чи займатися певною діяльністю на строк до трьох років або без такого;

- умисне розголошення лікарської таємниці особою, якій вона стала відома у зв'язку з виконанням професійних чи службових обов'язків, якщо таке діяння спричинило тяжкі наслідки.  
Карається штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян або громадськими роботами на строк до двохсот сорока годин або позбавленням права обіймати посади чи займатися певною діяльністю на строк до трьох років, або виправними роботами на строк до двох років;  
- незаконне знищення матеріальних носіїв інформації, зокрема виборчої документації або документів референдуму поза визначеним законом строком зберігання у державних архівних установах та в Центральній виборчій комісії України після проведення виборів або референдуму, а так само пошкодження виборчої документації або документів референдуму.  
Караються обмеженням волі на строк від трьох до п'яти років або позбавленням волі на строк від двох до чотирьох років.

Кримінальними злочинами є також:  
- порушення гарантованої Конституцією України таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер.  
Карається штрафом від п'ятдесяти до ста неоподатковуваних доходів громадян або виправними роботами на строк до двох років, або обмеженням волі до трьох років. Ті самі дії, вчинені щодо державних чи громадських діячів або вчинені службовою особою, або з використанням спеціальних засобів, призначених для негласного зняття інформації, караються позбавленням волі на строк від трьох до семи років;  
- розголошення таємниці усиновлення (удочеріння) всупереч волі усиновителя (удочерителя)

Карається штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років.

Серед злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж: і мереж: електрозвязку («комп'ютерні злочини»):  
- несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку; створення з метою використання, розповсюдження або збуту шкідливих програмних технічних засобів, а також їх розповсюдження або збут;  
- несанкціоновані дії з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї;  
ИТД. Караються штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на строк до трьох років із позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання та які є власністю винної особи.

**5. Особливості застосування інших видів санкцій за правопорушення в інформаційній галузі.**