Додаток Г

до п.п. 3.6

**(Ф \_\_- \_\_\_)**

**Міністерство освіти і науки України**

**Національний авіаційний університет**

**НАВЧАЛЬНО-НАУКОВИЙ ЮРИДИЧНИЙ ІНСТИТУТ**

**Кафедра КОНСТИТУЦІЙНОГО І АДМІНІСТРАТИВНОГО ПРАВА**

**Конспект лекцій**

з дисципліни

«Забезпечення прав людини і громадянина в інтернет-просторі»

за напрямом (спеціальністю): 081 «Право»

Укладач: Сопілко І.М. д.ю.н., доцент кафедри конституційного і

адміністративного права

Проскура Г.М., асистент кафедри конституційного і

адміністративного права

Конспект лекцій розглянутий та схвалений

на засіданні кафедри конституційного і

адміністративного права

Протокол № \_\_\_\_ від «\_\_\_»\_\_\_\_\_2018р.

Завідувач кафедри Пивовар Ю.І.

Продовження Додатку Г

**Лекція № 1**

Тема лекції: **Інтернет та міжнародна інституційна складова управління Інтернетом.**

**План лекції**

1. Вступ до Інтернету та Міжнародної інституційної складової управління Інтернетом.

2. ІСАNN як глобальне утворення sui generis.

3. Загальна картина управління Інтернетом – система Організації Об’єднаних Націй.

4. Європейський вимір управління Інтернетом.

5. Регіональні організації у зміцненні мережі управління Інтернетом.

6. Рушійна сила управління Інтернетом.

7. Участь мультистейкхолдерів в управлінні Інтернетом.

8. Виклики та тенденції в рамках інституційної архітектури управління Інтернетом.

**Література**

1. Закон України «Про інформацію» від 02.10.1992 року // Відомості Верховної Ради України. – 1992. – № 48. – ст. 650.

2. Закон України «Про поштовий зв'язок» від 04.10.2001 року № 2759-ІІІ – Електронний ресурс. – Режим доступу: <http://zakon3.rada.gov.ua/laws/show/2759-14>

3. Сопілко І.М. Захист авторських прав в мережі інтернет : монографія / І.М.Сопілко, О.В.Пономаренко. – К. : Комп’ютерпрес, 2013. – 247 с.

4. [Кульчій](https://www.coursera.org/learn/r-programming/) О.О. Інформаційне право: навчально-методичний посібник для самостійного вивчення навчальної дисципліни підготовки бакалавра спеціальності 081 «Право» [Електронний ресурс] / О.О. Кульчій. – Полтава: ВНЗ Укоопспілки «ПУЕТ», 2015. – Режим доступу: http://pravo.puet.edu.ua/files/lic2016bac/ip\_03.pdf

**Зміст лекції**

**1. Вступ до Інтернету та Міжнародної інституційної складової управління Інтернетом.**

Інтернет знаходяться в центрі уваги останніх найзначніших подій, дискусій, обговорень, суперечок та дебатів. Протягом певного періоду часу він розглядався у якості недослідженого феномену, але за останні роки звернув на себе велику увагу, особливо у зв’язку із розкриттям секретних документів Агентства національної безпеки СІІІА Едвардом Сноуденом. Більш того, управління Інтернетом стало важливим у багатьох секторах публічного та приватного життя - охороні здоров’я, освіті, публічній адміністрації.

**Екосистема управління** Інтернетом складається із декількох рівнів: уряди, спеціалізовані міжнародні інституції, міжурядові інституції, громадянське суспільство, приватний сектор, Інтернет спільнота, техноспільнота, Інтернет форуми і т.д. Усі вони чинять властивий їм вплив на управління Інтернетом.

**Історія Інтернету скдадаєьтьс з етапів:**

- **Предісторія** (1956-1966);

- **Етап перший:** від військового експерименту до програми цивільного призначення (1967-1995); ARPANET (1967-1972); Розвиток Інтернет-мережі на основі набору протоколів TCP/IP (1973-1983); Перехід від військової/дослідницької мережі до мережі цивільного призначення (1983-1995);

- **Етап другий**: комерціалізація Інтернету (1995 - ідо цього часу);Перший бум в історії Інтернету: 1995-2000; Web 2.0 (2000-2003); Мобільне сполучення, нагляд, кібер злочин, корпоративна влада, зміни цілей використання (2004 - ідо цього часу).

Історія Інтернету сягає, здебільшого, ери після закінчення Другої Світової війни, а його еволюцію можна зобразити у двох основних етапах: розвиток від військового експерименту до програми цивільного призначення та комерціалізація мережі Інтернет.

(а) Предісторія (1956-1966)

Доктрина взаємного гарантованого знищення (MAD) - регулювала ядерну противагу між Сполученими Штатами та Радянським Союзом. Вони викликала негайну потребу розробити систему комунікацій, здатну витримати руйнівну термоядерну атаку. Відреагував на виклик дослідник корпорації RAND, Пол Берен, який вигадав дизайн сітчастої схеми на основі високих рівнів надмірної кількості зв’язків та технології цифрового зв’язку під назвою комутація пакетів. Проте, вона так і не була побудована.

У 1962 році Джозеф Ліклайдер(1915–1990), керівник Агентства передових оборонних дослідницьких проектів США висловив ідею Всесвітньої комп'ютерної мережі.

Перший в світі Інтернет зародився зі створенням дослідної комп'ютерної мережі, яка отримала назву ARPANET. Її основним завданням була комутація пакетів Агентства перспективних дослідницьких проектів Міноборони США.

Після цієї події з метою підвищення ступеня інформаційної безпеки на випадок війни Міністерство оборони Сполучених Штатів в екстреному порядку віддало наказ розробити надійну систему для передачі даних і виділив на це необхідні кошти. Зайнялося питанням створенням комп'ютерної мережі спеціальне агентство DAPRA, яке відповідало за впровадження нових технологій в США. З плином часу APRANET розвивалася і ставала популярною вченими з різних сфер науки.

Спроба встановлення першої зв'язку по мережі була проведена 29 жовтня 1969 року. Чарлі Клайн з Каліфорнійського університету (р. Лос-Анджелес) пробував віддалено підключитися до ПК, що знаходиться на відстані 640 км у Стенфордському дослідницькому інституті, де Білл Дювалль в телефонному режимі підтверджував успішну трансляцію кожного символу. Однак з п'яти знаків слова «LOGON», яке було спеціальною командою авторизації в системі, з першої спроби вдалося передати лише перші три знаки – «LOG», після цього в мережі стався збій. Однак після повернення APRANET в робочий стан через кілька годин наступна спроба вчених встановити зв'язок на відстані увінчалася успіхом.

О**сновні аспекти проекту ARPANET**:

1. Успіху було досягнуто завдяки неабияким колегіальним діям: дизайн центральних протоколів мережі було доручено Робочій групі з мережі, що переважно складалась із студентів. Таким чином було сформовано колегіальний дух - важлива риса технічного розвитку Інтернету навіть на сьогоднішній день.

2. ARPANET передбачає цікаве конкретне дослідження соціального виміру технологій. Планувалось, що мережа стане інструментом обміну ресурсами, проте її користувачі переважно використовували її для спілкування один з одним, шляхом обміну файлами та програмним забезпеченням, а також для відправлення та отримання електронних листів.

3. Концепція нетворкінгу як об’єднання людей.

**Дата 22 жовтня 1969 року може по праву вважатися датою появи першого в світі Інтернету.** Перша програма для обміну електронними листами в Глобальній мережі з'явилася в 1971 році і відразу ж стала популярною серед користувачів Інтернету. У [1](https://uk.wikipedia.org/wiki/1973%22%20%5Co%20%221973)973 році до мережі через трансатлантичний кабель були підключені перші іноземні організації з Великобританії та Норвегії – мережа стала міжнародною.

У 1984 р. почала функціонувати комп'ютерна система розподілу доменних імен, яка дозволяла отримати інформацію про сайту в Мережі.

У 1984 р. з'явилася ще одна масштабна мережу NSFNet, яка була створена Національним науковим фондом Сполучених Штатів. Вона включала в себе безліч дрібних мереж, в тому числі і популярні тоді Bitnet і Usenet, і володіла значно більшою пропускною здатністю в порівнянні з мережею ARPANet. Таким чином, остання набула серйозного конкурента. До NSFNet підключилися понад 10 000 ПК менш ніж за рік, і зі словом «Інтернет» поступово стала асоціюватися саме ця мережа.

[Створення протоколу](http://webbuilding.com.ua/ukr/) IRC – Internet Relay Chat заклало основу першого чату, яке забезпечило спілкування користувачів в реальному часі. Це відбулося в 1988 році.

У 1989 році в Європі, в стінах Європейського центру ядерних досліджень (франц. Conseil Européen pour la Recherche Nucléaire, CERN) народилась концепція тенет. Її запропонував знаменитий британський вчений Тім Бернерс-Лі, він же протягом двох років розробляв протокол HTTP, мову гіпертекстової розмітки HTML та ідентифікатори URI.

Проте головним постачальником даних Глобальна мережа стала лише до 1995 р., коли її трафік перевищив за обсягом пересилається поширений протокол передачі файлів FTP. Це послужило поштовхом для створення **W3C – Консорціуму Всесвітньої павутини.** Саме остання надала вигляд раніше безликому Інтернету.

У 1990 році мережа ARPANET припинила своє існування, програвши конкуренцію NSFNet. Тоді ж було зафіксовано перше підключення до Інтернету телефонною лінією (так зване «дозво́нювання» англ. Dial-up access).

У 1991 році тенета стали доступні в Інтернеті, а в 1993 році з'явився знаменитий Веб-браузер (англ. web-browser) NCSA Mosaic. Всесвітня павутина ставала дедалі популярнішою.

У 1995 році NSFNet повернулась до ролі дослідницької мережі; маршрутизацією всього трафіку Інтернету тепер займались мережеві провайдери (постачальники послуг). В тому ж році тенета стали основним постачальником інформації в Інтернеті, обігнавши за обсягом трафіку протокол передачі файлів FTR; було сформовано Консиліум всесвітньої повутини. Можна сказати, що тенета перетворили Інтернет і створили його сучасний вигляд.

Таким чином, з 1996 р. терміни «Інтернет» і «Всесвітня мережа» практично повністю підміняють один одного.

У 1998 році Папа Римський Іоанн Павло II заснував Міжнародний день Інтернету, який щорічно святкується 4 квітня, в Україні з 2001 року "День Інтернету" відмічається щорічно 14 грудня.

У 2000 р. нараховувалося близько 327 млн користувачів, з них тільки в США чисельність перевищувала 100 млн чоловік.

У 2004 р. Інтернет нараховував 700 млн користувачів, і найближчим часом їхня кількість зросте до 1 млрд. Число сайтів, що становило в 1993 р. 26 тис., сьогодні перевищує 5 млн.

Соціальні мережі он-лайн - Linkedln (2003), Facebook (2004), Twitter (2006). 2007 - поява смартфону- доступ до Інтернету. 5 січня 2011 року кількість інтернет-користувачів у світі сягнула 2 мільярдів.

**Управління Інтернетом** - керування та координація технічними засобами Інтернету - такими як доменні імена, адреси, стандарти та протоколи, що уможливлюють роботу Інтернету.

Визначення, розроблене Проектом з Управління Інтернетом: **Управління Інтернетом** - процес колективного прийняття рішень власниками, операторами, розробниками та користувачами мереж, під’єднаними Інтернет протоколами, для встановлення політики, правил та процедур вирішення спорів стосовно технічних стандартів, надання ресурсів, та / чи поведінки людей, залучених до процесів глобальної взаємодії в мережі.

**Вузьке визначення:** Управління Інтернетом - керування та координація технічними засобами Інтернету - такими як доменні імена, адреси, стандарти та протоколи, що уможливлюють роботу Інтернету.

**Широке визначення:** Управління Інтернетом включає в себе багато факторів, що формують множинність питань, пов’язаних з Інтернетом, зокрема: інтелектуальна власність, приватність, свобода в Інтернеті, електронна торгівля та кібербезпека.

У 2003 році увага спільноти зосередилась на понятті Управління Інтернетом в межах Всевітнього саміту з питань інформаційного суспільства, що проходив в Женеві у 2003 році та в Тунісі у 2005 році.

**Управління Інтернетом повинне**:

– забезпечувати справедливий розподіл ресурсів;

– полегшувати доступ для всіх;

– гарантувати стабільне і захищене функціонування Інтернету;  
– враховувати багатомовність.

Управління Інтернетом охоплює як технічні питання, так і питання державної політики, і в ньому повинні брати участь усі заінтересовані сторони і відповідні міжурядові і міжнародні організації.

МІжнародне управління Інтернетом має бути багатостороннім, прозорим та демократичним, із повним залученням урядів, приватного сектору, громадянського суспільства та міжнародних організацій.

Як наслідок - заснування Робочої групи з Управління Інтернетом (WGIG) - баланс представників уряду, бізнесу, громадянського суспільства та технологічної спільноти, що працювали над розробкою єдиного бачення щодо Управління Інтернетом.

Сьогоднішній день Інтернету — це епоха електронної комерції, електроних бібліотек, віртуального офісу, дистанційного навчання, мультимедіальних цифрових ресурсів.

Якщо початково Інтернет представляв собою засіб поширення інформації, а розробка цілого ряду, що пішла за цим, програм для забезпечення різних видів мережевої взаємодії, операційних систем. На перше місце виходить використання Інтернету в комерційній діяльності підприємств, електронного урядування та дистанційного навчання.

**Електро́нне урядува́ння**— спосіб організації [державної влади](https://uk.wikipedia.org/wiki/%D0%92%D0%BB%D0%B0%D0%B4%D0%B0) за допомогою систем локальних інформаційних мереж та сегментів глобальної інформаційної мережі, що забезпечує функціонування органів влади в режимі реального часу та робить максимально простим і доступним щоденне спілкування з ними [громадян](https://uk.wikipedia.org/wiki/%D0%93%D1%80%D0%BE%D0%BC%D0%B0%D0%B4%D1%8F%D0%BD%D0%B8%D0%BD), [юридичних осіб](https://uk.wikipedia.org/wiki/%D0%AE%D1%80%D0%B8%D0%B4%D0%B8%D1%87%D0%BD%D0%B0_%D0%BE%D1%81%D0%BE%D0%B1%D0%B0), [неурядових організацій](https://uk.wikipedia.org/wiki/%D0%93%D1%80%D0%BE%D0%BC%D0%B0%D0%B4%D1%81%D1%8C%D0%BA%D0%B0_%D0%BE%D1%80%D0%B3%D0%B0%D0%BD%D1%96%D0%B7%D0%B0%D1%86%D1%96%D1%8F).

**2. ІСАNN як глобальне утворення sui generis.**

**Sui generis**(суі генеріс; букв. своєрідний, єдиний у своєму роді) — латинський вираз, що означає унікальність правової конструкції (акту, закону, статусуі т. д.), яка, незважаючи на наявність схожості з іншими подібними конструкціями, в цілому не має прецедентів. Унікальність будь-якого з випадків «sui generis» часто стає предметом затяжних суперечок.

**ICANN** є неурядовою організацією, відповідальною за управління базовою Інтернет інфраструктурою - адресами Інтернет Протоколу (ІП), доменними іменами та кореневими серверами.

Інтернет корпорація з присвоєння імен та номерів (англ. Internet Corporation for Assigned Names and Numbers, або ICANN (абревіатура вимовляється як МФА: [ˈaɪkæn]; цікаво що так само звучить англ. I can — я можу) — міжнародна некомерційна організація, створена восени 1998 за участю уряду США для регулювання питань, пов'язаних з доменними іменами, IP-адресами і іншими аспектами функціонування Інтернету.

З 1994 по 1998 роки була зроблена серія спроб передати адміністрування Інтернетом до рук приватних осіб. Спроби розпочались із Інтернет Суспільства (ISOC) у США. Існує прямий зв’язок між цими ранніми спробами ISOC приватизувати процес адміністрування Інтернету та фінальним підходом саморегулювання, прийнятого адміністрацією Клінтона. ICANN почала своє функціонування у якості об’єднання невеликої групи технологів на базі ISOC з метою збереження контролю над їх інтересом, коли розпочалась еволюція інституції в напрямку до комерційного утворення.

ICANN зареєстрована у Каліфорнії ЗО вересня 1998 року; голова Естер Дісон, Джон Постел - засновник.

ІСАNN складається із багатьох груп, кожна з яких представляє різні сфери Інтернету. Сюди входять три допоміжні організації: організації, що працюють з ІР-адресами, організації, що працюють з доменними іменами, менеджери доменів вищого рівня держави. Також є чотири консультативні комітети, що забезпечують ІСАІМІМ консультаціями та рекомендаціями. Вони представляють, уряди і міжнародні організації; операторів кореневих серверів; організації, що вирішують питання безпеки Інтернету; співтовариство в цілому. Діє також Технічна група співробітників зі зв’язків, що працює з організаціями, що розробляють основні протоколи для Інтернет-технологій.

3. **Загальна картина управління Інтернетом** - **система Організації Об’єднаних Націй.**

**Управління Інтернетом**— це комплекс заходів з розробки й застосування урядами, приватним сектором, громадянським суспільством та технічною спільнотою, у відповідних ролях, загальних принципів, норм, правил, процедур прийняття рішень і програм, які формують умови для розвитку і використання [Інтернету](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%22%20%5Co%22%20%5Ct%20%22_blank). Він включає такі питання, як історія регулювання Інтернету, протиріччя, які виникали на процесі розвитку Інтернету, а також триваючих дебатів про те, як повинен або не повинен регулюватися Інтернет в майбутньому.

**Функції ГА ООН вуправлінні Інтернетом:**

1. Перегляд результатів роботи Робочої групи зі зміцнення співробітництва Комісії ООН з науки і техніки з метою розвитку.

ГА Резолюцією 60/252, уповноважив ГА здійснити загальний перегляд процесу імплементації результатів ВСЮ у 2015 році. У відповідь ГА Резолюцією 68/302 вирішила, що загальний перегляд буде проведено шляхом дводенного засідання ГА на високому рівні та міжурядовим процесом, що також враховує результати роботи відповідних стейкхолдерів. Засідання ГА на високому рівні надають можливість для глибоких обговорень важливих питань щодо імплементації результатів, включно з прогресом, прогалинами та викликами, а також планами майбутньої діяльності.

Управління Інтернетом обговорюється у якості складової роботи різних комітетів ГА:

- Перший Комітет - Комітет із роззброєння та міжнародної безпеки - займається питаннями роззброєння, глобальних викликів та загроз миру, що впливають на міжнародну спільноту та шукає вирішення викликам режиму міжнародної безпеки.

Поточні теми Комітету зі сфери управління Інтернетом:

(a) Кібервійна

(b) Майбутнє кібербезпеки (**Кібербезпека** - новаційне питання в сфері міжнародної безпеки).

**Рада ООН з прав людини**

До 2011 року небагато уваги приділялось питанням Інтернету в рамках роботи Управління Верховного комісара ООН з прав людини, але з того часу ситуація змінилась. Спеціальний доповідач ООН зі свободи вираження Френк Ла Рю підготував детальний звіт щодо свободи вираження в Інтернеті.

В лютому 2011 року Рада ООН з прав людини організувала зустріч експертів за принципом мультистейкхолдеризму щодо Інтернету та прав людини.

В липні 2011 року Рада ООН з прав людини прийняла резолюцію про свободу вираження в Інтернеті - вона підтверджує, що ті права, які людини має он-лайн, мають захищатися і оффлайн. Подібна резолюція була прийнята також у 2014 році.

27 червня 2016 року Рада ООН з прав людини прийняла резолюцію щодо сприяння, захисту та використання прав людини в Інтернеті.

Комісія ООН з науки і техніки з метою розвитку є допоміжним органом ЕКОСОР. Вона була заснована у 1992 році у результаті реструктуризації та ревіталізації ООН у економічній, соціальній та пов’язаній сферах.

Комісія провела перше засідання в квітні 1993 року у Нью-Йорку, США. З липня 1993 року секретаріат ЮНКТАДу несе відповідальність за матеріальну підтримку Комісії. Потім Комісія провела засідання в Женеві, Швейцарія.

Основна ціль: Комісія була заснована з метою надання Генеральній Асамблеї та ЕКОСОР консультацій на вищому рівні з відповідних питань через аналіз та відповідні рекомендації для уможливлення даних органів керувати майбутнім ООН, розробляти спільну політику та узгоджувати відповідні дії.

**Міжнародний союз електрозв’язку**

Робоча група Ради з питань міжнародної публічної політики в сфері Інтернету - утворена як окрема група Резолюцією 1336 Ради MCE, у відповідності з Резолюціями 102 і 140 Конференції уповноважених представників 2010.

Членство в Робочій групі обмежується членами MCE, з відкритою консультацією усім стейкхолдерам. Попередньо ця група була заснована у якості Особливої групи - невід’ємної частини Робочої групи ВСЮ, відкритої лише для усіх держав членів.

Сфери діяльності:

1. Розповсюдження її результатів серед членів MCE та усіх належних організацій та стейкхолдерів, що беруть активну участь у питаннях, важливих для формування політики в сфері Інтернету;

2. Розгляд та обговорення діяльності Генерального секретаря та директорів Бюро щодо імплементації Резолюції 102 та допомоги в такій діяльності;

3. Ініціювання та проведення відкритих та змістовних консультацій з усіма стейкхолдерами.

**4. Європейський вимір управління Інтернетом.**

Рада Європи бере активну участь в усіх обговореннях та діалогах із стейкхолдерами задля забезпечення того, що права та свободи, гарантовані Конвенцією про захист прав людини та основоположних свобод, знаходяться в центрі розвитку Інтернету.

Рекомендація Комітету міністрів державам-членам щодо Керівництва з прав людини для користувачів мережі Інтернет (Схвалена Комітетом міністрів від 16 квітня 2014 року на 1197 засіданні заступників міністрів).

**Стратегія Управління Інтернетом 2016-2019**

Її мета у забезпеченні того, що публічна політика з управління Інтернетом зосереджується навколо людини з метою: Побудови демократії он-лайн; Захисту користувачів мережі Інтернет; Забезпечення поваги та захисту прав людини он-лайн.

**Пан-європейський діалог з управління Інтернетом**(англ. The Pan-European dialogue on Internet governance (EuroDIG)) — регіональний форум керування [Інтернетом](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%22%20%5Ct%20%22_blank), на якому обговорюється питання публічної політики, пов'язаної з ключовими елементами управління Інтернетом.

Метою заходу є пошук спільного розуміння щодо розвитку Інтернету в Європі, захисту прав людини в кібер-просторі та досягнення інтересів бізнесу та користувачів.

В 2016 EuroDIG проходить 9-10 червня 2016 у місті Брюссель, Бельгія.

**5. Регіональні організації у зміцненні мережі управління Інтернетом.**

**Африканський союз у зміцненні управління Інтернетом**

Питання управління Інтернетом в Африці активно піднімалось під час регіональних зустрічей, що проводились із 2002 по 2005 роки у Бамако, Аккрі, Аддис-Абебі, Каїрі, Йоганнесбурзі, Дуалі та Тунісі.

На даний момент вАфриці діє чотири регіональні ініціативи:

- Західноафриканський форум з управління Інтернетом;

Східноафриканський форум з управління Інтернетом;

- Центральноафриканський форум з управління Інтернетом;

- Південноафриканський форум з управління Інтернетом.

Незважаючи на їх ефективність, ці регіональні ініціативи охоплюють не всі держави у відповідних регіонах.

Відтак, є разюча потребазаснувати Африканський Форум з Управління Інтернетом , що підтримуватиме та консолідуватиме діючі регіональні ініціативи.

**Азіатсько-Тихоокеанське економічне співробітництво** (АРЕС) є регіональним економічним форумом, що об’єднує 21 країну з метою підтримки сталого економічного росту та благоустрою у Азіатсько-Тихоокеанському регіоні.

Ключові сфери співробітництва:

1. Права жінок он-лайн

2. Телекомунікації та інфраструктура

3. Доступ

4. Цифровий розрив

5. Електронна торгівля

6. Приватність та захист даних

Робоча група APEC з телекомунікацій та інформації (TEL) прагне просувати розвиток інфраструктури інформації та комунікаційних технологій, сприяти кооперації, обміну інформацією та розвитку ефективної політики інформаційних та комунікаційних технологій в межах Азіатсько-Тихоокеанського регіону. Також прагне зміцнити соціально-економічний розвиток через ефективне використання інформаційних та комунікаційних технологій, а також забезпечення безпечного та вартого довіри інформаційного та комунікаційного середовища.

TEL намагається гарантувати, щоб усі народи Азіатсько-Тихоокеанського регіону мали наявний доступ до інформаційних та комунікаційних технологій таІнтернету. У

Азіатсько-Тихоокеанська Телекомунікаційна спільнота (APT) була заснована як спільна ініціатива Економічної та Соціальної Ради 00Н для Азії та Тихоокеанського регіону (UNESCAP) та Міжнародного союзу електрозв’язку (MCE).

Міжамериканське співтовариство з питань телекомунікацій (ОАД) Міжамериканське співтовариство з питань телекомунікацій (СІТЕІ.) є утворенням Організації Американських Держав. Було засноване у якості Міжамериканської комісії електрозв’язку на П’ятій Міжнародній Американській Конференції у травні 1923 року. Має технічну автономію для виконання функцій в межах, визначених Хартією ОАД, його підзаконних актів та повноважень Генеральної Асамблеї.

Його мета у координації телекомунікацій, що відносяться до повноважень Генеральної Асамблеї ОАД та тих, що діють під час Самітів Американських Держав; сприянні та просуванні тривалого розвитку телекомунікацій у західній півкулі.

Інтернет Суспільство та СІТЕІ. підписали Меморандум про взаєморозуміння у вересні 2008 року.

Regional Internet Registry, RIR — організація, яка займається питаннями адресації та маршрутизіції в інтернеті.

RIR займаються технічною стороною функціонування Internet: виділенням IP-адрес, номерів автономних систем, реєстрацією реверсних зон DNS та іншими технічними проектами. Часто RIR займаються статистичним аналізом мереж, моніторингом точок обміну трафіком і підтримкою кореневих зон DNS.

**6. Рушійна сила управління Інтернетом.**

З того часу, як постачальники послуг Інтернету стали ключовими он-лайн посередниками, це зробило їх особливо важливими для управління Інтернетом. їх основна залученість відбувається на національному рівні у співробітництві з урядом та юридичними відомствами. На глобальному рівні деякі постачальники послуг Інтернету, зокрема з США та Європи, брали активну участь індивідуально у процесах через національні та регіональні чи секторально визначені бізнес організації такі, як Асоціація інформаційних технологій Америки (ІТАА) та інші.

Google, Facebook та Twitter особливо активні в управлінні Інтернетом. На їх бізнес моделі можуть прямо впливати, наприклад, урядові домовленості, що стосуються захисту даних та приватності. Розробники контенту, зокрема Дісней, також є важливими гравцями, які турбуються про збереження глобального впливу та переваги їх продуктів та моделей для місцевого розвитку контенту, а також захисту їх авторських прав. Бізнес пріоритети таких компаній тісно пов’язані із багатьма питаннями зі сфери управління Інтернетом, наприклад: інтелектуальна власність, приватність, кібербезпека, нейтральність. їх присутність помітна у глобальних процесах управління Інтернетом, включно і через фінансування ними форумів за участі мультистейкхолдерів.

Електронні комунікаційні мережі стали базовим інструментом для вільного обміну думками та інформацією, а користувачі покладаються на Інтернет, як важливий інструмент їхньої повсякденної діяльності (зв'язок, інформація, знання, комерційні перекази) і це призводить до цілком логічного очікування, що Інтернет послуги мають бути загальнодоступними та недорогими, безпечними, надійними та постійними.

**Мережевий нейтралітет** - це принцип, згідно з яким до всього Інтернет трафіку повинно забезпечуватись однакове ставлення, без дискримінації, обмежень або втручань незалежно від його відправника, отримувача, типу або контенту, з тим щоб свобода вибору користувачів Інтернет не обмежувалась за принципом наявності або відсутності сприяння передачі Інтернет трафіку в залежності від відповідного контенту, послуг, програм або пристроїв.

Принцип мережевого нейтралітету має застосовуватись незалежно від інфраструктури або мережі, яка використовується для підключення до Інтернет та доступу до всіх послуг Інтернет та транзитних послуг Інтернет, які пропонуються інтернет-провайдерами, незалежно від технології, яка використовується для передачі сигналу.

Метою даного принципу є уникнення негативного впливу (з боку непрозорого регулювання трафіку, а також дискримінації контенту та послуг або ускладнення доступу з відповідних пристроїв) на право користувачів щодо доступу до та розповсюдження на свій розсуд контенту в Інтернеті, а також програм і послуг, на безоплатній або платній основі, з можливістю використання відповідних пристроїв та створення нових інструментів та послуг.

Громадянське суспільство є найбільш діючим та активним прихильником підходу мультистийкхолдеризму до управління Інтернетом. Участь громадянського суспільства у попередніх багатосторонніх форумах критикувалась через відсутність належної координації та наявність занадто великої кількості, досить часто суперечливих, думок.

**7. Участь мультистейкхолдерів в управлінні Інтернетом.**

Термін мультистейкхолдер з’явився у 1990-х роках та відразу у політичному контексті Всесвітніх самітів ООН та у економічному сенсі теорії менеджменту. Відповідаючи на зростаючі соціальні побоювання стосовно проблем довкілля, Конференція ООН з навколишнього середовища та розвитку розпочала створення нових форм співпраці між урядовими та неурядовими групами, та таким чином асоціювалась зі змінами в участі глобального управління.

З академічної точки зору термінологія мультистейкхолдеризму виникла як частина розчленування теорії стейкхолдеризму. Стейкхолдери, за визначенням Фрімена, є будь-якою групою чи індивідом, що можуть впливати чи на яких здійснюється вплив процесом досягнення цілей організації.

Через невеликий період часу концепція мультистейкхолдеризму почала частіше з’являтися в академічній літературі, де вона отримала додаткові значення.

Наприклад, дослідження з глобального управління прийняли термін та використовували його для позначення нових форм пост-суверенного глобального управління та демократії участі. Відповідно до цієї думки, мережа мультистейкхолдерів заповнює регуляторні прогалини формування глобальної політики та реагує на зростаючу кількість міжнародних проблем, з якими міжурядова дипломатія не може впоратися самотужки.

Термін мультистейкхолдер ввійшов в сферу управління Інтернетом у 2005 році, наприкінці Всесвітнього саміту ООН з питань інформаційного суспільства (ВСЮ). Концепція мультистейкхолдеризму швидко розповсюдилась та почала впливати на дискусії між організаціями з управління Інтернетом. На сьогодні, підхід мультистейкхолдеризму відображає широкий ряд організаційних моделей та процесів.

Є чотири основні класи. Держави, офіційні міжурядові організації та фірми є

відносно прямими. Четвертий клас акторів включає неурядові організації, групи громадянського супісльства чи рухи та індивідів, що діють від їх імені.

Домовленості щодо управління можуть також відрізнятися залежно владних відносин між акторами.

Виділяють чотири варіанти: гомогенна поліархія,гетерогенна поліархія та анархія.

Ієрархія передбачає відносини супер або субординації, де один уповноважений управляти, а інші зобов’язані підпорядковуватись. Поліархія передбачає такі відносини, де влада розподіляється між різними акторами (Інженерна рада Інтернету).

У гетерогенній схемі відокремлені актори (чи класи акторів) володіють різними офіційними повноваженнями, але кожен здійснює владу лише над окремим аспектом управління (наприклад, розподіл влади між різними гілками уряду. Останній варіант - анархія - ситуація, за якої не існує ніяких владних відносин.

Коаліція була заснована у 2011 році на першій конференції інституції у Гаазі, Нідерланди, за ініціативою міністра закордонних справ Нідерландів.

**8. Виклики та тенденції в рамках інституційної архітектури управління Інтернетом.**

Публічна політика формує глобалізацію, а глобалізація, в свою чергу, визначає загалом управління та управління Інтернетом, зокрема.

**Управління Інтернетом є власне публічною політикою.**

Практично усі питання політики, що визначають управління Інтернетом, є публічними, а саме: регулювання контенту та культура; захист даних, приватність та нагляд; захист інтелектуальної власності та справедливе використання; політика конкуренції; безпека та стійкість публічної інфраструктури.

Традиційні інструменти міжнародної політико-правової системи, такі як: конвенції, угоди, хартії та міжурядові угоди, безумовно, відіграють важливу роль в управлінні Інтернетом, як арена для політичних експериментів та поле для досліджень. Проте, ‘власне політичними’ якостями розвитку алгоритму пошуку, видалення відео контенту, блокування доменних імен - це ті дії, що походять та знаходяться під контролем приватного сектору Інтернет інфраструктури - не варто нехтувати у нашій оцінці стану управління Інтернетом

Приватні актори на даний момент відіграють надзвичайно важливу роль у регулюванні контенту, а також форм вираження в Інтернеті, із акцентом на правах в Інтернеті та економічній свободі.

**Приватизація управління Інтернетом -** приватні компанії (наприклад, Google) делегуються урядами у якості регуляторів контенту та де факто основних акторів в управлінні Інтернетом.

Приватний аспект управління Інтернетом часто проявляється на рівні керування інфраструктурою - питанні, доступ публіки до якого є обмеженим. З інших питань роль приватного сектору в упорядкуванні потоку інформації в Інтернеті є більш видимою та чіткою. Наприклад, дії із видалення контенту, запит на що надсилається урядами та міжурядовими організаціями, вчиняються приватними компаніями.

**Лекція № 2**

Тема лекції: Права людини в онлайн-середовищі

**План лекції**

1. Загальний огляд.

2. Доступ та недискримінація.

3. Стаття 10 Європейської Конвенції про захист прав людини і основоположних свобод.

4. Стаття 11 цієї ж Конвенції – зібрання, об’єднання та участь онлайн. Приватність і захист даних.

**Література**

* + 1. Закон України «Про інформацію» від 02.10.1992 року // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.
    2. Марущак А.І. Інформаційне право України. Підручник / Марущак А.І. – К.: Дакор, 2011. – 456 с.
    3. Сопілко І. М. Державна інформаційна політика України: стан та шляхи реалізації: монографія / І. М. Сопілко. – К. : МП «Леся», 2014. – 424 с.
    4. B.C.Цимбалюк Основи інформаційного права України / B.C.Цимбалюк, В.Д.Гавловський, В.В.Гриценко та ін. – К.: Видавництво "Знання", 2004
    5. Пазюк А.В. Правові засоби захисту та відновлення прав користувачів Інтернету в Україні в контексті застосування Посібника Ради Європи з прав людини для інтернет-користувачів [Електронний ресурс] / А.В. Пазюка. – К. : ФОП Клименко, 2015. – 128 с. – Режим доступу: <https://rm.coe.int/1680599465>
    6. 3.3.3. Посібник з прав людини для інтернет-користувачів та пояснювальний меморандум [Електронний ресурс]. - Режим доступу: https://rm.coe.int/16802e3e96

**Зміст лекції**

**1. Загальний огляд.**

7 лютого 2017 року Україна відзначала День безпечного Інтернету. День безпечного Інтернету відзначається на другий день другого тижня другого місяця щорічно. Тисячі людей в усьому світі об’єднуються заради підвищення освіченості з питань безпеки онлайн та участі в заходах і активності в усьому світі.

 День безпечного Інтернету (SID) організовано мережами Insafe та INHOPE за підтримки Європейської комісії для просування безпеки та позитивного використання цифрових технологій, особливо дітьми та молоддю. Ідея онлайн-безпеки еволюціонувала останні роки, змінюючи фокус від створення «безпечного» Інтернету до створення «кращого» Інтернету.

Станом на 2016 рік в Україні користувачами Інтернету були 44,1% населення. Значна частка користувачів — діти й молодь.

У звичному для суспільства значенні «права людини» зазнали й продовжують зазнавати впливу Інтернету як віртуального середовища, у якому можуть реалізуватися та порушуватися права і свободи людини.

Задля просування ідеї прав людини в Інтернеті міжнародними організаціями розробляються та впроваджуються рекомендації, конвенції, керівництва тощо. Питання прав людини в Інтернеті розглядаються в документах ООН, ЮНІСЕФ, Ради Європи, Європейської комісії та інших міжнародних організацій.

На ХХІ сесії ООН у 2012 році спеціальний доповідач з питань про заохочення і захист права на свободу думок та їх вільне вираження Франк Ла Рю зазначив, що немає необхідності вводити нові правозахисні стандарти для Інтернету, оскільки принципи і доктрини в галузі прав людини застосовуються як в режимі офлайн, так і в режимі онлайн. Значну увагу просуванню ідей реалізації, поваги та захисту прав й основних свобод людини в Інтернеті приділяє Рада Європи, членом якої Україна є з 1995 року.

У 2014 році Комітет міністрів Ради Європи приймає Рекомендацію CM / Rec (2014) 6 та зазначає, що держави-члени зобов’язані забезпечити для всіх права людини та основні свободи, закріплені в Європейській конвенції про захист прав людини. Це зобов’язання також діє в контексті використання Інтернету. У Рекомендації зазначено, що права людини та основні свободи належать як до офлайн, так і до онлайн. Незаконним є порушення прав людини та основних свобод під час роботи в Інтернеті.

На своїй ХХХІІ сесії 27 червня 2016 року Рада ООН з прав людини ухвалила резолюцію «Заохочення, захист іздійснення прав людини в Інтернеті», у якій підтверджує, «що ті ж самі права, які людина має в офлайн-середовищі, повинні також захищатися в онлайн-середовищі».

**Перше покоління прав людини** включає в себе громадянські і політичні права, включені до Міжнародного пакту про громадянські і політичні права (МПГПП). Вони вважаються негативними тобто, вони вимагають від держави дозволяти певні індивідуальні свободи замість того, щоб надавати додаткові ресурси або послуги, їхнє застосування не вимагає від держави додаткових витрат, оскільки вони не потребують жодних вкладень. Вони можуть бути запроваджені без жодних передумов, тому їхня дія є миттєвою.

**Друге покоління прав людини.** Через особливості, зазначені вище, міжнародна спільнота вирішила розмежувати перелік прав людини з метою відокремлення другої групи/покоління прав людини, що охоплюються різними міжнародними угодами стосовно економічних, соціальних та культурних прав - Міжнародний пакт про економічні, соціальні і культурні права (МПЕСКП). На відміну від першої категорії, друге покоління прав людини охоплює ті права, які вважаються позитивними через те, що вони вимагають додаткових заходів з боку держав для реалізації їхньої мети.

**Третє покоління прав** людини охоплює ті права, які радше стосуються груп осіб, а не самих осіб, через що ці права вважаються колективними. До цієї групи входять права, що стосуються навколишнього середовища, зокрема право на здорове та адекватне навколишнє середовище; сексуальні права (лесбіянок, геїв, бісексуалів, трансгендерів (ЛГБТ), широко обговорюване право на аборт, що розцінюється як нехтування правом на життя або ж як розвинуте право на здоров'я та медичну допомогу. До цієї категорії також входить право на воду, яке вважається однією з умов права на життя (особи не можуть реалізувати власне право на життя без доступу до питної води), а не як утисканням права на власність, якщо розцінювати воду виключно як комерційний товар.

Тому третя група прав походить з інших прав людини, наприклад, права на життя, права на здоров'я або право на право на повагу до приватного і сімейного життя. Крім

того, сюди відносять право на комунікацію, яке ґрунтується на загальновизнаному праві свободи вираження поглядів.

**Четверте покоління прав людини.** Дискусія щодо поколінь прав людини почалася у 70-х роках 20-го сторіччя. На той час науковці-правники посилалися на три покоління прав людини. Маючи це на увазі, можна стверджувати, що до прав, які походять з одного або декількох прав людини з груп, які існують на даний момент, належать: право на доступ до Інтернету як похідне від права на доступ до інформації, право «бути забутим» як похідне від права на доступ до інформації.

**Право на доступ до Інтернету**(також відоме як право на широкосмуговий зв'язок) - передбачає, що всі люди повинні мати можливість доступу до мережі [Інтернет](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82) з метою здійснення і користування своїми [правами на свободу висловлення думки, переконань](https://uk.wikipedia.org/wiki/%D0%A1%D0%B2%D0%BE%D0%B1%D0%BE%D0%B4%D0%B0_%D1%81%D0%BB%D0%BE%D0%B2%D0%B0) та інших основних [прав людини](https://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%B0%D0%B2%D0%B0_%D0%BB%D1%8E%D0%B4%D0%B8%D0%BD%D0%B8). [Держава](https://uk.wikipedia.org/wiki/%D0%94%D0%B5%D1%80%D0%B6%D0%B0%D0%B2%D0%B0) повинна нести відповідальність за те, щоб доступ до [Інтернету](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82) був широко доступним. [Держави](https://uk.wikipedia.org/wiki/%D0%94%D0%B5%D1%80%D0%B6%D0%B0%D0%B2%D0%B0) не можуть необґрунтовано обмежувати доступ індивідів до Інтернету. Доступ до Інтернету визнається як право відповідно до законодавства ряду країн.

У грудні 2003 року під егідою [Організації Об'єднаних Націй](https://uk.wikipedia.org/wiki/%D0%9E%D1%80%D0%B3%D0%B0%D0%BD%D1%96%D0%B7%D0%B0%D1%86%D1%96%D1%8F_%D0%9E%D0%B1%27%D1%94%D0%B4%D0%BD%D0%B0%D0%BD%D0%B8%D1%85_%D0%9D%D0%B0%D1%86%D1%96%D0%B9) був скликаний Всесвітній саміт з питань інформаційного суспільства (ВСІС). Після тривалих переговорів між урядами, представниками громадянського суспільства та бізнесу була прийнята Декларація принципів ВСІС, що таким чином підтвердила важливість [інформаційного суспільства](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%B5_%D1%81%D1%83%D1%81%D0%BF%D1%96%D0%BB%D1%8C%D1%81%D1%82%D0%B2%D0%BE) для підтримки і зміцнення [прав людини](https://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%B0%D0%B2%D0%B0_%D0%BB%D1%8E%D0%B4%D0%B8%D0%BD%D0%B8).

5 січня 2012 року Європейська Комісія запропонувала комплексну реформу правил захисту даних у Європейському Союзі, які діють з 1995 року. Незважаючи на те, що основні принципи Директиви 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24.10.1995 р. (Далі – Директиви 95/46/ЄС) залишаються чинними, вона більше не здатна вирішувати проблеми швидкого технічного розвитку та глобалізації, і в результаті цього потребує перегляду. Одна з таких проблем **– це «право бути забутим»,** чи як його ще називають «право на забуття», яке вже включено до Директиви 95/46/ЄС, що гарантує особам право вимагати від контролера видалення незаконно оброблених персональних даних. Проте через те, що за даними Європейської Комісії, для особи важко забезпечити це право в онлайн-середовищі, були запропоновані деякі зміни до чинної законодавчої бази.

У 2014 р. Суд Європейського Союзу виніс рішення, яким право бути забутим було затверджене. Це викликало неабиякі зміни у юридичній практиці держав-членів ЄС та дискусії щодо відповідного права по всьому світу.

Відправною точкою справи було звернення іспанського громадянина Маріо Костехи Гонсалеса, який поскаржився на оголошення у газеті (електронна версія видання містилася на сайті), що були опубліковані в 1998 році, але все ще були доступні в Інтернеті. Вони стосувалися банкрутства та аукціону нерухомості, щодо продажу його будинку за борги. Пошуки Google за його іменем приводили до посилань на ці сторінки. Маріо Костехи хотів, щоб їх було видалено, оскільки його борги давно були погашені, і ця інформація була неактуальною і не відображала той стан справ, яким він є сьогодні, що шкодило його репутації. Європейський суд постановив, що з метою забезпечення прав, передбачених у згаданих положеннях Директиви, «оператор пошукової системи зобов’язаний видалити зі списку результатів, виданих у відповідь на пошуковий запит на основі імені особи, посилання на веб-сторінки, розміщені третіми особами, що містять інформацію про цю особу, також і у випадку, коли ім’я або інформація не видалена перед тим або у той самий час з самих веб-сторінок, і навіть тоді, коли публікація на цих сторінках розміщена на законних підставах».

Сама інформація щодо особистого банкрутства Маріо Костехи Гонсалеса залишається доступною на сайті газети La Vanguardia, але більше не індексується пошуковим механізмом Google.15 грудня 2015 р. була досягнута Угода між Радою, Парламентом та Комісією щодо законодавчого пакету, запропонованого Комісією в 2012 році для оновлення та модернізації правил захисту даних. Цей пакет складався з двох законодавчих інструментів: загальних правил захисту даних (призначених для заміни Директиви 95/46/ЄС 1995 року) та Директиви захисту даних у галузі правоохоронної діяльності (призначена замінити Рішення Ради в межах захисту персональних даних, що обробляються в рамках поліцейської та судової співпраці у кримінальних справах 2008/977/JHA 2008 року. Очікується, що ці правові акти наберуть чинності навесні 2018 року.

Вищезгадані зміни до законодавства ЄС є величезним кроком на шляху до захисту даних у Європі, який деякі автори розглядають як «коперніканський переворот». Запропоновані правила посилять права фізичних осіб та підвищать відповідальність контролерів за обробку персональних даних. Проте, право на забуття не є абсолютним, його завжди потрібно буде збалансовувати з іншими основними правами, такими як свобода вираження поглядів та засобів масової інформації. Положення про «Право на стирання (право бути забутим)», ймовірно, стане одним із найбільш суперечливих положень запропонованого Регламенту 2016/679 про захист персональних даних.

**Право на віртуальну особистість** як похідне від прав на інтелектуальну власність

Досліджувати проблему «віртуальної особистості» сьогодні є надзвичайно актуально. В наш час збільшуються можливості людини для використання комп’ютерних віртуальних технологій, з’являються технічні можливості поєднання їх з мережею Інтернет. З таким стрімким розвитком віртуальні технології все більше проникатимуть в різні сфери діяльності людини. Все це досить суттєво вплине на економічні, політичні, культурні відносини людства. Але всі ці зміни необхідно будувати на високих моральних принципах, направляти не на загибель душі і тіла людини, а на її розвиток.

Світ, що зараз формується, світ «віртуального» – це світ діалогічний, світ, головним засобом творення якого є комунікація. Саме тому «людям завжди цікаво слухати щось нове, а якщо це нове стосується наших друзів, знайомих – ми матимемо шалений трафік». Прикладом цього є Facebook – «бомба нашого часу» (Social Network).   
При написанні роботи ми зробимо спробу «зрозуміти віртуальну особистість» через її порівняння з особистістю реальною. Тому головним для нас методом буде метод порівняння, який буде використаний для того, щоб ми змогли побачити різницю між віртуальною та реальною особистостями. Також у даній роботі ми використовуватимо метод моделювання, який допоможе нам уявити «віртуальну особистість» як щось ціле, але не фіксоване. До проблеми осмислення віртуальної особистості зверталися: С. Жижек, Ж. Делез, Д. Іванов, М. Опенков та інші. У своїх роботах вони показали, що значить, на їх думку, «реальність віртуального», хто така віртуальна особистість і як вона пов’язана з кіберпростором. У своєму дослідженні спробуємо створити та проаналізувати цілісний образ «віртуальної особистості», базуючись на вже існуючих концепціях. Результатом цього дослідження виступає також розуміння як індивід буде поводити себе у майбутньому, як зміниться особистість під впливом інформації.

**2. Доступ та недискримінація.**

**Доступ до Інтернету** – це важливий засіб для реалізації вами своїх прав та свобод, а також для участі в демократичних процесах. Саме тому позбавити вас доступу до Інтернету проти вашої волі можуть лише за рішенням суду. В окремих випадках надання послуг може також припинятися за умовами договору, але це має відбуватися лише після того, як були вичерпані всі інші засоби.

Доступ має надаватися за розумну ціну і бути недискримінаційним**.**

**Принцип недискримінації** означає заборону необґрунтованого відмінного ставлення (а саме встановлення розрізнень, винятків, обмежень чи переваг) до осіб, які знаходяться в однаковій ситуації чи однакового підходу до осіб, які знаходяться в різних ситуаціях.

**Дискримінація** – це позбавлення, виключення, обмеження певного права людини окремої людини або групи через наявність у них певних ознак. І при цьому перевага у реалізації права віддається іншій людині або групі, у яких таких ознак немає.

Дискримінація має місце, коли до людей ставляться менш прихильно, ніж до інших людей в такій же самій ситуації тільки тому, що вони належать до певної групи чи категорії людей. Їх можуть позбавляти права (дискримінувати) через їхній вік, інвалідність, етнічну приналежність, політичні переконання, расу, релігію, стать чи гендер, сексуальну орієнтацію, мову, культуру та з багатьох інших причин.

Дискримінація забороняється за ознакою статі, раси, кольору шкіри та ін., оскільки всі люди народжуються вільними і рівними у своїй гідності та правах.

**Веб Доступність**(Web Accesability), стосується найкращих практик що застосовуються, аби дозволити вебсайту залишатись доступним не зважаючи на фізичні або технічні обмеження.

 Веб-доступність — це термін, що означає створення такого веб-сайту, який був би доступний для максимально можливої кількості людей, включаючи користувачів з обмеженими можливостями. Для вирішення проблем веб-доступності (графіки без супровідних даних, немарковані поля, посилання без тексту, зображення без альтернативного тексту, відео без підписів та багато іншого). Щоб виявити технічні проблеми, помилки сервера або навіть віруси, ви можете замовити моніторинг доступності веб-сайту. Крім того, існує безліч програм, які дозволяють вам перевірити рівень доступності вашого контенту.

**3. Стаття 10 Європейської Конвенції про захист прав людини і основоположних свобод.**

Свобода вираження поглядів та свобода преси в контексті ст. 10 Європейської Конвенції про захист прав людини і основоположних свобод

1. Кожен має право на свободу вираження поглядів. Це право включає свободу дотримуватися своїх поглядів, одержувати і передавати інформацію та ідеї без втручання органів державної влади і незалежно від кордонів. Ця стаття не перешкоджає державам вимагати ліцензування діяльності радіомовних, телевізійних або кінематографічних підприємств.

2. Здійснення цих свобод, оскільки воно пов'язане з обов'язками і відповідальністю, може підлягати таким формальностям, умовам, обмеженням або санкціям, що встановлені законом і є необхідними в демократичному суспільстві в інтересах національної безпеки, територіальної цілісності або громадської безпеки, для запобігання заворушенням чи злочинам, для охорони здоров'я чи моралі, для захисту репутації чи прав інших осіб, для запобігання розголошенню конфіденційної інформації або для підтримання авторитету і безсторонності суду.

У контексті прав людини, згаданих у Європейській Конвенції, свобода вираження поглядів важлива не лише сама по собі, а як чинник, що відіграє вирішальну роль у захисті інших прав, гарантованих Конвенцією. Без широких гарантій права на свободу вираження поглядів, на варті яких стоять незалежні й неупереджені суди, не може бути ні вільної країни, ні демократії. Ця основна теза є непорушною.

Свобода вираження поглядів є самодостатнім правом і водночас складовою частиною інших прав, гарантованих Конвенцією, — такого, наприклад, як свобода зібрань. Разом з тим свобода вираження поглядів може входити у конфлікт з іншими передбаченими Конвенцією правами — наприклад, правом на справедливий судовий розгляд, правом на повагу до приватного життя, на свободу совісті і віросповідання. У разі виникнення такої колізії Європейський суд зважує ці права з метою встановити пріоритет одного над іншим. Урівноваження суперечливих інтересів, одним з яких є свобода вираження поглядів, бере до уваги важливість останньої. Суд неодноразово заявляв, що «свобода вираження поглядів є одним із засадничих положень демократичного суспільства, однією з основних умов його розвитку і самореалізації кожної окремої особи”. Або що «преса відіграє визначальну роль у державі, яка керується принципом верховенства права».

Для демократичних політичних процесів і розвитку кожної людини гарантії свободи вираження поглядів є визначальними. В принципі, гарантії, встановлені у статті 10, поширюються на вираження будь-яких поглядів — незалежно від їхнього змісту, — котрі поширює та чи та особа, група осіб або засіб масової інформації. Єдине обмеження щодо змісту, до якого вдалася Комісія, стосувалося поширення ідей, що пропагували расистську та нацистську ідеологію, підбурювали до ненависті та расової дискримінації. На підставі статті 17 Конвенції Комісія вирішила, що свобода вираження поглядів не повинна використовуватися для того, щоб зменшувати права й свободи, гарантовані Конвенцією.

Відповідно до статті 10 ЄКПЛ держави зобов'язані обґрунтовувати будь-яке втручання в будь-яке вираження поглядів. З метою визначити ступінь захисту, застосовний до певної форми вираження поглядів, Суд бере до уваги вид поглядів (політичні, комерційні, мистецькі тощо), засоби їх поширення, (тобто поширює їх окрема особа, друкований орган, телебачення абощо), а також аудиторію (дорослі, діти, широкий загал, окрема група). Згідно з цими критеріями, навіть поняття «достовірність» виражених поглядів може мати різне значення.

Свобода дотримуватися своїх поглядів є основною передумовою інших свобод, Гарантованих статтею 10, і вона користується майже абсолютним захистом — у тому сенсі, що можливі обмеження, закладені в пункті 2, до неї не застосовні.

Держави не повинні піддавати своїх громадян ідеологічній «обробці» і не можуть практикувати диференційоване ставлення до осіб, які сповідують ті чи інші ідеї.

Свобода одержувати інформацію включає право збирати та розшукувати її в усіх можливих законних джерелах, у тому числі й право доступу до міжнародних телевізійних програм.

Свобода одержувати інформацію та ідеї стосується засобів масової інформації в плані надання їм можливості передавати таку інформацію та ідеї загалові, але складником цієї свободи, на думку Суду, є також і право громадськості на достатню поінформованість, зокрема з питань, що становлять громадський інтерес.

Хоч у статті 10 про свободу преси безпосередньо не згадано, Європейський суд напрацював значний масив прецедентної практики, в якій фактично міститься звід принципів і правил, які забезпечують пресі особливий статус щодо користування передбаченими цією статтею свободами.

Свобода преси користується особливим статусом і тоді, коли на кін поставлено інші питання, що становлять предмет громадського інтересу. У справі Торґейрсона йшлося про те, що заявник виступив у пресі із заявою проти поширеної практики поліцейських вдаватися до брутальних дій і назвав їх «звірами в уніформі», «особами, чий інтелектуальний рівень зведено до рівня немовляти через застосування задушливих захватів, яких поліцейських і охоронців навчають і до яких вони вдаються з брутальною бездумністю», та охарактеризував засоби, за допомогою яких поліція намагається захищатися, а саме: «залякування, підробка документів, незаконні дії, марновірство, нерозсудливість і тупість». У своїй країні Торґейрсона було піддано судовому переслідуванню та оштрафовано за дискредитацію працівників поліції. Європейський суд визнав, що заявник ставив питання про брутальну поведінку поліції в масштабах своєї країни і «...що на пресу покладено місію передавати інформацію та ідеї з питань, які становлять громадський інтерес». Окрім того, Суд заявив, що «в його прецедентному праві немає підстав для різного підходу до політичної дискусії та дискусії з інших питань, що зачіпають інтереси суспільства». І нарешті, Суд охарактеризував засудження Торґейрсона як «таке, що може перешкоджати відкритому обговоренню питань, що становлять громадський інтерес».

Іншим важливим питанням у контексті свободи преси є публікація чуток і тверджень, яких журналісти не в змозі довести. Як уже згадувалося, Суд поділяє думку, що оцінні судження не вимагають доведення.

**4. Стаття 11 цієї ж Конвенції – зібрання, об’єднання та участь онлайн.**

Конвенція про захист прав людини і основоположних свобод , яка набрала чинності для України 11 вересня 1997 р., відповідно до ст. 8 Конституції України є частиною національного законодавства. Стаття 11 Конвенції гарантує свободу мирних зібрань. Подібні положення містить ст. 39 Конституції України, яка проголошує право громадян збиратися мирно, без зброї і проводити збори, мітинги, походи і демонстрації, про проведення яких завчасно сповіщаються органи виконавчої влади чи органи місцевого самовря- дування. Обмеження щодо реалізації цього права може встановлюватися судом відповідно до закону і лише в інтересах національної безпеки та громадського порядку — з метою запобігання заворушенням чи злочинам, для охорони здоров’я населення або захисту прав і свобод інших людей.

Варто також наголосити, що Законом про ратифікацію Конвенції від 17 липня 1997 р. No 475/97-ВР Україна повністю визнала юрисдикцію Європейського суду з прав людини в усіх питаннях, що стосуються тлумачення і застосування Конвенції, а відповідно до ст. 17 Закону України «Про виконання рішень та застосування практики Європейського суду з прав людини» від 23 лютого 2006 р. № 3477-IV суди застосовують при розгляді справ Конвенцію та практику Суду як джерело права.

**5. Приватність і захист даних.**

**Право на приватність та Інтернет** – два явища, які з’явилися у двадцятому столітті і зобов’язані йому своїм народженням. Перше з’явилося раніше, на початку століття. Друге - на півстоліття пізніше, і як молодше спробувало похитнути старше, звести приватність мешканців кібернетичного простору – користувачів Інтернет - нанівець.

Обсяг даних, що записуються про людей буде продовжуватися розширюватися драматично. Диспути про приватність стають все більш різкими. Спроби стримати суспільство суцільного спостереження через нові закони будуть посилюватися.

Ідея приватності, яка нерозривно пов’язана із категорією свободи особистості, здатна суттєво впливати на самий розвиток інформаційного суспільства. Здатна об’єднувати людей, які цінують власну інформаційну свободу. Є непоодинокі випадки, коли завдяки наполегливості користувачів у відстоюванні своїх інтересів, вдалося запобігти або припинити порушення приватності в Інтернет.

Так, у 1996 році, компанія Yahoo зустріла публічний протест через застосування системи пошуку людей. Можливості системи дозволяли опрацювати дані про 175 мільйонів людей, вибравши їх із списків прямої розсилки реклами. Після отримання претензій, Yahoo вирішила знищити дані з адресами 85-ти мільйонів користувачів, що їх не було включено до цих списків. У 1997 році, компанія American Online (АOL) оприлюднила плани стосовно розкриття даних, які містили телефонні номери передплатників своїм партнерам по бізнесу. Передплатники виступили проти цього і зазначили, що це суттєво порушувало б умови угоди про надання послуги. У відповідь, компанія відмовилася від своїх планів.

Це дає сподівання, що проблема забезпечення приватності в Інтернет буде вирішуватися. Однак постійний розвиток існуючих і поява нових технологій вимагають прийняття адекватних заходів для забезпечення права на приватність користувачів глобальної мережі Інтернет.

**Право на приватність.** Приватна сторона життя людини отримала свій правових захист у вигляді права на приватність (right to privacy) не так давно. Своє світове визнання право на приватність отримало саме у двадцятому столітті, що пов’язано із появою нових технологій, завдяки яким втручання у приватну сферу життя людини значно спростилося.

З розвитком телекомунікаційних технологій, появою комп’ютерів і поширенням автоматизованої обробки персональної інформації, право на приватність набуває додаткового змісту. У відомому рішенні Федерального Конституційного Суду Німеччини, датованому 1983-тім роком воно сформульовано як право індивіда на інформаційне самовизначення.

**Концепція інформаційної приватності,** яка виросла з фундаментального права на повагу до приватного життя, на сучасному етапі перетворила цю категорію в окрему галузь права із своїми інститутами, суб’єктами і правовідносинами. В її основу покладено систему прав особи, що є суб’єктом даних, і якій кореспондують відповідні обов’язки інших суб’єктів стосовно дотримання правил роботи з персональними даними:

**Різновиди шахрайства в електронній комерції:**

- дані навмисно перехоплюються, читаються або змінюються.

- користувачі ідентифікують себе неправильно.

- користувач отримує несанкціонований доступ з однієї мережі до іншої.

**Засоби захисту інформації:**

1. **Шифрування інформації.** Шифрування використовується для автентифікації і збереження таємниці. Шифрування – метод перетворення первісних даних у закодовану форму. Криптографічні технології (методи захисту даних з використанням шифрування) забезпечують три основних типи послуг для електронної комерції: автентифікацію, неможливість відмови від здійсненого, збереження таємниці. Автентифікація – метод перевірки не тільки особистості відправника, а й наявності чи відсутності змін у повідомленні. Реалізація вимоги неможливості відмови полягає в тому, що відправник не може заперечити, що він відправив певний файл (дані), а отримувач – що він його отримав (це схоже на відправлення замовного листа поштою). Збереження таємниці – захист повідомлень від несанкціонованого перегляду.

**2. Симетричне шифрування або шифрування з таємним ключем.** Це найдавніша форма шифрування з використанням ключа. Під час шифрування за такою схемою відправник і одержувач володіють одним ключем, з допомогою якого обидва можуть зашифровувати і розшифровувати інформацію. Однак існують проблеми з автентичністю, оскільки особистість відправника або одержувача повідомлення гарантувати неможливо.

**3. Криптографія з відкритим ключем.** Заснована на концепції ключової пари. Кожна половина пари (один ключ) шифрує інформацію так, що її може розшифрувати тільки інша половина (другий ключ). Одна частина ключової пари – особистий ключ – відома тільки її власнику. Інша половина – відкритий ключ – розповсюджується серед усіх його респондентів, але зв'язана тільки з власником. Ключові пари володіють унікальною властивістю: дані, зашифровані будь-яким з ключів пари, можуть бути розшифровані тільки іншим ключем з цієї пари.

**Щодо захисту комерційної інформації їх поділяють на дві групи:**

- системи на основі пластикових карток;

- системи на основі цифрових грошей.

В інформатиці поняття комп’ютерної безпеки є досить широким, воно має на увазі такі поняття: надійність збереження даних і програмного забезпечення, захист даних від несанкціонованого доступу, крадіжки інформації, програмного забезпечення і апаратного забезпечення, захист від вірусів, збереження таємниці листування.

Об’єктами злочину можуть бути інформаційне забезпечення, технічне забезпечення, з другого боку вони можуть виступати інструментом злочину.

Комп’ютерні злочини бувають навмисні і ненавмисні. Ще їх можна поділити на: несанкціонований доступ до інформації (як правило за допомогою чужого імені, зміною фізичних адрес, модифікація ПЗ та ІЗ; хакери - електронні пірати, які виконують несанкціонований доступ); введення в ПЗ логічних бомб (бомби починають працювати після виконання певних умов, це не програми, що само розповсюджуються, бувають часові бомби і троянські програми; вони частково виводять програмне забезпечення з ладу і маскуються під корисні програми, можуть бути застосовані для захисту авторських прав); розробка і впровадження комп’ютерних вірусів; крадіжка і модифікація даних (підключення до каналів передачі даних, крадіжка носіїв інформації, наприклад, зміна результатів голосування).

**Заходи по захисту комп’ютерних систем.**

**- Організаційні заходи** – комплекс адміністративних заходів, спрямованих на оперативне вирішення проблем захисту і регламентації діяльності персоналу, а також порядку функціонування системи.

**- Технічні засоби –** блокування каналів витоку інформації, блокування несанкціонованого доступу до інформаційних ресурсів, сигналізація, ідентифікація, перевірка справності технічного забезпечення.

**- Програмні засоби –** ідентифікація користувачів і ресурсів, розмежування доступу шляхом паролів, кодування інформації (електронний підпис печатка), цілісність даних, реєстрація та облік дій користувачів, маскування, реагування (відключення сигналізація, повідомлення, зупинення роботи) на несанкціонований доступ.

**Лекція № 3**

Тема лекції: Право міжнародних комунікацій

**План лекції**

1. Чому міжнародні комунікації потребують регулювання взагалі, регулювання на міжнародному рівні зокрема?

2. Пошта. Підводні телекомунікаційні кабелі.

3. Світова організація торгівлі й телекомунікації.

4. Міжнародний союз електрозв’язку: загальний огляд.

5. Регламент міжнародного електрозв’язку.

6. Радіочастотний ресурс і геостаціонарні орбіти.

7. Спеціалізовані й надзвичайні телекомунікації.

8. Регулювання міжнародних (теле)комунікацій на регіональному та національному рівнях.

**Література**

* + 1. Закон України «Про інформацію» від 02.10.1992 року // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.
    2. Марущак А.І. Інформаційне право України. Підручник / Марущак А.І. – К.: Дакор, 2011. – 456 с.
    3. Сопілко І. М. Державна інформаційна політика України: стан та шляхи реалізації: монографія / І. М. Сопілко. – К. : МП «Леся», 2014. – 424 с.
    4. B.C.Цимбалюк Основи інформаційного права України / B.C.Цимбалюк, В.Д.Гавловський, В.В.Гриценко та ін. – К.: Видавництво "Знання", 2004
    5. Сопілко І.М. Державна інформаційна політика України: стан та шляхи реалізації: монографія / І.М. Сопілко. – Київ: МП «Леся», 2014. – 424 с.

**Зміст лекції**

**1. Чому міжнародні комунікації потребують регулювання взагалі, регулювання на міжнародному рівні зокрема?**

Знайти нормативні визначення “телекомунікацій” значно легше ніж для “комунікацій”.

Так частина перша статті 1 Закону України від 18 листопада 2003 року № 1280-ІУ «Про телекомунікації» (Закон про телекомунікації) визначає **телекомунікації (електрозв’язок)** як «передавання, випромінювання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних або інших електромагнітних системах». Нормативне визначення коммунікацій знайти важче, але загалом це ширше поняття, що позначає всі способи спілкування між людьми, включаючи телекомунікації, але також різні види поштового зв’язку, кур’єрські служби тощо. І якщо комунікації так чи інакше супроводжують людство протягом усієї його історії, то в епоху телекомунікацій воно вступило менш як два століття тому — із відкриттям і впровадженням електричного телеграфу в XIX столітті.

Міжнародно-правове регулювання телекомунікацій сильно залежить не лише від їхніх технологічних параметрів (дротові, бездротові, супутникові, підводні тощо), але й від економічних умов їхнього функціонування й експлуатації. Більше того, за допомогою юридичних інструментів такі умови регулярно задаються та змінюються. Наприклад глобальний процес приватизації, інтернаціоналізації й дерегуляції телекомунікаційних послуг значною мірою завдячував створенню Світової організації торгівлі та включенню послуг до предмету її відання й регулювання.

Наступна конвергенція — між телекомунікаціями й обчислювальною технікою. Цей процес помічено, наприклад, в одній статті 1996 року: «Індустрія телекомунікацій за своє сторічне існування покладалася на спеціалізовані термінали такі як “телефон” або “набір для відеоконференцій”, або ж “радіо” чи “телевізор”. У кожному разі маємо спеціалізовану скриньку, призначені для єдиної телекомунікаційної функції.

Наступне визначальне слово, що визначало розвиток регуляторних рамок для телекомунікацій за ці роки, — «лібералізація»: тобто телекомунікації (самі по собі та в поєднанні з телерадіомовленням) перестали розглядатися як гарантована суспільна послуга на користь більш комерційно-орієнтованого підходу.

З юридичного боку це було оформлено через включення телекомунікаційних послуг разом із іншими послугами в рамки Світової організації торгівлі, тобто в рамки ГАТС, якщо точніше. Ринки телекомунікаційних послуг зазнали лібералізації по всьому світі. Авжеж стрімкість змін варіювалася, однак самі зміни були більш-менш глобальними. Як наслідок маємо відомий парадокс. За загальним переконанням лібералізація йде рука в руку з дерегуляцією, тобто з усуванням регуляторних бар’єрів і скороченням кількості правил. Цього не спостерігаємо принаймні в царині телекомунікацій, принаймні на національному та європейському комунітарному рівнях. Навпаки, обсяг регуляторного паперу, видається, зростає, що більш вільними й дерегульованими стають ринки.

Наступне визначальне для світового телекомунікаційного сектора слово — **«інтернаціоналізація».** До 90-х років 20-го століття державні кордони були нездоланною перешкодою для входу гравців із-за кордону на національні телекомунікаційні ринки (якщо це так можна назвати), де безроздільно панували національні монополії, сильно контрольовані урядами. Певний виняток становили Сполучені Штати й Канада, котрі покладалися на немонополістичні комерційні підприємства для забезпечення загалу послугами зв’язку. На сьогодні це вже не так і в багатьох частинах світу, у Європі насамперед, на ринках телекомунікацій панують багатонаціональні компанії.

**Регіоналізація.** Уже згадано дедалі більшу активність, проявлену ЄС у регулюванні комунікацій, починаючи з кінця 80-х. Загалом загальносвітова тенденція регіональної економічної інтеграції дала про себе знати вусьому світі.

Зважаючи на стрімкі й дедалі стрімкіші зміни у світі (теле)комунікацій розумно запитати, чи є лишається в них щось стабільне і чи не застаріє інформація цього курсу негайно після його завершення.

Деякі речі не змінюються, принаймні не так швидко. Фізична інфраструктура — одна з них. Хоча телефонні дроти як інструмент зв’язку все більше поступається бездротовим мобільним мережам, ніхто не збирається поки ліквідувати кілометри протягнутих дротів. По-друге, сама організація міжнародних комунікацій також доволі стабільна, які би технології не покладались у її основу:

Міжнародний контур обміну даними складається з трьох сегментів: внутрішнього сегменту країни, де контур починається, внутрішнього сегменту країни, де контур закінчується, та міжнародного сегменту, що з’єднує два внутрішні сегменти. Внутрішні сегменти забезпечує одна чи декілька національних організацій зв’язку, а міжнародний сегмент — одна чи декілька організацій міжнародного зв’язку. З’єднання між внутрішніми й міжнародними постачальниками здійснюються в певних “містах-шлюзах”, визначених двома країнами як точки з’єднання. Успішні міжнародні комунікації вимагають координації та співпраці між усіма залученими постачальниками, регуляторами від урядів відповідних країни, а також додержання погоджених міжнародних стандартів.

**2. Пошта. Підводні телекомунікаційні кабелі.**

**По́шта**(від [лат.](https://uk.wikipedia.org/wiki/%D0%9B%D0%B0%D1%82%D0%B8%D0%BD%D1%81%D1%8C%D0%BA%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0) posta) — установа для транспортування повідомлень (наприклад [листів](https://uk.wikipedi), [листівок](https://uk.wikipedia.org/wiki/%25D0%259F%25D0%25BE%25D)), дрібних товарів, частково людей. Найчастіше вона є державною установою. Більшість поштових організацій перебувають у [Всесвітньому поштовому союзі](https://uk).

Стаття 1 Закону України про «Про поштовий зв’язок» визначає **поштовий зв'язок** як «приймання, обробка, перевезення та доставка (вручення) поштових відправлень, виконання доручень користувачів щодо поштових переказів, банківських операцій». Поштове же відправлення визначено як «листи, поштові картки, бандеролі, секограми, дрібні пакети, міжнародні відправлення з оголошеною цінністю, посилки, прямі поштові контейнери, оформлені відповідно до законодавства України». Як уже зазначалося, поштовий зв’язок охоплюється ширшою категорією комунікації та не належить до телекомунікацій ні в національному, ні в міжнародно-правовому, ні у побутовому розумінні. Історично передуючи телекомунікаціям, цей тип зв’язку поступово здавав останнім свої позиції та втрачав значення для спілкування на далекі відстані, через що правомірне запитання про виправданість уваги, приділеної пошті в цьому курсі. Потребу хоча би побіжно глянути на міжнародно-правові аспекти традиційної паперової пошти можна обґрунтувати щонайменше двома аргументами:1) залишковою важливістю пошти, 2) електронною комерцією та 3) логікою регулювання.

За статистикою Всесвітнього поштового союзу (ВПС) у 2014 році (останній поки рік, що є в базі даних) було доставлено 3 461 381 882 об'єктів письмової кореспонденції (листів, поштівок, друкованих видань, дрібних пакетів, секограм). Загальносвітовий обсяг внутрішньої письмової кореспонденції за той самий рік — 32 390 233 793 (тобто в 9,4 рази більше).

У Середні Віки в Західній Європі паралельно діяли кілька корпоративних поштових систем у рамках Католицької церкви, університетів, між купцями та в рамках певних гільдій (дивним чином навіть у м’ясників), і вони пали першими жертвами з приходом абсолютистських монархій, разом з чим почалась історія пошти в сучасному розумінні слова. Контроль над каналами поширення інформації був важливою складовою концентрації влади в руках монарха та інструментом при розбудові модерної державності. Цей процес задав загальну логіку функціонування поштового

зв’язку на століття наперед, у тому числі її міжнародно-правової складової. Наприклад, 1464 року король Франції Луї XI поклав обмеження на гінців Паризького університету й перебрав на себе контроль над поштовими станціями. Його початковий був зарезервувати поштові потужності для королівських відправлень, але за двадцять років почали доставляти також і приватну пошту аристократів. 1591 року англійська королева Єлізавета І постановила, що лише королівські гінці могли переправляти міжнародні листи. Її мета полягала в установленні монополії над правом спілкуватися з іноземцями, а не просто монополії в (неіснуючому) бізнесі з доставления листів.

Окрім поштової монополії, другим важливим нововведенням, що сформувало сучасну пошту була тарифна реформа, вперше проведена у Великій Британій 1840 року відомим сером Роуландом Хіллом, що була швидко підхоплена рештою світу. Складна система обрахунку вартості кожного окремого поштового відправлення на основі складного набору чинників як-от вага й потенційний маршрут з можливістю післяплат або часткової оплати відправником і одержувачем була замінена простою й одноманітною, за якою всі поштові відправлення мали передплачуватися за одноманітними тарифами, що залежали лише від ваги відправлення. Відстань (принаймні всереднині країни) на ціну не впливала. Технічним інструментом такої системи стала винайдена тоді вперше поштова марка.

**Паризька поштова конференція 1863 року**

Після кількох регіональних ініціатив, у Парижі 1863 року було скликано конференцію п’ятнадцяти держав, щоби внести якийсь порядок у міжнародні відносини в поштовій сфері. Конференція підтримала набір стандартних принципів, що як такі не були обов’язкові, але мали впроваджуватись у подальших поштових угодах. Тобто було запропоновано підхід, якому нині ефективно слідують, наприклад, при уникненні подвійного оподаткування: декілька авторитетних організацій (ООН і ОЕСР) пропонують і регулярно переглядають моделі угод, котрі більш або менш суворо відтворюються в двосторонніх договорах між державами, чим забезпечується одноманітність й узгодженість таких договорів. Але для пошти такий підхід не спрацював і від нього скоро відмовилися на користь повноцінного багатостороннього регулювання

1874 року в Берні (Швейцарія) представники двадцяти держав Європи, Сполучених Штатів і Єгипту уклали перший багатосторонній поштовий договір, заснувавши «**Загальний поштовий союз**». Оскільки незабаром до ініціативи приєдналася низка інших націй, то структуру перейменували на «Всесвітній поштовий союз», що став другою найдавнішою міжнародною організацією у світі, що досі діє. Дата підписання Бернського договору — 9 травня — святкується нині як Всесвітній день пошти.

Міжнародне право стикається з підводними кабелями в двох точках: права на прокладання кабелів у різних зонах Світового Океану (“laying rights") т заходи на убезпечення кабелів від різних загроз, насамперед пов’язаних із людською діяльністю.

**Паризька конвенція про захист підводних телеграфних кабелів 1884 року**

Найперший багатосторонній договір, що стосувався кабелів, укладено 1884 року. Це досі чинна Паризька конвенція про захист підводних телеграфних кабелів, 380381 Попри слово «телеграфний» у назві перша стаття передбачає, що “ця Конвенція застосовується за межами територіальних вод до всіх правомірно прокладених підводних морських кабелів [a tous les cables sous-marins legalement etablis] з виходом на суходіл на територіях, в колоніях або інших володіннях однієї чи декількох Високих Договірних Сторін». Тобто уточнення про функціональне призначення кабелів у тексті відсутнє. Як буде показано далі, Женевські конвенції 1958 року та Конвенція ООН з морського права 1982 також юридично не розрізняють підводні морські кабелі за функціями: так що телекомунікаційні кабелі мають такий самий міжнародно-правовий режим, що й високовольтні електричні.

У найзагальніших рисах Паризьку конвенцію можна класифікувати як класичну кримінально-правову конвенцію, адже її ключовий метод правового регулювання й основне зобов’язання — криміналізувати умисне пошкодження підводних морських кабелів: «Є караним діянням поламка чи пошкодження підводного морського кабелю, умисні чи внаслідок злочинної недбалості [negligence coupable], у такий спосіб, що може перервати чи перешкодити телеграфному зв’язку повністю або частково, причому таке покарання застосовується без шкоди для будь-якого цивільного позову про компенсацію заподіяної шкоди» (Пункт 1 статті 2). Згадка саме про «телеграфний зв’язок» створює сьогодні певну амбівалентність, утім загалом є тенденція тлумачити Конвенцію як застосовну до кабельного зв’язку будь-якого типу, включно з передачею голосу й цифрових даних у вигляді електричних або оптичних сигналів.

**Підводний комунікаційний кабель**— кабель, який прокладено по [морському](https://uk.wikipedia.org/wiki/%D0%9C%D0%BE%D1%80%D1%81%D1%8C%D0%BA%D0%B5_%D0%B4%D0%BD%D0%BE) чи [океанічному дну](https://uk.wikipedia.org/wiki/%D0%9E%D0%BA%D0%B5%D0%B0) для забезпечення передачі даних через водойму. Перші підводні комунікаційні кабелі були прокладені в 1850-х роках та передавали [телеграфні](https://uk.wikipedia.org/w) сигнали. Наступні покоління забезпечували [телефонний](https://uk.wikipedia.org/wiki/%D0%A2%D0%B5%D0%BB%D0%B5%D1%84%D0%BE%D0%BD) зв'язок, потім трафік даних, в тому числі — [Інтернет](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82). Сучасні кабелі використовують [оптоволоконні технології](https://uk.wikipedia.org/wiki/%25D0%259E%25D0%25BF%25D1%2582%25D0%25BE%25D0%25B2%25D0%25BE%25). Як правило, сучасні кабелі мають 69 міліметрів у [діаметрі](https://uk.wikipedia.org/wiki/%D0%94%D1%96%D0%B0%D0%BC%D0%B5%D1%82%D1%80); відрізок в 1 метр важить приблизно 10 кілограмів. Тонші та легші кабелі використовуються на глибоководних ділянках. Станом на [2010](https://uk.wikipedia.org/wiki/2010%22%20%5Co%20%222010) рік, підводні кабелі сполучають всі континенти, окрім [Антарктиди](https://uk.wikipedia.org/wiki/%D0%90).

**3. Світова організація торгівлі й телекомунікації.**

**Світова організація торгівлі (СОТ)**— це міжнародна організація, метою якої є розробка системи правових норм міжнародної торгівлі та контроль за їх дотриманням. Головними цілями Організації є забезпечення тривалого і стабільного функціонування системи міжнародних торговельних зв’язків, лібералізація міжнародної торгівлі, поступове скасування митних і торговельних обмежень, забезпечення прозорості торговельних процедур.

СОТ була створена у січні 1995 року після підписання відповідної багатосторонньої угоди у м.Марракеш (Марокко) 15 квітня 1994 року. СОТ стала правонаступницею Генеральної угоди з тарифів і торгівлі (ГАТТ) - організації, яка проіснувала з 1947 по 1994 рік і нараховувала 128 членів. У рамках ГАТТ було проведено вісім раундів багатосторонніх переговорів, спрямованих на лібералізацію торгівлі, скасування тарифних обмежень та зниження митних зборів. У ході переговорів було укладено 28 угод, що формують основу нормативно-правової бази СОТ, основними з яких є ГАТТ, Генеральна Угода з торгівлі послугами (ГАТС), Угода про торговельні аспекти прав інтелектуальної власності (ТРІПС), Угода про вирішення спорів, Угода про сільське господарство, Угода про застосування санітарних та фітосанітарних заходів, Угода про технічні бар'єри в торгівлі, Угода про правила походження, Угода про процедури імпортного ліцензування, Угода про пов'язані з торгівлею інвестиційні заходи, Угода про субсидії та компенсаційні заходи, Угода про захисні заходи.

Станом на вересень 2015 року членами СОТ є 161 країна світу, 22 країни ведуть переговори щодо вступу до СОТ. Членство у СОТ передбачає обов’язкову участь у всіх багатосторонніх угодах, крім декількох з обмеженим колом учасників.

Вищим органом СОТ є Міністерська Конференція, яка скликається раз на 2 роки і приймає найбільш важливі рішення у сфері торгівлі. Керівний орган - Генеральна Рада СОТ.

Засідання цього органу проводяться кожні два місяці для здійснення нагляду за функціонуванням організації і виконанням відповідних угод. Генеральна Рада також виступає в якості вищого органу для розв'язання спорів і проведення огляду торговельної політики країн-членів.

Секретаріат СОТ розміщується у Женеві, його очолює Генеральний директор, якому допомагають 4 заступники.

З 1 вересня 2013 року Генеральним директором СОТ є Роберто Азеведо (до обрання обіймав посаду Постійного представника Бразилії при СОТ та інших міжнародних економічних організаціях у Женеві).

Процес вступу України до СОТ розпочався 30 листопада 1993 року, коли до Секретаріату ГАТТ було подано офіційну заявку Уряду України про намір приєднатися до ГАТТ. 5 лютого 2008 року у Женеві відбулося засідання Генеральної Ради СОТ, на якому було підписано Протокол про вступ України до СОТ.

10 квітня 2008 року Верховна Рада України прийняла законопроект «Про ратифікацію Протоколу про вступ України до Світової організації торгівлі». 16 квітня 2008 року Закон про ратифікацію був підписаний Президентом України. Згідно з процедурами СОТ, 16 травня 2008 року Україна стала повноправним членом цієї Організації.

Вступ України до СОТ відкрив перспективи для розвитку національної економіки. Україна на абсолютно рівних умовах та правах з іншими членами організації бере безпосередню участь у формуванні новітніх правил торгівлі на світовому ринку у рамках поточного раунду багатосторонніх торговельних переговорів з метою максимального врахування національних інтересів нашої держави у торговельно-економічній сфері.

Як член СОТ Україна отримала право використовувати механізм врегулювання суперечок в рамках СОТ, що сприяє справедливому вирішенню будь-яких суперечок з приводу дотримання положень угод СОТ, які можуть виникнути у країни з її торговими партнерами. У рамках зазначеного механізму було позитивно вирішено ряд важливих питань, а саме дискримінаційного оподаткування, ліцензування деяких видів української продукції. Україна продовжує використовувати цей механізм СОТ, оскільки це є частиною системних зусиль, спрямованих на забезпечення та розширення присутності українських товарів на інших ринках.

Набуття Україною членства в СОТ створило необхідні передумови для підписання у червні 2010 року Угоди про вільну торгівлю з Європейською асоціацією вільної торгівлі (Норвегія, Швейцарія, Ісландія та Ліхтенштейн), яка набрала чинності з 1 червня 2012 року; стало потужним стимулом для започаткування переговорів з Європейським Союзом щодо створення зони вільної торгівлі. Політичну частину [Угоди про асоціацію з Європейським Союзом](http://uk.wikipedia.org/wik) [України](http://uk.wikipedia.org/wiki/%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B0) було підписано 21 березня 2014 року. Економічну частину цієї угоди було підписано 27 червня 2014 року.

Уряд України здійснює активну зовнішньоторговельну політику шляхом участі нашої країни у багатосторонніх торговельних переговорах та проводить ефективну роботу, спрямовану на реалізацію переваг членства України у СОТ з метою розширення експортних можливостей вітчизняних товаровиробників та захисту економічних інтересів держави на зовнішніх ринках.

Система СОТ створює ефективний механізм для врегулювання торговельних суперечок. Після Другої світової війни торгуючі країни в ході переговорів погоджували правила торгівлі, які зараз діють у рамках СОТ. Вони містять у собі зобов'язання щодо розгляду своїх суперечок у СОТ і незастосування однобічних дій.

Кожна суперечка, що виноситься у СОТ, розглядається насамперед з огляду на діючі норми і правила. Після ухвалення рішення країни концентрують свої зусилля на його виконанні, і, можливо, наступному перегляді норм і правил шляхом переговорів. З моменту створення СОТ в 1995 році близько 200 торговельних суперечок було винесено на її розгляд. Угоди СОТ створюють правову основу для ухвалення чіткого рішення.

Число суперечок, які виносяться у СОТ, постійно збільшується. Це свідчить не про наростання напруженості у світі, а скоріше про зміцнення економічних зв'язків і довіру країн, до даної системи врегулювання суперечок.

**4. Міжнародний союз електрозв’язку: загальний огляд. Регламент міжнародного електрозв’язку.**

**Міжнародний союз електрозв’язку** (МСЕ) – спеціалізована установа ООН у сфері глобального електрозв’язку, покликана здійснювати законодавчі, управлінські, виконавчі та консультативні функції, надавати технічну підтримку, розробляти стандарти і правила у сфері електрозв’язку та формулювати рекомендації, спрямовані на активізацію розвитку телекомунікацій та підвищення якості послуг.

**Основною метою співробітництва України** у рамках МСЕ залишається вдосконалення та раціональне використання інформаційно-комунікаційної інфраструктури, а також долання «цифрового розриву» в телекомунікаційних технологіях на національному та міжнародному рівнях. Супутньою метою співпраці з МСЕ залишається спільна діяльність з розробки та використання відкритих, функціонально сумісних, недискримінаційних міжнародних стандартів, що визначаються споживчим попитом.

Важливого значення для України також набуває діяльність дослідних комісій МСЕ, яка охоплює сферу технічного прогресу і міжнародної стандартизації в області мовлення, а також споріднених йому аудіовізуальних та мультимедійних застосувань, заснованих на використанні радіотехнологій

Супутньою метою сучасного етапу співробітництва України у рамках МСЕ у галузі міжнародної стандартизації мовлення є забезпечення міжнародного правового захисту сумісного використання в Україні радіомовних аналогових і цифрових систем, служб і технологій на весь перехідний період від аналогового до цифрового мовлення, врахування національних інтересів України під час розроблення міжнародних нормативних документів, що стосуються стратегії впровадження цифрового мовлення, подолання цифрового розриву, а також створення цифрових служб нових поколінь.

Генеральним секретарем МСЕ є представник Китаю Хоулінь Чжао (2015-2018 рр.).

Керівний орган – Повноважна конференція, яка скликається раз на чотири роки і обирає Раду МСЕ в складі 46 членів, яка проводить свої засідання щорічно. Представники усіх країн-членів МСЕ на Повноважній конференції визначають основні напрямки діяльності кожного сектора і формують нові робочі групи та затверджують плани робіт на наступні чотири роки.

Структура МСЕ включає наступні підрозділи: МСЕ-Р (ITU-R) - Сектор радіозв’язку. [МСЕ-Т (ITU-T) - Сектор стандартизації електрозв’язку](http://www.itu.int/ru/ITU-T/Pages/default.aspx%22%20%5Ct%20%22_blank). [МСЕ-Д (ITU-D) - Сектор розвитку електрозв’язку](%22http://).

Усі сектори мають дослідні комісії.

Ключові заходи МСЕ проводяться як правило раз на чотири роки. Серед них:

- Всесвітня конференція радіозв’язку (ВКР)

- Всесвітня асамблея стандартизації електрозв’язку (ВАСЕ)

- Всесвітня конференція розвитку електрозв’язку (ВКРЕ)

- Повноважна конференція (ПК)

- Засідання Ради МСЕ – раз на рік.

ВКР проводяться кожні три-чотири роки. До завдань ВКР відноситься аналіз і, в разі необхідності, перегляд Регламенту радіозв’язку. Перегляди здійснюються на основі порядку денного, який визначається Радою МСЕ і враховує рекомендації попередніх ВКР. Попередній порядок денний ВКР встановлюється завчасно за чотири-шість років,

**Адміністративні регламенти** (Регламент радіозв'язку і Регламент міжнародного електрозв'язку), які доповнюють Статут і Конвенцію, регулюють використання засобів електрозв'язку. Останній варіант Регламенту радіозв'язку був підписаний 4 липня 2003 року (Женева), а більшість його положень вступили в чинності 1 січня 2005 р Регламент міжнародного електрозв'язку було підписано 9 грудня 1988 року (Мельбурн) і вступив в чинності 1 липня 1990 р Адміністративні регламенти відносяться до основних документів МСЕ і обов'язкові для дотримання всіма його членами.

Основні документи МСЕ повинні дотримуватися не тільки державами-членами, а й експлуатаційними організаціями, які отримують у держави дозвіл на створення і експлуатацію служби електрозв'язку і які беруть участь в міжнародних службах.

**5. Радіочастотний ресурс і геостаціонарні орбіти.**

ЗаконУкраїни “Прорадіочастотний ресурс України” визначив **радіочастотний ресурс -** частина радіочастотного спектра, придатна для передавання та/чи приймання електромагнітної енергії.

Відповідно до Декларації керівних засад використання мовлення через супутники для вільного поширення інформації, розвитку освіти і розширення культурних обмінів (Париж, 15 листопада 1972 року) і ч. 2 ст. 44 Статуту Міжнародного союзу електрозв'язку, радіочастоти і орбіта геостаціонарних супутників є обмеженими природними ресурсами, що належать усім народам і їх використання регулюється Конвенцією Міжнародного союзу електрозв'язку та її Регламентом радіозв'язку. Статут Міжнародного союзу електрозв'язку і Конвенція Міжнародного союзу електрозв'язку (Женева, 22 грудня 1992 року) ратифіковані Законом України від [15 липня](https://uk.wikipedia.org/wiki/15_%D0%BB%D0%B8%D0%BF%D0%BD%D1%8F) [1994](https://uk.wikipedia.org/wiki/1994%22%20%5Co%20%221994) року.

Положення міжнародно-правових актів відображені у п. 4 Концепції розвитку зв'язку України до 2010 року, затвердженої постановою Кабінету Міністрів України від [9 грудня](%22https) [1999](https://uk.wikipedia.org/wiki/1999%22%20%5Co%20%221999) року № 2238, згідно з яким, радіочастотний ресурс є обмеженим природним ресурсом, ефективність використання якого впливає на економічне становище країни та на стан довкілля.

 Кабінет Міністрів України затверджує такі нормативно-правові акти: Національну таблицю розподілу смуг радіочастот; [План використання радіочастотного ресурсу України](https://uk.wikipedia.org/wiki/%D0%9F%D0%BB%D0%B0%D0%BD_%D0%B2%D0%B8%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D0%B0%D0%BD%D0%BD%D1%8F_%D1%80%D0%B0%D0%B4%D1%96%D0%BE%D1%87).

Національна таблиця розподілу смуг радіочастот України регламентує розподіл смуг радіочастот радіослужбам в Україні; розподіл на смуги спеціального та загального користування; тощо.

[**Геостаціонарна орбіта**](http://ru.wikipedia.org/wiki/%D0%93%D0%B5%D0%BE%D1%81%D1%82%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%B0%D1%80%D0%BD%D0%B0%D1%8F_%D0%BE%D1%80%D0%B1%D0%B8%D1%82%D0%B0%22%20%5Ct%20%22_blank)**(ГСО**) – кругова орбіта, що розташована над екватором Землі, супутник рухається по цій орбіті з такою ж кутовою швидкістю, що і обертається Земля. Список геостаціонарних супутників починається і закінчується від [Міжнародної лінії зміни дат](https://uk.wikipedia.org/wiki/%D0%9C%D1%96%D0%B6%D0%BD%D0%B0%D1%80%D0%BE%D0%B4%D0%BD%D0%B0_%D0%BB%D1%96%D0%BD%D1%96%D1%8F_%D0%B7%D0%BC%D1%96%D0%BD%D0%B8_%D0%B4%D0%B0%D1%82). Ге[остаціонарні супутники](https://uk.wikipedia.org/wiki/%D0%93%D0%B5%D0%BE%D1%81%D1%82%D0%B0%D1%86%D1%96%D0%BE%D0%BD%D0%B0%D1%80%D0%BD%D0%B0_%D0%BE%D1%80%D0%B1%D1%96%D1%82%D0%B0) розташовані строго над [екватором](%22h), на висоті 35 786 км над рівнем моря, у зв'язку з цим для опису положення супутника досить вказати, над яким [меридіаном](https://uk.wikipedia.org/wiki/%25D0%259) він знаходиться.

Для нерухомого наземного спостерігача геостаціонарний супутник неначе висить в одній і тій же точці неба, не змінюючи свого положення в залежності від часу доби та пори року. Якби геостаціонарні супутники були видні на небі неозброєним оком, то лінія, на якій вони були б видимі, збігалася б із «поясом Кларка» для даної місцевості.

**6. Спеціалізовані й надзвичайні телекомунікації.**

Регулювання міжнародних (теле)комунікацій на регіональному та національному рівнях.

Спеціалізовані й надзвичайні телекомунікації: морські телекомунікації; повітряні телекомунікації; надзвичайні телекомунікації.

Використання телекомунікацій часто становить важливу складову загального зусилля з подолання наслідків природних і рукотворних катастроф. Наявність таких комунікацій забезпечує швидшу реакцію на надзвичайні події та вищу ефективність у застосуванні рідкісних ресурсів.

З іншого боку, самі умови широкомасштабного лиха часто означають, що нормальні (тобто зазвичай залежні від мережі — дротової чи стільникової) комунікації або недоступні, або марні, через що постає потреба в спеціальній апаратурі (супутниковій або портативній). Катастрофи вимагають швидкого розгортання спеціальних телекомунікацій, що нормально не використовуються широким загалом, у зонах, що постраждали.

Доставка такого обладнання в такі зони часто саме по собі непроста задача, однак юридичний і регуляторний бік справи можуть іще більше все ускладнити. Зазвичай країни встановлюють різноманітні правила для імпортування пристроїв, що емітують радіохвилі. Наприклад, в Україні навіть такі поширені девайси як мобільні телефони вимагають сертифікації.

Правила ввезення можуть бути доволі заплутаними, тож імовірність ненароком щось порушити буває достатньо високою, особливо коли рідкісне професійне іноземне обладнання експлуатується іноземними фахівцями, запрошеними постраждалою країною лише задля допомоги в подоланні наслідків лиха. Нарешті, навіть достатньо прості імпортні правила можуть скласти серйозну перешкоду, навіть стандартна вимога заплатити (високі чи навіть помірні) мита на ввезену апаратуру.

Навіть якщо залучені особи достатньо обізнані про правила, що застосовуються, слідування всім процедурам може забрати багато дорогоцінного часу, що в ситуації лиха може означати майнові втрати, шкоду довкіллю, подекуди людські жертви.

Отже, ключові питання використання телекомунікацій для подолання наслідків лих, що потребують міжнародно-правової відповіді, наступні:

- зняття чи пом’якшення внутрішніх юридичних і адміністративних перешкод використанню телекомунікацій у надзвичайних ситуаціях;

- забезпечення провайдерам надзвичайних телекомунікаційних послуг захисту від пов’язаних юридичних ризиків, а також гарантування власності (особливо телекомунікаційної апаратури) таких провайдерів від експропріації та інших посягань.

**Лекція № 4**

Тема лекції: Вирішення спорів онлайн

**План лекції**

1. Огляд курсу. Введення у вирішення спорів онлайн.

2. Альтернативне вирішення спорів і вирішення спорів онлайн.

3. Онлайн посередництво та арбітраж.

4. Кібер суди – на порозі нової реальності?

5. Онлайн методи та належна правова процедура онлайн.

6. Регулювання спорів онлайн.

7. Вирішення спорів онлайн і виконання.

8. Вирішення спорів онлайн і світовий ринок.

**Література**

* + 1. Закон України «Про інформацію» від 02.10.1992 року // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.
    2. Марущак А.І. Інформаційне право України. Підручник / Марущак А.І. – К.: Дакор, 2011. – 456 с.
    3. Сопілко І. М. Державна інформаційна політика України: стан та шляхи реалізації: монографія / І. М. Сопілко. – К. : МП «Леся», 2014. – 424 с.
    4. B.C.Цимбалюк Основи інформаційного права України / B.C.Цимбалюк, В.Д.Гавловський, В.В.Гриценко та ін. – К.: Видавництво "Знання", 2004
    5. Резолюція 60/45, прийнята Еенеральною Асамблеєю Організації Об’єднаних Націй, «Досягнення у галузі інформатизації та телекомунікацій в контексті міжнародної безпеки» від 08.12.2005 р. – Електронний ресурс. – Режим доступу: <http://zakonl.rada.gov.ua/laws/show/995_e45>
    6. Пазюк А.В. Правові засоби захисту та відновлення прав користувачів Інтернету в Україні в контексті застосування Посібника Ради Європи з прав людини для інтернет-користувачів [Електронний ресурс] / А.В. Пазюка. – К. : ФОП Клименко, 2015. – 128 с. – Режим доступу: <https://rm.coe.int/1680599465>
    7. Посібник з прав людини для інтернет-користувачів та пояснювальний меморандум [Електронний ресурс]. - Режим доступу: https://rm.coe.int/16802e3e96

**Зміст лекції**

**1. Огляд курсу. Введення у вирішення спорів онлайн.**

Інтернет та цифрові технології змінюють наш світ. Вирішення спорів онлайн (ВСО) це сукупність різноманітних процедур, призначених для запобігання, управління або вирішення спірних ситуацій в Інтернет-середовищі.

У той час як Інтернет був створений у 1969 році у США, потреба в ВСО з’явилась лише на початку 1990-х років. За перші два десятиліття Інтернетом користувалась обмежена кількість людей, а також можливості такого використання були обмеженими. Доступ в Інтернет був пов'язаний або з військовими або з науковими установами, і навіть в тому середовищі, відносно невелике число комп’ютерів мали доступ до Інтернету. Різноманітні зображення на екранах і електронна пошта з рекламою є звичайним явищем сьогодні, вони все ж були невідомі в той час. У свою чергу, всесвітня павутина (WWW) була створена у 1989 році.

Насправді, ВСО відзначає свій початок двадцять років тому - від епохальної статті Девіда Джонсона і Девіда Поста, «Закон і кордони - поширення права в кіберпросторі»394. Ця подія співпадає з десятою річницею ще значної для кібер права події. У травні 1996 року в тому ж місяці, коли на світ з’явилась вищезгадана стаття, була проведена перша конференція з врегулювання суперечок онлайн. На ній обговорювалось не так прийняття правил для кіберпростору, як розбудова механізмів для врегулювання суперечок, що виникають в кіберпросторі. Зустріч поклала початок руху онлайн вирішення спорів, який розвинувся з одного спору, який виник в межах проекта Віртуальний магістрат (Virtual Magistrate) і набув величезних масштабів у кілька мільйонів спорів, оброблених SquareTrade, Інтернет стартапом, який став найбільшим провайдером вирішення спорів в світі.

У статті Джонсон і Пост дали початок досить жвавій і досі триваючій дискусії про створення правил для кіберпростору. Ризикуючи занадто спростити стан речей, одна зі сторін в цій суперечці вважає, що територіальні держави є відповідним джерелом для будь-яких правил, пов’язаних з діяльністю в кіберпросторі. Інший підхід, викладений в статті, полягає у тому, що є достатньо підстав вважати кіберпростір окремим місцем, яке може і повинно мати свої власні правила. В принципі, основне питання щодо впливу нових технологій зводиться до впливу ІКТ на владу ідержави в контексті забезпечення дотримання закону.

Рішення Національного наукового фонду (США) у 1992 році про зняття заборони на здійснення комерційної діяльності в Інтернеті є досить спірним і надзвичайно значним. Після зняття заборони, почали виникати перші спори пов’язані з Інтернет-комерцією. У 1994 році, наприклад, з’явився перший комерційний спам: два юриста намагалися завербувати клієнтів взяти участь в імміграційному шахрайстві. Через кілька місяців, Федеральна комісія з торгівлі США («ФТК») представила свій перший випадок нібито онлайнового шахрайства. Випадок був пов’язаний з AmericaOnline, який рекламує наступне: Всього за $ 99,00 ми покажемо вам, як створити файл абсолютно нового кредиту в усіх 3-х з основних кредитних бюро ... 100% легально і 200% гарантовано.

ФТК не вважає це законним або гарантованим. В результаті, абонент погодився припинити рекламу кредитних програм і надав компенсації споживачам.

Проект ECODIR (електронне вирішення спорів між споживачами) за сприяння Європейської комісії, був також результатом роботи в Центрі з досліджень публічного права Університету Монреаля. ECODIR був консорціумом європейських (Universite de Namur, CNRS, і Університетський коледж в Дубліні) і канадських (CRDP та eResolution) партнерів, метою якого було запропонувати електронну платформу для європейських споживачів, щоб вони могли владнати розбіжності під час електронної торгівлі. Платформа для переговорів і посередництва була зроблена доступною сторонам в жовтні 2001 року. Вона стала першою в Європі.

ВСО може бути застосовано в цілій низці суперечок: від міжособистісних суперечок, включаючи споживача до споживчих спорів або розірвання шлюбу; в судових спорах і міждержавних конфліктах. Вважається, що ефективні механізми врегулювання суперечок через Інтернет будуть впливати на розвиток електронної комерції. У той час як застосування ВСО не обмежується спорами, що виникають у сфері бізнесу та споживчими спорами в Інтернеті, все ж воно, здається, найбільш відповідним для цих сфер, оскільки логічно використовувати те ж саме середовище (Інтернет) для вирішення торгівельних електронних суперечок, коли сторони часто розташовані далеко одна від одної.

ВСО - процес відбувається в основному онлайн для здійснення більшої частини процедури вирішення спорів в Інтернеті, в тому числі початкової подачі, нейтрального призначення, процеси доказування, усні слухання, якщо це необхідно, онлайн-обговорення та навіть винесення обов’язкових рішень.

Таким чином, ВСО - це інше середовище для вирішення спорів, від початку до кінця, з дотриманням відповідних принципів. В якості реагування на зростаючу потребу в стабільних механізмах ВСО, що випливають із діяльності в Інтернеті, Національний центр з автоматизованих інформаційних досліджень (NCAIR) у 1996 році ініціював конференцію з інтернет-вирішення. Конференція стала найбільш важливою подією в середині 1990-х років, оскільки в її результаті було профінансовано три експериментальні проекти ВСО.

Одним з найперших експериментів в цій області став проект CyberTribunal в рамках Університету Монреаля. Він спочатку викликав великий скептицизм в міжнародному юридичному співтоваристві. Проект був запущений в 1996 році, щоб запропонувати споживачам повністю онлайн посередництво і арбітражні послуги для вирішення спорів між ними і онлайн-продавцями. У той час, більшість юристів не могли собі уявити, як технологія може бути використана для проведення або повністю юридичних (наприклад, арбітраж для спорів щодо доменних імен) або напівправових процедур (таких, як посередництво) без фізичної присутності сторін. їх присутність вважалась необхідною на всіх етапах судового розгляду. У правовому розумінні, те що сторони або їхні адвокати мають бачити один одного є прописною істиною. Така скритність і сумніви все ж не зупинили ініціаторів проекту. Структура університету добре підходить для проведення експериментів і випробувань попри будь-які сумніви. Проект CyberTribunal також вписується в дослідження в ЧПВР з права інформаційних технологій. Дійсно, саме дослідження в цій області й породило думку про CyberTribunal. CyberTribunal був заснований на наступних постулатах: • 3 поширенням різних інформаційних операцій в Інтернеті, будуть виникати конфлікти, які традиційне національне законодавство не буде в змозі вирішити в силу позатериторіального характеру кіберпростору;

Дослідники хотіли з’ясувати, наскільки ефективним може бути онлайн-посередництво, коли взаємодія відбувається без особистих зустрічей.

Експеримент показав, що більше 75% користувачів eBay висловили бажання взяти участь в онлайн-посередництві тоді як в інших експериментах з автономного посередництва число учасників, що бажали взяти участь було близько 50%. У всіх випадках пояснювалось, що посередництво є добровільним процесом. Сайт eBay - це віртуальний ринок, де зустрічаються покупці і продавці. Тому громадська безпека є дуже важливою, і це досягається за рахунок декількох засобів, серед яких «рейтингова система зворотного зв’язку» є найбільш важливою.

**2. Альтернативне вирішення спорів і вирішення спорів онлайн.**

«**Альтернативне врегулювання спорів (АВС)**- це група процесів, за допомогою яких вирішуються спори і конфлікти без звернення до формальної системи судочинства. Включає: **Основні види АВС – переговори, арбітраж та медіація.**

**Арбітраж** – це процес, у ході якого дві сторони зустрічаються в присутності нейтральної третьої особи, яка є спеціально підготовленим арбітром та вислуховує обидві сторони і потім виносить обов’язкове або необов’язкове для виконання сторонами рішення, залежно від того, про що сторони домовились заздалегідь (як правило, у контракті). Фактично арбітраж створює приватну судову систему. Якщо одна із сторін не бажає дотримуватися умов рішення, примусити таку сторону до виконання рішення можна через державний суд.

Міжнародний арбітраж використовується, коли сторони або предмет спору знаходяться в різних юрисдикціях. Зазвичай сторони укладають угоду, у якій зазначається, до якого міжнародного арбітражного суду вони можуть звертатися у разі виникнення суперечки. Такий вид арбітражу також використовується урядами для вирішення міжнародних спорів.

Внутрішній арбітраж застосовується, якщо сторони мешкають або мають підприємства, зареєстровані в тій самій країні, і означає, що спір вирішується в третейському суді у цій країні.»

**Медіація** – це метод вирішення спорів із залученням посередника (медіатора), який допомагає сторонам конфліктуналагодити процес комунікації і проаналізувати конфліктну ситуацію таким чином, щоб вони самі змогли обрати той варіант рішення, який би задовольняв інтереси і потреби усіх учасників конфлікту. На відміну від формального судового чи арбітражного процесу, під час медіації сторони доходять згоди самі – медіатор не приймає рішення за них.

**Медіатор** - нейтральна по відношенню до сторін конфлікту третя сторона (спеціально підготовлений посередник), яка сприяє досягненню сторонами взаємоприйнятної згоди розв'язати цей спір, зосереджуючись при цьому на інтересах сторін, а не на правових позиціях або договірних правах.

Комерційна медіація (commercial mediation) - процес вирішення спорів у сфері господарських правовідносин, корпоративного управління та ін. між сторонами, не підпорядкованими одна одній. Для проведення комерційної медіації залучаються сторонні незалежні медіатори. Сторонам забезпечуються рівні можливості обрання незалежного медіатора.

Медіація в організації (work-place mediation) - процес вирішення конфліктів, в якому сторони конфлікту-представники однієї організації, а медіатором може виступати внутрішній або сторонній незалежний медіатор. Така медіація є частиною системи управління конфліктами в організації.

Головні відмінності АВС від судового розгляду: 1. У суб'єкті процедури: домінантне положення самих сторін 2. У предметі процедури: головна увага не фактам, а реальним інтересам 3. У ході процедури: гнучкість та неформальність 4. У результатах та наслідках: взаємоприйнятне рішення, спільно вироблене сторонами.

**Принципи медіації:**

1. Добровільність  2. Конфіденційність  3. Щирість намірів щодо вирішення конфлікту 4. Неупередженість посередника 5. Правомочність сторін 6. Неформальність та гнучкість процедури медіації

Переваги медіації: 1. Економія часу 2. Зниження вартості процесу вирішення спору 3. Можливість впливати на результат 4. Конфіденційність процедури 5. Можливість збереження або відновлення ділових взаємин з партнерами 6. Можливість запобігти виникненню подібних конфліктів у майбутньому 7. Гарантія виконання рішення (у разі успішної медіації)

**Поняття альтернативного вирішення спорів (АВС)**

**Альтернативне вирішення спорів** включає в себе різні підходи до вирішення спорів неконфліктним шляхом, починаючи від переговорів між двома сторонами, багатосторонніх переговорів, посередництва, формування консенсусу та арбітраж.

Альтернативне вирішення спорів (також існує під назвою «належне вирішення спорів») є узагальненим терміном, що використовується для визначення набору підходів і методів, спрямованих на вирішення спорів неконфліктним шляхом. Він охоплює широкий спектр підходів, від участі двох сторін в переговорах як найбільш прямий шлях до досягнення взаємоприйнятного вирішення, до арбітражу і судового рішення, де третя сторона пропонує рішення. В принципі, АВС є чимось «середнім» між двома вище окресленими підходами, це процес «посередництва», за допомогою якого третя сторона допомагає сторонам спору досягти взаємоприйнятного рішення.

Сфера «вирішення спорів» розвивалась як міждисциплінарна галузь з елементами психології, соціології, соціальних досліджень, права,бізнесу, антропології, тендерних досліджень, політичних наук і міжнародних відносин. Дисципліна є складною, тому що вона має справу з конфліктами на різних етапах їх існування, а також тому, що це поєднання теорії та практики, а також мистецтва і науки, як блискуче продемонстрував у своїй книзі «Мистецтво та наука переговорів» (1982) Говард Раіфа. «Наука» є систематичним аналізом вирішення проблем, а «мистецтво» - це навички, особисті здібності і мудрість.

**3. Онлайн посередництво та арбітраж**.

Інтернет посередництво переставляє традиційне посередництво в електронному середовищі. Посередник у справі призначається постачальником послуг або сторонами, а також пропонує рішення спору.

Це може включати заслуховування посередником сторін разом або окремо. Протягом усього процесу, комунікації та обмін документами відбувається в електронному вигляді, наприклад, по електронній пошті (на Internet Neutrals) або за допомогою захищеного веб-сайту (наприклад, ECODIR платформи). Як і в традиційному посередництві, онлайн посередництво є повністю добровільним, а це означає, що сторони можуть вийти з процесу в будь-який час.

Процес онлайн посередництва не надто сильно відрізняється від процесу в автономному режимі, за винятком того, що використовуються інші форми комунікації, ніж під час процедури. Першим кроком в онлайн процесі посередництва є реєстрація скарги на веб-сайті інтернет-посередника або посередницької організації. Наступним кроком є прийняття скарги до розгляду посередницькою організацією; вони будуть зв’язуватися з іншою стороною, щоб з’ясувати, чи готова вона взяти участь в процедурі онлайн-медіації. Якщо попередньо домовитись вдається, то посередник вже або обирається сторонами або в інших призначається на інших умовах. Обидві сторони повинні бути поінформовані про правила медіації, як правило, це досягається за допомогою посилання на відповідному веб-сайті. Посередник представиться і поінформує сторони про процес. У деяких випадках буде підписано угоду про медіацію, про те, що сторони мають намір вирішити свої проблеми шляхом посередництва.

Встановлено, що для сторін три елементи процесу мають важливе значення для його ефективності: позитивність, координація і взаємна увага. У цьому ключі навіть найдрібніші сигнали мають значення. Мова йде про такі знаки як посмішка, напрям погляду, сіпання головою, положення тіла, положення рук і ніг. Зчитуючи та користуючись цими невербальними знаками, посередники можуть безпосередньо впливати на ступінь взаєморозуміння зі сторонами. Взаєморозуміння породжує довіру. Взаєморозуміння створює довіру і впевненість у медіаторі, якщо він встановлює контакт зі сторонами.

**4. Кібер суди – на порозі нової реальності?**

Слід зазначити, що тут мова йде не тільки про використання більшої кількості технологій в звичайному залі суду, а й створення нового типу судів - кібер судів, які пояснюються як «суди, шо вирішують спори за допомогою електронних засобів зв’язку з адвокатами і сторонами без їх перебування в традиційному залі суду, і дозволяють проводити судові засідання в електронному вигляді».

Слід зазначити, що це не нова річ в правовій системі - вона вже розроблена і діє в США. Все більше і більше країн намагаються використовувати і створити цей новий інструмент для вирішення суперечок. Використання кібер судів дозволяє економити час і навіть відстань і не стоїть на заваді засіданням суду, і особливо з використанням альтернативних вирішення спорів засобами. Кібер суди надають можливість вирішити спір, навіть якщо сторони знаходяться в різних країнах. Крім того, не тільки для сторін, а й для суддів система кібер судів допомагає у боротьбі з навантаженнями і проблемами синхронізації. Очевидно, що в багатьох випадках, коли суди змушені дивитися на ситуацію окремо і відкладати або переносити судове засідання. Ці ситуації не допомагають досягти прогресу в суперечці. Як вже було сказано, «основним завданням суду є вирішення спорів. Сторони та адвокати в епіцентрі суперечки весь час зіштовхуються зі старими проблемами щодо часу і витрат. Інформаційні технології відкривають нові і творчі рішення для цих старих проблем».

Через Інтернет і будь-який інші онлайн-системи, використовуючи можливості комп’ютерів в майбутньому зростає ймовірність того, що будуть створені величезні бази даних з матеріалами судового розгляду з вільним доступом сторін спору. Слід також зазначити, що нові технології в правовій системі несуть не тільки переваги. Навіть в залі суду. Заміна людини в судовому процесі може привести до величезної кількості помилок, які можуть залишитися не поміченими. Комп’ютер це машина, яка була створена людиною, і це показує, що немає кращого судді в суперечці, ніж людина. На думку автора, це було б найкраще, коли технології замінять людину в повторюваних, рутинних і процедурних судових завданнях в той час, як прийняття рішень буде покладено на реального суддю - людину.

Віртуальний Проект Магістрат - це арбітражна система запущена в Інтернеті на короткий час в 1996 році, ідея якої полягала в тому, що Інтернет-провайдери, які називалися сісопи, додавали б мову в свої контракти з користувачами, які передбачають будь-які суперечки, які направляються до проекту Віртуального магістрату (ВМ). Зокрема, віртуальна машина була задумана як форма Інтернет самоконтролю для обробки вмісту запитів на видалення до появи Закону про авторське право в цифрову епоху. Американська арбітражна асоціація, Центр Вілланова інформаційного права і політики, а також кілька інших організацій використовували ВМ. ВМ не зв’язувався законами будь-якої конкретної юрисдикції, а, скоріше, став форма арбітражу, рішення якого, підлягають виконанню в судах США.

Хоча він надихнув на багато наукових коментарів, ВМ пропонував лише одне рішення, яке піддалось жорсткій критиці, а потім зник в кібер історії. Наступні послуги альтернативного врегулювання спорів онлайн не стали широко прийняті.

В Мічигані був прийнятий закон в 2002 році для розробки першого цивільного кібер суду. Кібер суд повинен був мати паралельну юрисдикцію з окружними судами штату Мічиган в більш певних комерційних справ з сумою спору понад 25 000 доларів.

Відеоконференції вже широко застосовується в кримінальних судах.

**5. Онлайн методи та належна правова процедура онлайн.**

Воно дозволяє сторонам, арбітрам та адміністратором переглядати, шукати і брати необхідні документи. Проте, онлайн документація може створити ризики безпеки і повинні бути прийняті запобіжні заходи від несанкціонованого доступу.

Засоби телекомунікації, такі як відео конференції, можуть бути використані для заміни традиційних слухань для розгляду і перехресного допиту свідків. Перевагою відеоконференцій є те, що ні свідки, ні сторони, ні арбітри не повинні подорожувати, скорочуючи витрати часу і коштів. Одна з можливих проблем - зв’язок достатньої якості. Це означає, зокрема, що з’єднання дозволяє уникнути затримок і перерв в роботі, і свідка може бути добре видно і чутно. Фізична манера поведінки і тон голосу повинні бути доступними для аналізу, щоб оцінити достовірність. Наприклад, це може бути не очевидним, якщо свідок червоніє, тому що колір монітора не є достатньо яскравим. Таким чином, устаткування повинно бути придатним і з’єднання повинно мати достатню ємність. Для того, щоб уникнути коучингу свідка, картина повинна охоплювати всю кімнату зі свідком, що вимагає щонайменше, дві камери.

Нарешті, найбільша значення надається доказам через відео-зв’язок, якщо представлені обидві сторони або якщо член суду присутній на обох кінцях каналу зв’язку. Однак це не завжди можливо. В якості альтернативи можна скористатися послугами довіреної третьої сторони, такої як юридична фірма, арбітражна установа, нотаріус або суд.

Інший спосіб, щоб вивчити і допитати свідка - це використання письмового синхронного онлайн форуму, такого як онлайн-чат. Це дозволяє сторонам спілкуватися в режимі реального часу, писати і відповідати на питання. Звичайно, набагато важче оцінити достовірність таких свідчень, що не є реальною альтернативою усним свідченням (і візуальним).

Крім того, цікавий онлайн метод є використання мультимедійних стенограм під час особистих слухань, що дозволяє учасникам не тільки одночасно чути докази, а й бачити занотовані матеріали справи на екрані перед собою. Ідея полягає в тому, що це покращує уявлення про докази і робить їх зрозумілішими. Стенограми можна шукати і бачити на екрані. Крім того, можна підключитись до заслуховування віддаленим зв’язком.

Найбільш очевидним онлайн методом арбітражу є використання електронної пошти для спілкування і обміну документами між сторонами, арбітрами та адміністраторами. Очевидно, що електронна пошта є більш зручним і більш швидким способом, ніж традиційні листи або факси. З метою документування, електронна пошта згодом може супроводжуватися роздруківками. З іншого боку, повідомлення електронної пошти, відправлені через Інтернет є незахищеними, і з цієї причини особливі запобіжні заходи повинні бути прийняті.

Один надзвичайно корисним онлайн методом арбітражу є електронне управління файлами, особливо для складних, великомасштабних арбітражів.

Електронне управління файлами означає, що всі документи, що мають відношення до даної справи, зберігаються в електронному вигляді в систематичному порядку. Електронне програмне забезпечення для управління файлами дозволяє легко відновлювати окремі документи або паки, роздруковувати, робити перехресні посилання, порівнювати, шукати за ключовими словами. Електронне управління файлами скорочує час, що витрачається на пошук документів і виключає використання великої кількості паперу. Система перехресних посилань дозволяє «підв’язувати» текст, наприклад, в судових дебатах, для доказу. Електронне управління файлами вже широко використовується на практиці. Зазвичай сторони обмінюються електронними документами на Сй-дисках, що дозволяє (майже) повністю уникнути використання паперу. Слід зазначити, що існують деякі обмеження. Деякі рукописні документи не можуть бути перетворені в електронний формат (скануватися). Крім того, технологія сканування або оптичного розпізнавання символів (ОРС) точна на 99,3% і, отже, не є досконалою. Крім того, слід мати на увазі, що в той час як є деякі гарантії, що забезпечують цілісність відсканованих версій документів, немає ніякої гарантії (від випадкових або навмисних) змін. Нарешті, учасникам процесу все ж легше читати документи на папері, ніж з екрану.

**Основні принципи онлайн правосуддя**. Деякі з цих ініціатив належать уряду, інші були прийняті асоціаціями споживачів, ділових ооганізацій та професійних організацій.

**Прозорість** охоплення інформації, наданої процесуальних норм(правил процедури, регламенту) також особливо важливо при роботі зі споживачами.

**Доступність** також має важливе значення в контексті взаємодії зі споживачами, що включає в себе відсутність витрат на перешкоди доступу.

**Незалежність** - це традиційна необхідна умова і стосується питання фінансування в онлайновому контексті.

**Своєчасність** -швидкість є ще одним з головних переваг ВСО, особливо враховуючи повільність традиційних судових розглядів та строки розгляду судових справ.

**Чесність** - з незалежністю становить фундамент процесуальних гарантій. З цих п’яти принципів, принципи справедливості і незалежності, заслуговують більшої уваги, як і питання контролю якості. Чесності повинні дотримуватися незалежно від методу вирішення спорів, що обрали сторони.

**6. Регулювання спорів онлайн.**

На відміну від посередництва і переговорів, при здійсненні арбітражу потрібно виконувати обов’язкові вимоги, при виконанні деяких з них в онлайн середовищі можуть виникати труднощі.

Особливо це стосується прийнятності, вимоги письмової форми і включення арбітражної угоди шляхом посилання на неї. По-перше, арбітраж повинен бути прийнятним.

Споживчі суперечки підлягають розгляду в арбітражному порядку в рамках доктрини. Однак, їх підсудність (арбітрабельність) може стати предметом обмеження (обмежуватись). Існують загальні обмеження дійсності арбітражних угод, укладених до виникнення спору.

Відповідно до Директиви ЄС щодо несправедливих умов споживчих договорів, несправедливі положення у споживчих договорах не є обов’язковими до виконання споживачами.

У справі Осеано проти Росио Мурчиано Кинтеро (Oceano v. Rocio Murciano Quintero), Європейський Суд застосуваз це положення до вибору позасудового порядку і визнав дане застереження несправедливим «оскільки викликає... значний дисбаланс (нерівноправність) в правах і зобов’язаннях сторін, що випливають з договору, і надання переваги продавцю. Той же самий висновок, безумовно, може бути застосований до арбітражних застережень, в тому числі положень, що передбачають проведення арбітражу в режимі онлайн. Якщо онлайн процедура арбітражу є недорогою і не вимагає особливих навичок роботи з комп’ютером, немає жодних причин, чому це повинно викликати дисбаланс (нерівноправність) і наносити шкоду споживачу. Зовсім навпаки, правосуддя таким чином стає більш доступним для споживача. У державах-членах ЄС, у національному законодавстві країн-членів можуть додатково бути передбачені обмеження щодо здійснення споживчого арбітражу.

**7. Вирішення спорів онлайн і виконання.**

У Франції до спорів споживачів щодо побутових (сімейних) справ арбітражні застереження є недійсними (не застосовуються). У міжнародному арбітражі, однак, дійсність даних застережень заперечується (обговорюється). Касаційний суд Франції в двох випадках ухвалив, що укладення арбітражної угоди до спору споживача - дійсне відповідно до міжнародних договорів, оскільки законодавство Франції про захист прав споживачів щодо юрисдикції (Цивільний кодекс Франції, ст. 2061 і Кодекс про захист прав споживачів Франції, ст. L. 132 (2 )) не застосовується до міжнародних випадків.

Ці рішення зазнали критики з боку французьких коментаторів, що стверджували, що споживачі заслуговують такого ж захисту в міжнародних і національних спорах. У Сполучених Штатах, як правило, набагато більше використовують споживчий арбітраж, нещодавні рішення виявили «надмірні витрати за встановлення наявності критеріїв». У деяких випадках у якості захисту у суді (заперечення на позов) в контракті виявляють незаконність (недобросовісність), що спричинює анулювання арбітражного застереження в договорі про приєднання (типовому контракті). Для уникнення цієї ситуації арбітражні застереження до виникнення спору включають в загальні умови договору і можуть, зокрема, вважатися недобросовісними виключно, якщо вони накладають надмірні витрати на споживача, що не дозволяє йому або їй їх зменшити. Наприклад, у справі Green Tree Financial Согр. проти Рендольфа, Верховний суд постановив, що надмірно висока вартість може виправдати недійсність арбітражної угоди до виникнення спору, але позивач не повинен доводити ймовірність (можливість виникнення) понесення таких витрат.

15 лютого 2016 року Європейська комісія запустила нову платформу, щоб допомогти споживачам і торговцям вирішити онлайн спори з приводу придбання товарів в режимі онлайн (через мережу Інтернет). Платформа з Вирішення спорів онлайн пропонує єдину точку входу, що дозволяє споживачам і торговцям ЄС врегулювати свої суперечки в обох випадках при здійсненні внутрішніх і транскордонних покупок. Це робиться шляхом направлення спорів до національних органів з Альтернативного вирішення спорів (ABC), що підключені до платформи і обрані державами-членами відповідно до критеріїв якості і повідомлені Комісії.

**8. Вирішення спорів онлайн і світовий ринок.**

У справі Cole V. Burns International Security Services, Апеляційний суд в окрузі Колумбія встановив, що витрати на арбітраж дійсно були непомірно високими, і вирішив, що їх повинен сплатити виключно роботодавець. У справі Gutierrez v. Autowest, Каліфорнійський апеляційний суд встановив, що "споживачі можуть оскаржити арбітражне застереження до суперечки, як недобросовісне (непомірне), якщо плата за початок процесу розгляду справи вимагається занадто висока, і угода не може надати споживачеві реальну можливість вимагати звільнення від сплати збору. На підставі того ж висновку щодо витрат, Дев’ятий окружний апеляційний суд прийняв рішення у справі, Ting v. AT&T, що арбітражні застереження - недобросовісні, аргументуючи це тим, що вони не дозволили споживачам подати позови вдержаві, де передбачено таке їх право.

Значною перевагою онлайн спорів є те, що відстаней у них не існує (скасовуються). Спір вирішується таким же чином, як і укладено контракт, і виконується шляхом завантаження програмного забезпечення. Як правило, ефективним методом вирішення спорів є той, який має концептуальну схожість з діяльністю, що спричинила виникнення спору. Це, однак, ширша тема, що простягається далеко за межі ВСО. Що стосується стурбованості щодо забезпечення справедливого онлайн правосуддя у випадку, якщо компетентний суд знаходиться далеко від будинку заявника, ВСО гарантуватиме доступ до правосуддя, яке за звичайних умов не могло бути здійсненим. Тим більш це необхідно, тому що люди в мережі Інтернеті і підприємства, чиї шляхи ніколи б не перетинались в сучасному світі (не онлайн мережі) зараз мають змогу укладати договори один з одним.

Перевага ВСО полягає в подоланні географічних (обмежень) кордонів, поки не доходить до дотримання результатів процедури ВСО. Якщо результатом є обов’язкове до виконання рішення арбітра, сторона, що отримала перемогу повинна подати заяву на отримання екзекватури, можливо, навіть на іншому боці земної кулі, так як онлайн виконати рішення на даний момент ще неможливо. Якщо в результаті вирішення спору, рішення не виконується, то ситуація стає більш проблематичною, оскільки кредитор повинен подати новий судовий позов, а не просто відкрити виконавче провадження. Це навряд чи задовольнить кредитора.

ЄС розглянув це питання в «Директиві ЄС про електронну комерцію» (98/0325 (COD)). Перша частина статті 17 Директиви говорить: "Держави-члени повинні забезпечити, щоб у разі виникнення розбіжностей між постачальником послуг інформаційного суспільства та одержувачем послуг, їх законодавство не перешкоджало використанню позасудових механізмів для врегулювання суперечок, що відповідають національному законодавству, включаючи відповідні електронні засоби. У березні 2000 року у Брюсселі проведено семінар-практикум ЄС щодо позасудової системи врегулювання суперечок у сфері електронної торгівлі. У звіті даного семінару-практикуму розглянуто також онлайн варіанти врегулювання спорів в середовищі електронної комерції.

**Лекція № 5**

Тема лекції: Міжнародні правові аспекти боротьби із кіберзлочинністю

**План лекції**

1. Огляд. Вступ до поняття кіберзлочинності.

2. Підходи до регулювання.

3. Історія боротьби із кіберзлочинністю.

4. Основні міжнародні інструменти боротьби із кіберзлочинністю.

5. Основні міжнародні міжурядові організації в боротьбі з кіберзлочинністю.

6. Женевські домовленості щодо правового регулювання кіберзлочинів.

7. Додаткові джерела регулювання кіберзлочинності.

8. Взаємна допомога у розслідуванні кіберзлочинів.

9. Європейська Судова Мережа з Кіберзлочинності та Євроюст.

10. Захист прав дітей онлайн – завдання та дії.

11. Блокування, фільтрування та видалення незаконного контенту в Інтернеті.

12. Електронні докази.

**Література**

* + 1. Закон України «Про інформацію» від 02.10.1992 року // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.
    2. Марущак А.І. Інформаційне право України. Підручник / Марущак А.І. – К.: Дакор, 2011. – 456 с.
    3. Сопілко І. М. Державна інформаційна політика України: стан та шляхи реалізації: монографія / І. М. Сопілко. – К. : МП «Леся», 2014. – 424 с.
    4. B.C.Цимбалюк Основи інформаційного права України / B.C.Цимбалюк, В.Д.Гавловський, В.В.Гриценко та ін. – К.: Видавництво "Знання", 2004
    5. Загальна декларація прав людини 1948 року // Голос України, 2008. – № 236.
    6. Конвенція про захист прав людини і основоположних свобод 1950 року // Голос України, 2001. – № 3.
    7. Конвенція про кіберзлочинність від 23 листопада 2001 року // Офіційний вісник України, 2007. – № 65.
    8. Резолюція 60/45, прийнята Еенеральною Асамблеєю Організації Об’єднаних Націй, «Досягнення у галузі інформатизації та телекомунікацій в контексті міжнародної безпеки» від 08.12.2005 р. – Електронний ресурс. – Режим доступу: <http://zakonl.rada.gov.ua/laws/show/995_e45>

**Зміст лекції**

**1. Огляд. Вступ до поняття кіберзлочинності.**

Сучасні інформаційно-комунікаційні технології запроваджуються і розвиваються набагато швидше, ніж законодавчі та правоохоронні органи можуть адекватно реагувати на їх збільшення.

Одне з найбільш критичних зауважень до визначення комп'ютерного злочину, зроблене Міністерством юстиції СІІІА (РСи), є його надмірно широка концепція. DOJ визначає комп’ютерний злочин як "будь-яке порушення кримінального закону, із залученням знання комп'ютерної техніки для його здійснення, дослідження або розслідування. За таким визначенням, практично будь-який злочин може бути класифікований як комп'ютерний злочини, просто тому, що детектив використовував комп'ютерну базу даних в рамках проведення розслідування”.

Одним з факторів, які роблять повноцінне визначення кіберзлочинності складним є юрисдикційна дилема. Закони в різних юрисдикціях визначають терміни по-різному, і для співробітників правоохоронних органів, які розслідують злочини, а також мережевих адміністраторів, які хочуть брати участь в переслідуванні кіберзлочинності, які відбуваються стосовно комп’ютерних мереж, важливо ознайомитися з чинним законодавством.

Крім того, однією з основних проблем, пов'язаних з адекватним визначенням кіберзлочинності є відсутність конкретних статистичних даних про ці злочини. Фактично, повідомлення про скоєння злочину є диспозитивним. Це означає, що наявні цифри майже напевно набагато нижчі за фактичний рівень виникнення мережевих злочинів.

У багатьох випадках злочини, що законодавці назвали б кіберзлочинами, це ті ж звичайні злочини, за винятком того, що якимось чином задіяна комп'ютерна мережа. Комп'ютерна мережа дає злочинцям новий спосіб вчиняти ті ж самі злочини. Існуючі законодавчі акти, які забороняють ці дії, можуть бути застосовані до людей, які використовують комп'ютер для їх здійснення, а також до тих, хто комп’ютер не використовував.

В інших випадках, злочин є унікальним і почав існувати з появою мережі. Злам комп'ютерної системи є прикладом; в той час як це може бути пов'язано із незаконним проникненням в будинок або офісний будинок, елементи, з яких складається несанкціонований доступ до комп'ютерів і фізичного злому і проникнення - різні.

Законодавство більшості штатів СІІІА мають посилання на комп'ютерну злочинність. Ці законодавчі акти, як правило, застосовуються державними органами та місцевою поліцією, і можуть містити свої власні визначення термінів. Секція комп'ютерної злочинності Кримінального кодексу Техасу, визначає тільки один злочин - Порушення комп’ютерної безпеки - як '(а) особа вчиняє злочин, якщо свідомо отримує доступ до комп'ютерної, комп'ютерної мережі або комп'ютерній системі без явної згоди власника.

Кримінальний кодекс Каліфорнії, з іншого боку, визначає список з восьми актів, що представляють собою комп'ютерний злочин, включаючи зміну, пошкодження, видалення, або іншим чином використання комп'ютерних даних для виконання схеми, з метою введення в оману, вимоги про контроль або неправомірного контролю або отримання грошей, майна або даних, використовуючи комп'ютерні послуги без дозволу, порушуючи комп'ютерні послуги, надаючи допомогу іншим в незаконному доступі до комп'ютера, або введення вірусів у систему або мережу. Таким чином, визначення кіберзлочинності відповідно до законів відрізняється, в залежності від штату.

**Кіберзлочинність в вузькому сенсі:** Будь-яке незаконне поводження, здійснюване за допомогою електронних операцій, що ставить під загрозу безпеку комп'ютерних систем іданих, оброблених ними.

**Кіберзлочинність в широкому сенсі:** Будь-яке незаконне поводження, здійснюване за допомогою або відносно комп'ютерної системи або мережі, в тому числі такі злочини, як незаконне зберігання та розміщення інформації за допомогою комп'ютерної системи або мережі».

Ці визначення, хоча і не є повністю остаточними, дають хорошу відправну точку - і щодо яких наявне певне міжнародне визнання та узгодження - для визначення тільки того, що ми маємо на увазі під терміном кіберзлочинність. Кіберзлочинність за цими визначеннями включає участь комп'ютерів і мереж. У боротьбі з кіберзлочинністю, компонент “кібер" зазвичай відноситься до вчинення якісно нових видів злочинів, які з'являються з розвитком інформаційних технологій та інтеграції кіберпростору в більш традиційні види діяльності.

**Кіберзлочин** часто визначають, як будь-яку форму кримінальної діяльності, в якій задіяні комп’ютери або мережі. Також називають комп’ютерні злочини, електронні злочини, е-злочини, мережеві злочини, хай-тек злочини.

Визначення за Electronic Communications and Transactions Amendment Bill, 2012 у ПАР (26 жовтня 2012): **Кіберзлочин** - будь-який кримінальний або інший злочин, що був виконаний за допомогою або за участі використання електронних комунікацій або інформаційних систем, включаючи будь-який пристрій або Інтернет, їх разом або інші предмети.

Dictionary.com: Кримінальна діяльність або злочин, у яких використовується Інтернет, комп’ютерна система або комп’ютерні технології.

Encyclopaedia Britannica: Кіберзлочин - комп’ютерний злочин, використання комп’ютера як засіб для незаконних дій.

Кіберзлочинність стосується не лише якої-небудь злочинної діяльності, в якій комп'ютер або мережа грає ключову роль, а й до незаконної діяльності у інших злочинах - в яких злочинець використовує Інтернет або по електронну пошту за допомогою комп'ютера.

**Термін «кіберзлочинність»** часто вживається поряд з терміном «комп`ютерна злочинність», причому нерідко ці поняття використовуються як синоніми. Дійсно, ці терміни дуже близькі один одному, але все-таки, не синонімічні. Поняття «кіберзлочинність» (в англомовному варіанті – cybercrime) ширше, ніж «комп`ютерна злочинність» (computer crime), і більш точно відображає природу такого явища, як злочинність в інформаційному просторі.

Так, Оксфордський тлумачний словник визначає приставку «cyber» як компонент складного слова. Її значення – що відноситься до інформаційних технологій, мережі Інтернет, віртуальної реальності. Практично таке ж визначення дає Кембриджський словник. Таким чином, «cybercrime» – це злочинність, пов`язана як із використанням комп`ютерів, так і з використанням інформаційних технологій і глобальних мереж. У той же час термін «computer crime» в основному стосується злочинів, які скоєні щодо комп’ютерів або комп’ютерних даних. Ідея поділу термінів «кіберзлочинність» і «комп`ютерна злочинність» й використанню саме першого терміну і закріплена в міжнародному праві. Рада Європи в листопаді 2001 року прийняла Конвенцію про кіберзлочинність, вживши саме термін «cybercrime», а не «computer crime» . В даний же час офіційне визначення кіберзлочинності на міжнародному рівні відсутнє.

Хоча аналіз національного законодавства України, що регулює суспільні інформаційні відносини, дозволяє стверджувати, що наша держава вживає необхідних заходів, спрямованих на профілактику та протидію комп’ютерної злочинності. Прикладом цьому може служити Указ Президента від 31 липня 2000 року «Про заходи розвитку національної складової глобальної інформаційної мережі Internet та забезпечення широкого доступу до цієї мережі в Україні», а також Розділ 16 «Злочини у сфері використання ЕОМ, систем та комп’ютерних мереж» чинного Кримінального кодексу України. Але цього виявляється не достатньо для повного подолання кіберзлочинності в нашій країні.

Тому, однією з проблем, на яких доцільно акцентувати увагу є проблема понятійно-категорійного апарату. Термін «кіберзлочин», яким зараз у наукових колах прийнято позначати специфічні види злочинів, віднесених до так званої «кібернетичної сфери» набув на пострадянському просторі достатньо широкого вжитку, не маючи сформованого загальновизнаного юридичного наповнення. Залишається не вирішеною проблема не тільки встановлення співвідношення «кіберзлочину» з такими правовими категоріями як «комп’ютерний злочин», «злочин у сфері комп’ютерної інформації», «злочин у сфері використання комп’ютерів», «злочин у сфері використання інформаційних технологій», або із законодавчим в Україні поняттям «злочин у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку», а й концептуального визначення місця «кіберзлочину» в системі протиправних діянь передбачених національним законодавством: як окремого виду цих діянь, як специфічної форми їх скоєння, як того і іншого.

Конвенція «Про кіберзлочинність» також не дає визначення поняття «кіберзлочинність». Водночас в її преамбулі зазначено, що Конвенція є необхідною для зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп’ютерних систем, мереж і комп’ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, необхідною для зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп’ютерних систем, мереж і комп’ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, як це описано у Конвенції, надання повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню, як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого і надійного міжнародного співробітництва .

Отже в цьому контексті кіберзлочинність – це дії, а саме: незаконний доступ; нелегальне перехоплення; втручання у дані або у систему; зловживання пристроям; шахрайство; правопорушення, пов’язані з дитячою порнографією; порушення авторських і суміжних прав; правопорушення, спрямовані проти конфіденційності, цілісності і доступності комп’ютерних систем, мереж і комп’ютерних даних, а також зловживання такими системами, мережами і даними, що тягнуть кримінальну відповідальність.

Резюмуючи вищезазначене, акцентую увагу на тому, що, перш за все, засобом для здійснення кіберзлочину є комп’ютер, а саме комп’ютерні мережі чи комп’ютерні системи. З кримінально-правової точки зору він характеризується прямим умислом, майже виключається можливість недбалості. Також суб’єктом виступає осудна фізична особа. Даний вид злочину спрямований на порушення діяльності інформаційних та комп’ютерних систем, порушення авторських і суміжних прав, незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення та ін.

Наслідки кіберзлочинності зачіпають не лише інтереси окремих осіб, що стали жертвами, але й компанії, організації, уряди і суспільство в цілому. Кіберзлочини найчастіше ставлять під загрозу життєво важливу як інформаційну, так і взагалі критичну інфраструктуру, яка в багатьох країнах не контролюється публічним сектором, і такі злочини можуть вчиняти дестабілізуючий вплив на всі верстви суспільства. Таким чином стверджую: кіберзлочинність виступає загрозою національній безпеці в кібернетичній сфері.

Проаналізувавши теоретичні та практичні дослідження в галузі визначення поняття кіберзлочину, можна висновувати, що серед сучасних українських науковців немає єдиного підходу до визначення поняття кіберзлочину. Причому підходи досить суттєво відрізняються, що може бути причиною неправильного трактування, а це у свою чергу може призвести до неправильної кваліфікацію злочинних дій, що створить проблеми не тільки на теоретичному, а й на практичному рівнях.

Кіберзлочини поділяють на види залежно від об`єкта, від предмета посягання, залежно від способів скоєння і т. п.

Найбільш поширена класифікація кіберзлочинів в даний час ґрунтується на структурі Конвенції Ради Європи про кіберзлочинність. Ця класифікація в даний час виступає «еталоном», оскільки наявні міжнародні та регіональні документи, а також наукова практика, використовують саме цей поділ.

1) правопорушення проти конфіденційності, цілісності та доступності комп’ютерних даних і систем: незаконний доступ — навмисний доступ до цілої комп’ютерної системи або її частини без права на це з метою отримання комп’ютерних даних або втручання в дані, навмисне пошкодження, знищення, погіршення, зміну або приховування комп’ютерної інформації без права на це; втручання в систему – навмисне серйозне перешкоджання функціонуванню комп’ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, заміни або приховування комп’ютерних даних без права на це; зловживання пристроями, а саме їх виготовлення, продаж, придбання для використання, розповсюдження або надання для використання іншим чином;

2) правопорушення, пов’язані з комп’ютерами;

3) правопорушення, пов’язані зі змістом;

4) правопорушення, пов’язані з порушенням авторських та суміжних прав;

5) акти расизму та ксенофобії, вчинені за допомогою комп`ютерних мереж.

 Серед основних видів кіберзлочинності виділяють поширення шкідливих програм, злам паролів, крадіжку номерів кредитних карт і інших банківських реквізитів, а також поширення протиправної інформації через Інтернет.

За об’єктом посягання виділяються наступні групи кіберзлочинів: злочини проти конфіденційності, цілісності та доступності комп`ютерних даних і комп`ютерних мереж, економічні комп`ютерні злочини, комп`ютерні злочини проти особистих прав і недоторканності приватної сфери, комп`ютерні злочини проти суспільних і державних інтересів. Проте, варто відзначити, що багато кіберзлочинів зазіхають відразу на декілька об`єктів. Ще одна категорія злочинів, не включена окремо в Конвенцію Ради Європи (і отримала поширення після прийняття Конвенції) – identity theft, крадіжка, передача і використання персональних даних з метою вчинення злочинів .

На сьогодні досить розповсюдженою є класифікація кіберзлочинів на:

1) агресивні — кібертероризм, погроза фізичної розправи (наприклад, передана через електронну пошту), кіберпереслідування, кіберсталкінг (протиправне сексуальне домагання та переслідування іншої особи через Інтернет), дитяча порнографія (створення порнографічних матеріалів, виготовлених із зображенням дітей, розповсюдження цих матеріалів, отримання доступу до них);

2) неагресивні — кіберкрадіжка, кібервандалізм, кібершахрайство, кібершпигунство, розповсюдження спаму та вірусних програм.

У той же час, з урахуванням мотивації злочинців, кіберзлочини представляється можливим умовно розділити на наступні категорії: кібершахрайство з метою заволодіння коштами; кібершахрайство з метою заволодіння інформацією (для власного користування або для подальшого продажу); втручання в роботу інформаційних систем з метою отримання доступу до автоматизованих систем управління (для навмисного пошкодження за винагороду або для нанесення шкоди конкурентам); інші злочини.

**Найпоширенішими видами таких злочинів** є:

**Кардинг**– використання в операціях реквізитів платіжних карт, отриманих зі зламаних серверів інтернет-магазинів, платіжних і розрахункових систем, а також із персональних комп'ютерів (або безпосередньо, або через програми віддаленого доступу, «трояни», «боти»).

**Фішинг**– вид шахрайства, відповідно до якого клієнтам платіжних систем надсилають повідомлення електронною поштою нібито від адміністрації або служби безпеки цієї системи з проханням вказати свої рахунки та паролі.

**Вішинг –** вид кіберзлочинів, у якому в повідомленнях міститься прохання зателефонувати на певний міський номер, а при розмові запитуються конфіденційні дані власника картки.

**Онлайн-шахрайство –** несправжні інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку.

**Піратство –** незаконне розповсюдження інтелектуальної власності в Інтернеті.

**Кард-шарінг**– надання незаконного доступу до перегляду супутникового та кабельного TV.

**Соціальна інженерія –** технологія управління людьми в Інтернет-просторі.

(Соціа́льна інженерія — це наука, що вивчає людську поведінку та фактори, які на неї впливають. Нині її часто використовують для маніпуляції з метою спонукати людину виконати певні дії чи розголосити конфіденційну інформацію.

Основною метою соціальної інженерії є: дослідження причин тої чи іншої поведінки людини; обставин та середовища, що впливають на формування системи цінностей індивіду, і як наслідок - їх поведінки.

На базі цих досліджень можна визначити, що саме спонукає людину на конкретну дію.

Наприклад: вивчення середовища, в якому жив вбивця, допоможе зрозуміти його систему цінностей. Ця інформація надасть можливість розробити соціальну структуру, в якій будуть формуватись інші системи цінностей. Системи цінностей, у яких насамперед буде цінуватись людське життя та індивідуальність.

Термін «соціальна інженерія» як акт психологічної маніпуляції також пов'язують із суспільними науками, однак він широко використовується серед спеціалістів з [комп'ютерної](https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0) та [інформаційної 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).

- С[оціальна інженерія (безпека)](https://uk.wikipedia.org/wiki/%D0%A1%D0%BE%D1%86%D1%96%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0_%D1%96%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D1%96%D1%8F_(%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0)) — злочинне вивідування даних.

- [Соціальна інженерія (соціологія)](https://uk.wikipedia.org/wiki/%D0%A1%D0%BE%D1%86%D1%96%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0_%D1%96%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D1%96%D1%8F_(%D1%81%D0%BE%D1%86%D1%96%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%8F)) — технологічний напрям соціології, що ґрунтується на критичному і дієвому ставленні до процесів [соціальних змін](https://uk.wikipedia.org/wiki/%D0%A1%D0%BE%D1%86%D1%96%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0_%D0%B7%D0%BC%D1%96%D0%BD%D0%B0) у суспільстві.

- Соціальна інженерія (від франц. ingenieur – винахідний, мистецький) – термін, що приміняється в соціології по відношенню до тієї галузі прикладної соціології, завдання якої вбачається у розробці і використанні засобів впливу на поведінку і установки людей, з метою розв’язання гострих соціальних проблем, адаптації соціальних інститутів до умов що змінюються і збереження соціальної стабільності.

**Мальваре –** створення та розповсюдження вірусів і шкідливого програмного забезпечення.

**Протиправний контент –** контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства.

**Рефайлінг**– незаконна підміна телефонного трафіку.

**2. Підходи до регулювання.** Глобальний інформаційний простір, інформаційна мегасреда нематеріальні і по суті своїй несвідомих до фізичного носія, в якому втілені. Тому термін «комп`ютерна злочинність» все-таки декілька вже за своїм смисловим навантаженням, і зводить суть явища до злочинів, скоєних за допомогою комп`ютера. У теперішній же час з розвитком інформаційних технологій вже саме поняття «комп`ютер» стає розмитим. Наприклад, сьогодні практично всі мобільні телефони мають доступ в мережу Інтернет. З розвитком 3G мереж мобільні телефони здатні підключатися до глобальної мережі за технологією HSPDA (мережа четвертого покоління) або UMTS (мережа третього покоління), що за швидкістю ненабагато поступається можливостям підключення до мережі Інтернет за допомогою звичайного комп`ютера, а в перспективі і перевищує їх.

У 2013 р. Управління ООН з наркотиків і злочинності в опублікованому звіті «Всебічне дослідження проблеми кіберзлочинності та відповідь заходів з боку держав - членів, міжнародного співтовариства і приватного сектора» відзначає, що поняття «кіберзлочинність» залежить від контексту і мети вживання цього терміна. При цьому, як наголошується в тому ж документі, що хоча основне "ядро" цього терміна представляють злочини проти конфіденційності, цілісності та доступності даних, крім цього досить обмеженого списку комп`ютерних злочинів, в поняття «кіберзлочинність» включаються будь-які дії, спрямовані на нелегальне вилучення прибутку, контент-злочини, та інші протизаконні діяння в кіберпросторі. При цьому, як відзначають автори звіту, у створенні якогось універсального визначення кіберзлочинності немає необхідності, так як, наприклад, з метою міжнародного співробітництва в розслідуванні злочинів набагато важливіше гармонізувати норми, що відносяться до збору та поданням електронних доказів. Ця необхідність не обмежується якимось штучним терміном «кіберзлочинів», оскільки на електронних носіях і в електронних комунікаціях може міститися інформація, що відноситься до будь-якого виду злочинів, скоєних як у кіберпросторі, так і поза ним.

В Україні до кіберзлочинів відносять порушення авторського права і суміжних прав, шахрайство, незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення; ухилення від сплати податків, зборів (обов’язкових платежів), ввезення, виготовлення, збут і розповсюдження порнографічних предметів, незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю.

Терміни, які вживаються в Конвенції та додатковому протоколі до неї, так і не знайшли свого визначення у вітчизняному законодавстві. Так, у Законі України «Про основи національної безпеки України» згадуються терміни «комп’ютерна злочинність» та «комп’ютерний тероризм», проте закон не дає визначення цим поняттям, також ці визначення відсутні в інших нормативних актах. Не визначено й поняття «комп’ютерний тероризм» (кібертероризм) у Законі України «Про боротьбу з тероризмом», а питання, які можуть охоплюватися цим поняттям, частково викладені як складова поняття «технологічний тероризм”.

Слід зазначити, що в «Доктрині інформаційної безпеки України» згадувалися поняття «комп’ютерна злочинність» та «комп’ютерний тероризм», а також питання захисту інформації від «кібернетичних атак». Проте в жодному із перелічених актів так і не було відображено визначення цих понять.

Відзначу, що частина цих деліктів передбачена в якості злочинів в КК України у Розділі XVІ «Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку». Поряд з цим, суспільні відносини в даній сфері регулюються низкою підзаконних нормативно-правових актів.

В Указі Президента України Про рішення Ради національної безпеки і оборони України від 4 березня 2016 р. «Про Концепцію розвитку сектору безпеки і оборони України» від 14 березня 2016 р. неодноразово вживаються поняття «кіберзлочин», «кіберзлочинність», «кіберзагроза», «кібербезпека», «кібершпигунство» та інші, однак не дається визначення жодному з цих понять.

4 червня 2013 року був зареєстрований проект закону «Про кібернетичну безпеку України», однак в ньому також не міститься визначення поняття «кіберзлочинність» чи «кіберзлочин». Пізніше, у проекті закону «Про основні засади забезпечення кібербезпеки України» № 2126а, зареєстрованому 19.06.2015 р., під кіберзлочином визначають суспільно небезпечне винне діяння у кіберпросторі, передбачене законодавством України про кримінальну відповідальність, а під кіберзлочинністю — сукупність кіберзлочинів. Нині питання кіберзлочинності є надзвичайно актуальним на державному рівні. Найчастіше кіберзлочини посягають на об’єкти критичної інфраструктури, в тому числі і інформаційної інфраструктури: енергетичні об’єкти, транспорт та банківський сектор. Таким чином, протидія та попередження кіберзлочинності та рівень кібербезпеки на сьогодні є одним із найпріоритетніших напрямків в політиці нашої держави. Але для комплексної боротьби з цією проблемою необхідними є спільні зусилля держави, громадян та міжнародної спільноти в цілому.

На сьогоднішній день в Україні діє низка Законів України та нормативних документів різних рівнів, що охоплюють проблеми забезпечення кібербезпеки держави. Водночас спостерігається вільне використання значної кількості термінів (та їх синонімів) що часто не узгоджені між собою. Так у Законі України «Про основи національної безпеки України» згадуються «комп’ютерна злочинність» та «комп’ютерний тероризм», при чому жоден з цих термінів на має свого визначення а ні в цьому, а ні в інших нормативних документах. В Законі України «Про боротьбу з тероризмом» поняття «комп’ютерний тероризм» не згадується взагалі, а ті елементи, що можуть до нього відноситись прописані як складова частина поняття «технологічний тероризм». У «Стратегії національної безпеки України» (в редакції від 12 лютого 2007 року № 105/2007) комп’ютерні загрози не згадуються, а «кібербезпека» - лише в контексті необхідності «розробки та впровадження національних стандартів та технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих з відповідними європейськими стандартами, у тому числі згідно з вимогами ратифікованої Верховною Радою України Конвенції про кіберзлочинність». Однак нова оприлюднена редакція «Стратегії національної безпеки» (2011 року) вже використовує термін «кібербезпека». В «Доктрині інформаційної безпеки України» також згадуються «комп'ютерна злочинність» та «комп'ютерний тероризм», знову ж таки – без жодних пояснень чи посилання на такі пояснення. Крім того, в Доктрині згадуються і «кібератаки» без визначення терміну. Отже можна констатувати, що в більшості своїй вітчизняне нормативно-правове поле в сфері інформаційної (кібернетичної) безпеки оперує термінами визначень яких фактично немає. Національним інститутом стратегічних досліджень було спрямовано низку офіційних запитів до ключових відомств (Служба безпеки України, Служба зовнішньої розвідки, Головне управління розвідки Міністерства оборони України, Міністерство внутрішніх справ) та наукових установ (Інститут телекомунікацій і глобального інформаційного простору Національної академії наук України, Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю Ради національної безпеки і оборони України), що мають відношення до інформаційної (в тому числі – технологічної компоненти) безпеки держави з метою визначення підходів до основних термінів в даній сфері.

Законом України «Про Державну службу спеціального зв’язку та захисту інформації України» на ДССЗЗІ покладено функцію участі у «формуванні та реалізація державної політики у сфері захисту державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації». Обмеженість суто захистом (технічним) державних інформаційних ресурсів не відповідає сучасним тенденціям в сфері боротьби із кіберзлочинністю, що потребує додаткового розширення зон уваги правоохоронних органів в тому числі на приватні комп’ютерні мережі та окремі ПК. Крім того, ДССЗЗІ не має повноважень проводити оперативно-розшукову діяльність, чим займаються профільні відділи, управління та департаменти СБУ та МВС України. Діяльність цих трьох відомств у сфері боротьби із кіберзлочинністю є ключовою. Інтернаціональний характер загроз цілком може змусити долучати до такої діяльності та інші відомства, що можуть відноситись до військової організації держави – Головне управління розвідки Міністерства оборони України та Служба зовнішньої розвідки. Частково з метою вирішення цих проблем та невпорядкованості нормативно-правового поля державними безпековими інституціями проводиться цілий ряд заходів. Основою для них стало рішення Ради національної безпеки і оборони України від 17 листопада 2010 року «Про виклики та загрози національній безпеці України у 2011 році», яке затверджено Указом Президента України від 10 грудня 2010 року № 1119/2010. Відповідно до даного Указу в Україні має бути створена Єдина загальнодержавна система протидії кіберзлочинності. Проміжним результатом згаданого Указу є рішення першого віце-прем’єр-міністра України Клюєва А.П. від 2 лютого 2011 року щодо необхідності підготовки законопроекту про кібернетичну безпеку України.

Проблема профілактики кіберзлочинності в Україні — це комплексна проблема. Сьогодні закони мають відповідати сучасним реаліям, а не рівню розвитку чи то науки, чи то розуміння правлячої групи щодо пріоритетності тих чи інших національних інтересів. Розвиток технологій, кіборгізація та подальше впровадження штучного інтелекту в наше життя це вже не майбутнє, а сьогодення. Тому будь-які подальші рефлексії з цього питання лишень затягуватимуть час тоді, коли відносини у кіберпросторі розвиваються швидкоплинно і нелінійно.

Пріоритетним напрямком є також організація взаємодії і координація зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх не лише найсучаснішою матеріально-технічною базою, а й розвиток акмеологічних засад кібербезпекової освіти, підготовка відповідних фахівців. Жодна держава сьогодні не в змозі самотужки протистояти кіберзлочинності самостійно. Нагальною є необхідність активізації участі України в інтересах національної безпеки в різноманітних системах міжнародної та глобальної інформаційної безпеки, посилення співпраці з всесвітніми інформаційними гігантами: Facebook, Apple, Google із залученням широкого кола аналітичних центрів, в тому числі недержавних та інститутів громадянського суспільства.

Експерти впевнені: саме хакери в недалекому майбутньому стануть загрозою номер один, змістивши тероризм. Незважаючи на віртуальність злочинів, безпосередню шкоду вони завдають в реальному світі. Яскравим прикладом стала масштабна атака вірусу Petya на українські ресурси, виведення з ладу чисельних інформаційних систем органів державної влади України.

**3. Історія боротьби із кіберзлочинністю.**

З 1985 по 1989 р. Спеціальний Комітет експертів Ради Європи з питань злочинності, пов'язаної з комп'ютерами, виробив Рекомендацію № 89, затверджену комітетом Міністрів ЄС 13.09.1989 року. Вона містить список правопорушень, рекомендований країнам - учасницям ЄС для розробки єдиної карної стратегії, пов'язаної з комп'ютерними злочинами. Також в документі відмічена необхідність досягнення міжнародного консенсусу з питань криміналізації деяких злочинів, пов'язаних з комп'ютерами. Рекомендація містить два списки злочинів - «мінімальний» і «факультативний (додатковий)». «Мінімальний» список включає діяння, які обов'язково мають бути заборонені міжнародним законодавством і підлягають переслідуванню в судовому порядку. «Додатковий» список містить ті правопорушення, по яких досягнення міжнародної згоди представляється скрутним.

Значення Рекомендації № 89 важко переоцінити. На відміну від прийнятої більш ніж через 10 років після неї Конвенції Ради Європи про кіберзлочинність, яка досі не ратифікована рядом країн, що підписали її, цей документ зробив великий вплив на розвиток і зміну законодавства країн Європи.

У 1990 році VIII Конгрес ООН з попередження злочинності і поводження з правопорушниками ухвалив резолюцію, що закликає держави - члени ООН збільшити зусилля із боротьби з комп'ютерною злочинністю, модернізуючи національне карне законодавство, сприяти розвитку в майбутньому структури міжнародних принципів і стандартів запобігання, судового переслідування і покарання в області комп'ютерної злочинності. 14 грудня 1990 року Генеральна Асамблеєю ООН ухвалила резолюцію, що закликає уряди держав - членів керуватися рішеннями, прийнятими на VIII Конгресі ООН.

У 1995 році в Ліоні (Франція) була проведена міжнародна конференція Інтерполу з комп'ютерної злочинності. Учасники конференції підкреслили, що викликає тривогу відсутність міжнародного механізму для раціонального і ефективного протистояння цьому виду злочинності. За підсумками конференції був зроблений висновок, що у більшості країн світу спостерігається усе зростаюче використання інформаційних технології в кримінальній діяльності. Це викликає необхідність постійного вивчення цього кримінального прояву, оскільки розвиток комп'ютерних технології призводить до використання цих інновацій при скоєні комп'ютерних злочинів .

Підхід Інтерполу до боротьби з кіберзлочинністю полягає в тому, щоб використовувати досвід його членів у боротьбі із злочинами у сфері інформаційних технологій шляхом функціонування робочих груп або експертних груп. Робочі групи створюються для вивчення регіонального досвіду і існують в Європі, Азії, Африці і Північній і Південній Америці.

У 1997 році міністри внутрішніх справ і міністри юстиції Великої Вісімки на зустрічі у Вашингтоні прийняли «Десять принципів боротьби з високотехнологічними злочинами», що включають, у тому числі, положення про те, що «для тих, хто зловживає інформаційними технологіями, не повинно бути ніяких» зон безпеки. Правова система повинна забезпечити захист конфіденційності, цілісності і придатності даних і систем від протиправного ушкодження і гарантувати покарання за серйозні правопорушення .

Продуктом багаторічних зусиль Ради Європи стала прийнята 23 листопада 2001 року у Будапешті Конвенція Ради Європи про кіберзлочинність. Це один з найважливіших документів, що регулюють правовідносини у сфері глобальної комп'ютерної мережі і доки єдиний документ такого рівня. Прийняття його - це своєрідна віха в історії боротьби з кіберзлочинністю. Наша країна ратифікувала цю конвенцію 7 вересня 2005 року .

Підготовка Конвенції була тривалим процесом - за чотири роки було складено 27 проектів. Завершальна версія, що містить преамбулу і чотири глави, датована 25 травня 2001 року, була представлена Європейській комісії з боротьби з кіберзлочинністю на 50-м пленарному засіданні 18-22 червня 2001 року.

Про Конвенцію Ради Європи в цій роботі вже було сказано немало, зокрема, про види злочинів, передбачених нею. Ще раз відмітимо, що Конвенція підрозділяє злочини в кіберпросторі на 4 групи. У першу групу злочинів, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних даних і систем входять: незаконний доступ (ст. 2), незаконне перехоплення (ст. 3), дія на комп'ютерні дані (ст. 4) або на системи (ст. 5). Також до цієї групи злочинів входить протизаконне використання спеціальних технічних пристроїв (ст. 6). Об'єктом злочину виступають не лише комп'ютерні програми, розроблені або адаптовані для скоєння злочинів, передбачених в статтях 2-5 Конвенцій, але і комп'ютерні паролі, коди доступу і їх аналоги, за допомогою яких може бути отриманий доступ до комп'ютерної системи в цілому або будь-якій її частині (з урахуванням злочинного наміру). Норми ст. 6 Конвенцій застосовні тільки у тому випадку, якщо використання (поширення) спеціальних технічних пристроїв спрямоване на здійснення протиправних діянь.

До другої групи входять злочини, пов'язані з використанням комп'ютерних засобів : підлог і шахрайство з використанням комп'ютерних технологій (статті 7, 8 Конвенцій).

Третю групу складають злочини, пов'язані з контентом (змістом) даних. До четвертої групи увійшли порушення авторського права і суміжних прав.

Крім того, на початку 2002 р. до Конвенції ухвалив протокол, що додає в перелік злочинів поширення інформації расистського і іншого характеру, що підбурює до насильницьких дій, ненависті або дискримінації окремої особи або групи осіб, що ґрунтуються на расовій, національній, релігійній або етнічній приналежності.

Таким чином, перший розділ Конвенції присвячений видам діянь, що підлягають криміналізації. Її другий розділ освітлює процесуальні аспекти боротьби з кіберзлочинністю.

У Конвенції піднімається одна із основних проблем правового регулювання Інтернету - визначення юрисдикції (ст. 22). Конвенція пропонує традиційне рішення проблеми юрисдикції : карна юрисдикція визначається відповідно до територіальної ознаки (територія держави; борт судна або літака держави). Проте у разі, якщо злочин скоєний поза територіальною юрисдикцією держави, то застосовується карне законодавство тієї держави, громадянином (підданим) якої є злочинець. Відповіді на поставлені питання, судячи з усього, з'являться найближчими роками - у міру появи практики рішення конкретних правових суперечок в всесвітній мережі. Таким чином, проблема визначення підвідомчості і осудності злочинів в кіберпросторі як і раніше залишається відкритою. Щоб уникнути можливих подальших суперечок в Конвенції передбачається, що внутрішні закони держав можуть містити інші норми про юрисдикцію.

Зважаючи на відсутність кордонів в глобальних мережах, Конвенція уточнює ситуацію колізії юрисдикції декількох держав: у такому разі, згідно п. 5 ст. 22, держави повинні проводити консультації для визначення відповідної юрисдикції для судового переслідування.

Глава III Конвенції – «Міжнародна співпраця» - присвячена питанням екстрадиції, спільній діяльності держав-учасників у сфері боротьби з комп'ютерними злочинами і досягнення узгодженості для збору доказів в електронній формі.

Конвенція про кіберзлочинність на сьогодні є одним з базових міжнародно-правових актів у сфері права телекомунікацій, але і цей документ не позбавлений недоліків. Ще до підписання Конвенції деякі групи по захисту громадянських прав і провайдери інтернет-послуг приводили серйозні аргументи проти укладення цього договору, який на їх погляд має неясні формулювання і пред'являє провайдерам непосильні вимоги.

У число організацій, що підписали протест проти прийняття Конвенції, увійшли «Фонд Електронних Меж» (Electronic Frontier Foundation, США), міжнародна організація «Суспільство Інтернет» (Internet Society), «Організація кіберправа і кіберсвободи» (Cyber - Rights & CyberLiberties, Великобританія), «Кріптополіс» (Kriptopolis, Іспанія) і інші. У протесті відзначається, що Конвенція несе в собі загрозу для норм захисту особи, що встановилися, невиправдано розширює поліцейські функції уряду, а також знижує відповідальність держави в правоохоронній діяльності.

Звичайно, єдиним критерієм ефективності Конвенції, так само як і справедливості заперечень критично налагоджених опонентів, являється практика її застосування положень. Окремі положення Конвенції (наприклад, що стосуються процесуальних питань, визначення юрисдикції і класифікації кіберзлочинів) надалі будуть переглянуті. Але сьогодні можна констатувати, що прийняття Конвенції послужить фундаментом для міжнародного законодавства, що формується. Навіть ті країни, які з яких-небудь причин не підписали Конвенцію можуть використовувати досвід, що накопичується, по правовому регулюванню нової предметної області – кіберпростір.

Зусилля, що робляться на міжнародному рівні, пов'язані з діями з реформування карного законодавства на національному рівні. Національні і міжнародні зусилля доповнюють один одного, забезпечуючи глобальну увагу до проблем кіберзлочинності і обумовлюючи координацію кроків по боротьбі з кіберзлочинністю і уніфікацію національних законодавств.. Міжнародні і наднаціональні організації, безумовно, внесли величезний вклад в реформування національних законодавств і координацію процесуальних, технічних і інших дій з виявлення кіберзлочинів, їх розслідування і судового переслідування.

Але навіть якщо враховувати прогрес в реформуванні національних законодавств і координації міжнародних зусиль експертами постійно підкреслюється необхідність розвитку усебічних, послідовних національних стратегій, які наслідуватимуть глобальну стратегію боротьби з кіберзлочинністю. Зусилля, що робляться на міжнародному рівні, обов'язково повинні підкріплюватися діями на рівні окремо взятої держави.

10 березня 2004 року європейським парламентом створено європейське агентства по мережевій і інформаційній безпеці (ENISA). Це агентство Євросоюзу, створені з метою підвищення ефективності функціонування внутрішнього ринку. Агентство виступає в ролі консультанта і центру передових технології у сфері мережевої і інформаційної безпеки для країн-членів і інститутів Євросоюзу. Крім того, агентство сприяє розвитку зв'язків між країнами-членами Євросоюзу, інститутами Євросоюзу, господарюючими суб'єктами і приватним бізнесом.

**У січні 2013 року в Гаазі відкрився Європейський** центр боротьби з кіберзлочинністю (ЕС3). Завдання ЕС3 - присікати дії організованих злочинних мереж. На даний момент об'єкти уваги ЕС3 обмежені трьома онлайн-шахрайство, що заподіює великий збиток фінансовим організаціям і їх клієнтам; поширення дитячої порнографії, кібератаки на ключові інфраструктури і інформаційні системи .

## Центр з боротьби з кіберзлочінністю (European CyberCrime Centre, EC3) розпочав свою роботу в Європейському Союзі з початку 2013 року.

Як повідомляє Європол (Europol), EC3 стане координаційним центром ЄС у боротьбі з кіберзлочінністю. Держави-члени ЄС та європейські інституції будуть підтрімуваті ЄC3 для створення оперативних і аналітичних можливостей розслідування злодіянь у мережі і для співпраці з міжнароднімі партнерами.

Діяльність Центру охопить боротьбу з наступними видами кіберзлочинності: злочини, вчинені організованими групами для отримання злочинних доходів, зокрема, online-шахрайство; злочини, які завдали серйозної шкоди жертві, зокрема, сексуальна експлуатація дітей; злочини, які завдали шкоди критично важливим інфраструктурним та інформаційним системам в ЄС. Офіційно EC3 почав функціонувати з 1 січня нинішнього року. Тим не менше, церемонія відкриття відбудеться 11 січня у штаб-квартирі Європолу в Гаазі (Нідерланди).

У 2007 році в Україні створено CERT-UA (Computer Emergency Response Team of Ukraine – команда реагування на комп’ютерні надзвичайні події України) – спеціалізований структурний підрозділ Державного центру захисту інформаційно-телекомунікаційних систем Державної служби спеціального зв’язку та захисту інформації України (Держспецзв’язку). CERT-UA з 2009 року була акредитована у FIRST (Forum for Incident Response and Security Teams – Форум команд реагування на інциденти інформаційної безпеки) та вже протягом 5 років є його повноправним членом. Слід зазначити, що членство у FIRST, в рамках протидії кібернетичним загрозам на міжнародному рівні, надає можливість оперативно взаємодіяти з 284 командами реагування на комп’ютерні інциденти (CERT) з 61 країни світу.

В нашій державі нормативно-правову базу правового регулювання в даній сфері складають Конституція України, Кримінальний кодекс України, Конвенція Ради Європи «Про кіберзлочинність», Закони України «Про основи національної безпеки України», «Про захист інформації в інформаційно-телекомунікаційних системах» тощо, Укази Президента України від 08 липня 2009 року № 514/2009, від 08 червня 2012 року № 389/2012, № 390/2012, інші нормативно-правові акти.

У ряді міждержавних нормативно-правових актів визнано, що кіберзлочинність сьогодні представляє загрозу не лише національної безпеки окремих держав, а погрожує людству і міжнародному порядку.

З початку 90-х років ХХ століття вказаній проблемі приділяється значна увага у багатьох країнах світу. Позначені питання знаходяться і у полі зору урядових структур нашої держави. Стимулом для цього також виступають узяті Україною зобов'язання по інтеграції у міжнародну та світову спільноту, у тому числі відповідно до Програми інтеграції України в Європейський Союз (розділ 13 - "Інформаційне суспільство").

Дуже високий рівень латентності кіберзлочинності обумовлено рядом причин таких як: низький рівень спеціального технічного оснащення правоохоронних структур сучасними засобами комп'ютерної техніки і комп'ютерними технологіями; відсутність знань і навичок виявлення, розкриття і розслідування кіберзлочинів із-за обмеження доступу до сучасних методик, тактики і техніки; низький рівень інформаційної культури, підготовленості широкого круга кадрів правоохоронних органів і суддів про залучення винних до карної відповідальності; недовіра потерпілих в правоохоронні органи (пов'язано з вищезгаданими чинниками) і т.д.

Порівняльний аналіз досліджень передового зарубіжного досвіду боротьби з кіберзлочинністю свідчить, що вона має тенденцію до росту. Однією з умов її росту є ускладнення сучасних телекомунікаційних та технічних систем глобального зв'язку і спрощення доступу до використання комп'ютерних технологій широкого круга користувачів через персональні комп'ютери.

У ведучих, економічно розвинених країнах рівень втрат від кіберзлочинності вимірюється кількісно тисячами, а економічні збитки складають мільярди доларів США. За оцінками Інтерполу тільки в Європі збиток від дій кіберзлочинців щорічно складає 750 мільярдів євро. Втрати США від кіберзлочинності складають від 20 до $ 140 млрд. доларів, або близько 1% від ВВП країни, а в Латинській Америці фінансові втрати від діяльності кіберзлочинців в 2013 склали 1,1 млрд. доларів. Такі дані опублікувала неурядова організація LACNIC, що займається аналізом Інтернет - активності в регіоні.

Дослідження питань боротьби з кіберзлочинністю показало, що орієнтація тільки на технічні засоби забезпечення інформаційної безпеки в умовах інформатизації суспільства, у тому числі профілактики боротьби з кіберзлочинами, не досягла значних успіхів. Це в значній мірі зобов’язано з підвищенням рівня знань користувачів комп'ютерної та телекомунікаційної техніки.

Парадокс полягає в тому, що чим складніше стає програмне забезпечення (software), тим більш вразливими виявляються традиційні організаційні заходи і засоби інженерного та технічного захисту інформації в комп'ютерних та інформаційних системах, зокрема стосовно несанкціонованого доступу до комп’ютерів та мереж.

Ще однією проблемою порядку є і те, що з розвитком електронних засобів інформації розвиваються технічні засоби перехоплення і несанкціонованого доступу до інформації, яка передається по електронним системах зв'язку.

Найбільшу небезпеку для держави та суспільства складає міжнародна організована кіберзлочинність особливо у сфері економічних відносин в фінансових та банківських системах.

Правовою основою по протидії комп'ютерної злочинності на національному рівні є Кримінальний кодекс України (КК). В цьому КК окремі види комп'ютерних злочинів (кіберзлочинів) виділено в розділ VI Особливої частини - Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж (ст. 361, 361, 363). Окремі види злочинів, в яких комп'ютерні продукти визначені як засіб злочини, розміщені в інших розділах Особливої частини : В Розділу V Особливої частини зазначені окремі види злочинів, в яких комп'ютерні продукти визначені як засіб злочину (ст. 163, 176, 177) та Злочини у сфері господарської діяльності (ст. 200) в Розділу VII.

**Шанхайська організація співробітництва** (ШОС) є міжнародною організацією з шести країн-членів (Китай, Казахстан, Киргизстан, Росія, Таджикистан і Узбекистан), яка була створена в 2001 для цілей політичного, військового та економічного співробітництва. Особлива увага приділяється боротьбі з «тероризмом, сепаратизмом та екстремізмом».

У 2009 році було укладено Угоду між урядами держав-членів ШОС про співробітництво в галузі забезпечення міжнародної інформаційної безпеки (Єкатеринбург, 16 червня 2009 року) 12 вересня 2011 роки чотири члени ШОС представили проект міжнародного кодексу поведінки для інформаційної безпеки Генеральній Асамблеї Організації Об'єднаних Націй. Ця первісна група була розширена до шести членів в 2015 році, коли було представлено новий проект Генеральній Асамблеї ООН, хоча зміст цього документа не сильно відрізнявся від попереднього.

**4. Основні міжнародні інструменти боротьби із кіберзлочинністю.**

Кіберзлочинність є однією з найбільш швидко зростаючих сфер злочинності. Все більше і більше злочинців експлуатують швидкість, зручність і анонімність, що пропонують сучасні технології, щоб використати широкий спектр злочинної діяльності. До них відносяться напади на комп'ютерні дані і системи, крадіжка особистих даних, поширення зображень сексуального насильства, інтернет-шахрайство, проникнення до систем інтернет-фінансових послуг, а також поширення вірусів, ботнетів і різні шахрайства щодо електронної пошти, такі як фішинг.

Глобальний характер Інтернету дозволяє злочинцям здійснити практично будь-яку незаконну діяльність в будь-якій точці світу, що робить адаптацію внутрішніх автономних засобів управління країн необхідною для боротьби зі злочинами, що вчинені в кіберпросторі. Використання Інтернету терористами, зокрема для вербування і підбурювання радикалізації, являє собою серйозну загрозу для національної і міжнародної безпеки.

Крім того, загроза тероризму змушує владу звертати увагу на усунення вразливостей безпеки утворень, пов'язаних з інформаційно-технологічною інфраструктурою, таких як електростанції, електричні мережі, інформаційні системи і комп'ютерні системи державних і приватних компаній.

Цифрові технології забезпечують цей зв'язок і надають своїм користувачам багато переваг. Але в той же час, забезпечують середовище для злочинної діяльності, починаючи від вандалізму до крадіжки особистої інформації та секретної урядової інформації.

Цей інноваційний тип злочину був складним питанням для правоохоронних органів, частково через відсутність законодавства для надання допомоги в галузі кримінального переслідування, а також через брак кваліфікованих дослідників в технології, яка в даний час переживала атаки хакерів. Було ясно, що комп'ютерні системи були вразливі для злочинної діяльності. Ічим більш складні зв'язки ставали доступні споживачеві, тим більше можливостей для кіберзлочинності розроблялося.

У 1986 році системний адміністратор в Національній лабораторії Лоренса Берклі, Кліффорд Столл, помітив деякі порушення в облікових даних. Працюючи над першими цифровими методи судово-медичної експертизи, він вирішив, що неавторизований користувач намагався зламати його комп'ютерну мережу. Столл використовував тактику, яка приваблює хакера назад в мережу, поки не будуть зібрані дані, щоб відстежувати проникнення до його джерела. За вторгненням до лабораторії Берклі незабаром прослідувало відкриття вірусу хробака Морріса, створеного Робертом Морісом, студентом Корнельського університету. Цей черв'як пошкодив більше 6000 комп'ютерів і призвело до збитків у $ 98 млн. Інші інциденти стали слідувати в безперервному, стійкому потоці. Конгрес відповів, запустивши в роботу першу низку законів пов’язаних із хакерською діяльністю - Федеральний закон комп'ютерного шахрайства та зловживання, 1986. Цей закон перетворив акт комп'ютерного злочину на кримінальний злочин, який карається позбавленням волі на значний час і грошовими штрафами.

У 1990 році під час проекту, який охрестили Операція Sundevilf:, агенти ФБР конфіскували 42 комп'ютери і більше 20 000 дискет, які, нібито, використовувалися злочинцями для незаконного використання кредитних карт і телефонних послуг. Ці два роки зусиль вимагали 150 агентів. Незважаючи на низьке число обвинувальних висновків, операція розглядається як успішний приклад зв'язків з громадськістю, виконаних співробітниками правоохоронних органів. Гері М. Дженкінс, помічник директора Секретної служби CLLIA, пояснив на прес-конференції, що ця діяльність направляє повідомлення злочинцям, що "за ними пильнують у всьому світі, навіть в тих нечесних і засекречених гніздах кібернетичного пороку, підземних системах".

Незважаючи на їх ефективність, рішення і діяльність правоохоронних органів щодо розслідування кіберзлочинів не завжди досконалі. Якщо правоохоронні органи роблять помилку, законослухняні громадяни можуть постраждати. Видавнича компанія Steve Jackson Games була майже витіснена з бізнесу після звинувачення в зберіганні незаконно скопійованого документа. Спецслужби вважали, цей документ був в розпорядженні Джексона, і конфіскували комп'ютери, що використовувалися в його бізнесі. Оскільки обладнання не було повернуто вчасно, він був змушений звільнити співробітників, пропустив терміни і його бізнес був майже зруйнований. Коли були повернуті комп'ютери, Джексон виявив, що було здійснено втручання в електронну пошту компанії і дані про клієнтів було видалено. Секретна служба так і не звинуватила його у жодному злочині.

**Electronic Frontier Foundation** (EFF) - фундація, утворена в 1990 році у відповідь на погрози громадянським свободам, які можуть мати місце через надто сувору діяльність і помилки, що здійснюються співробітниками правоохоронних органів, які розслідують кіберзлочинність і пов'язані з цим питання. Це група технологів, юристів і інших фахівців, які діють у сфері захисту споживачів від незаконного переслідування.

в нашому суспільстві, незалежно від кращих зусиль системи кримінального правосуддя. Державному і приватному сектору необхідно шукати висококваліфікованих фахівців для боротьби з цією загрозою і запобіганню переслідуванню невинних людей.

Першою міжнародною ініціативою з комп'ютерної злочинності в Європі стала **конференція Ради Європи з Кримінологічних аспекти економічної злочинності** в Страсбурзі в 1976 р. Було введено кілька категорій комп'ютерних злочинів.

**Арабська конвенція про боротьбу з правопорушеннями у сфері інформаційних технологій.** Його Величність Султан Кабус бін Саїд, султан Омана видав сьогодні понеділок, 09/03/2015 А.Д., указ про видання "Арабської конвенції про боротьбу з правопорушеннями у сфері інформаційних технологій". Інформаційне агентство Оману (СМА) говорить, що указ про ратифікацію "Арабської конвенції про боротьбу з інформаційних технологій" проступків, підписаний Султанату на 15/02/2012 Ай був виданий на основі загального інтересу.

Ця конвенція спрямована на зміцнення та підтримку зв'язків співробітництва між арабськими державами в області боротьби з ІТ-злочинами. Мета - побороти небезпеку злочинів, забезпечення безпеки арабських держав, інтересів і безпеки своїх громадян і членів.

Конвенція передбачає, що кожна держава-член, відповідно до її основних системами або конституційних принципів, має виконувати свої зобов'язання, що випливають із застосування цієї Конвенції відповідно до принципів рівності, територіального суверенітету держав і невтручання у внутрішні справи інших держав, а також, що Конвенція не дає права будь-якій державі-члену на території іншої держави набувати юрисдикції, ні функції, які входять виключно до компетенції органів цієї держави відповідно до її внутрішнього закону.

Угода між урядами держав-членів Шанхайської організації співпраці про співпрацю в області забезпечення міжнародної інформаційної безпеки

Шанхайська організація співробітництва (ШОС) є міжнародною організацією з шести країн-членів (Китай, Казахстан, Киргизстан, Росія, Таджикистан і Узбекистан).

У 2009 році було укладено Угоду між урядами держав-членів

ШОС про співробітництво в галузі забезпечення міжнародної інформаційної безпеки (Єкатеринбург, 16 червня 2009 року) 12 вересня 2011 роки чотири члени ШОС представили проект міжнародного кодексу поведінки для інформаційної безпеки Генеральній Асамблеї Організації Об'єднаних Націй. Ця первісна група була розширена до шести членів в 2015 році, коли було представлено новий проект Генеральній Асамблеї ООН, хоча зміст цього документа не сильно відрізнявся від попереднього.

Поняття «міжнародної інформаційної безпеки» є спірним. Беручи до уваги, що держави-члени ШОС вважають, що контент є потенційною загрозою безпеці, і повинен регулюватися, то «західний консенсус» вважає цей рівень регулювання загрозою фундаментальним людським правам.

**5. Основні міжнародні міжурядові організації в боротьбі з кіберзлочинністю**

**Організація Об'єднаних Нації**

Існують численні глобальні організації. Проте, ООН може бути ідентифікована як єдина глобальна організація, яка створила форум своїх 191 держав-членів з більш повними функціями. У порівнянні з професійними організаціями, ООН не обмежує свою діяльність певними областями. На відміну від регіональних організацій, ООН необмежує свою діяльність декількома державами (в області захисту кібербезпеки і запобігання кіберзлочинності). Дії ООН мають унікальні переваги в координації міжнародних позицій.

У 1985 році Резолюція Генеральної Асамблеї 40/71 від 11 грудня закликала уряди і міжнародні організації вжити заходів відповідно до Рекомендації Комісії про правове значення комп’ютерних записів 1985, для забезпечення правової безпеки на тлі найширшої можливості використання обробки інформації в міжнародному спілкуванні.

У 1990 році Генеральна Асамблея ООН прийняла Керівні принципи, що стосуються комп'ютеризованих персональних даних. Вона запропонувала вжити відповідних заходів для захисту файлів від природних і штучних небезпек. Рекомендації продовжили захист урядових міжнародних організацій.

"Міжнародний огляд кримінальної політики: Посібник Організації Об'єднаних Націй з профілактики та боротьби з комп'ютерною злочинністю" закликав до подальшої міжнародної роботи і представив належну постановку задачі. Було зазначено, що на міжнародному рівні можуть бути проведені подальші дії, в тому числі гармонізація матеріального права, а також створення юрисдикційної основи.

Конвенція Ради Європи про кіберзлочинність була відкрита для підписання на конференції в Будапешті, Угорщина, 23 листопада, 2001. Конвенція є історичною віхою в боротьбі з кіберзлочинністю, і вступила в чинність 1липня 2004.

Додатковий протокол про криміналізацію актів расистського та ксенофобського характеру, що здійснюються через комп'ютерні системи з січня 2003 року також був прийнятий. Конвенція складається з чотирьох розділів.

Глава 1 включає в себе визначення термінів (комп'ютерна система, комп'ютерні дані, оператор мережі ідані за трафіком).

Глава 2 включає в себе заходи, які повинні бути прийняті на національному рівні і охоплює матеріальне кримінальне право, процесуальне право та юрисдикції. Матеріальне кримінальне право містить злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, злочинів, що пов’язані з комп’ютерами і з торгівлею людьми, також такі злочини як підроблення та шахрайство, злочини, пов'язані з дитячою порнографією, а також злочини, пов'язані з порушенням авторського права і суміжних прав. Положення процесуального права поширюються на будь-який злочин, скоєний за допомогою комп'ютерної системи, а також на збір доказів у електронній формі.

Глава 3 про міжнародне співробітництво включає в себе принципи, що стосуються видачі, загальні принципи, що стосуються взаємної допомоги, процедур, що стосуються прохань про надання взаємної допомоги в разі відсутності відповідних міжнародних угод, взаємної допомоги щодо тимчасових заходів, взаємну допомогу у зв'язку зі слідчими повноваженнями і 24/7 мережу.

Глава 4 у заключних положеннях містить прикінцеві положення, в основному, у відповідності зі стандартними положеннями договорів Ради Європи. Відповідно до статті 40, будь-яка держава може заявити, що вона скористалася можливістю вимагати додаткових елементів, як це передбачено в деяких статтях. Аналогічно для застережень відповідно до статті 42, будь-яка держава може заявити, що вона користується застереженнями, передбаченими вдеяких статтях.

**ОЕСР**

Організація економічного співробітництва і розвитку (ОЕСР), у 2002 році прийняла нові Керівні принципи з безпеки інформаційних систем і мереж: до культури безпеки.

Такий підхід до захисту критичної інформаційної інфраструктури є орієнтиром, і як такий не є обов’язковим для членів ОЕСР.

У 2003 році в Осло було проведено Глобальний форум з інформаційних систем і мережевої безпеки була в 2003 році. Семінар по боротьбі з кіберзлочинністю був приурочений до цього Форуму.

Цільова група ОЕСР по спаму була створена в 2004 році і виступила з доповіддю в 2006.

А семінари спільної роботи АТЕС-ОЕСР з питань безпеки інформації було проведено в Сеулі в 2005 році, де були обговорені кілька тем, в тому числі сприяння реакції щодо глобальних урядових інцидентів.

Організація приділяє багато уваги кібербезпеці, а також сприяє глобальному скоординованому підходу до політики зміцнення довіри. Робоча група ОЕСР з інформації та конфіденційності розробляє міжнародні керівні принципи.

**Ліга арабських держав**

Кілька країн Ліги арабських держав, такі як Саудівська Аравія і Об'єднані Арабські Емірати, прийняли законодавство про кіберзлочинність, ОАЕ була першою країною в регіоні, яка прийняла законодавство, Закон про кіберзлочинність № 2, в лютому 2006 року. Рада зі співробітництва країн Перської затоки за участю Бахрейну, Кувейту, Оману, Катару, Саудівської Аравії і Об'єднаних Арабських Еміратів на конференції в червні 2007 року рекомендувала, щоб країни заключали договори про кіберзлочинність.

**Африканський союз**

Деякі члени Африканського союзу, такі як Маврикій, Південна Африка і Замбія прийняли законодавство щодо кіберзлочинності.

Східна Африка включає Танзанію, Кенію та Уганду. Прогрес в боротьбі з кіберзлочинністю законодавства був повільним в цьому регіоні, за винятком Уганди. У 2008 році в Уганді був прийнятий Закон про порушення права користування комп'ютером і законодавчий процес почався. Країни Східної Африки намагаються координувати зусилля з тим, щоб законодавчі акти були аналогічні законам щодо кіберзлочинів в південній частині Африки.

Проекти доповідей про узгодження політики і регулювання телекомунікаційних, інформаційних та комунікаційних технології були опубліковані. Вони також включають відстеження і боротьба з кіберзлочинністю в усіх формах. Співтовариство розвитку Півдня Африки за участю Замбії, Зімбабве, ПАР, Малаві і Мозамбік, ініціювало зусилля по гармонізації законів про кіберзлочинність в 2005 році.

Женевські домовленості щодо правового регулювання кіберзло чинів

**Міжнародний союз електрозв'язку в Женеві.**

Найбільш активним інститутом ООН в досягненні узгодженості в глобальній кібербезпеці і кіберзлочинності є Міжнародний союз електрозв'язку (МСЕ) в Женеві. Генеральна Асамблея ООН визнала в 2001 році потребу в багатофазних Всесвітніх самітах питань інформаційного суспільства (ВСЮ) і просила МСЕ взяти на себе провідну роль в координації надійної, багатосторонньої участі в цих заходах.

Перший етап ВСЮ відбувся у Женеві в грудні 2003 року , Другий етап відбувся в Тунісі в 2005 році. Після ВСЮ та Повноважної конференції МСЕ 2006 року, МСЕ взяв на себе важливу роль в координації зі зміцнення довіри і безпеки при використанні інформації та комунікаційних технологій (ІКТ).

На ВСЮ в Тунісі в 2005 році МСЕ була доручена роль посередника для : "Зміцнення довіри і безпеки при використанні інформаційно-комунікаційних технологій (ІКТ)".

Глобальна програма кібербезпеки була запущена в травні 2007 року Генеральним секретарем в якості глобальної основи для діалогу та міжнародного співробітництва, спрямованого на стратегії для пошуку рішень для підвищення рівня безпеки в інформаційному суспільстві. Програма складається з семи основних стратегічних цілей, в тому числі основної стратегічної мети для законодавчих заходів.

З метою надання допомоги Генеральному секретарю МСЕ в розробці стратегічних пропозицій для держав-членів, було створено групу експертів високого рівню в жовтні 2007 року. Це глобальна експертна група з більш ніж 100 експертів, що в червні 2008 року наддала поради щодо стратегії в наступних п'яти областях роботи: юридичні заходи, технічні та процедурні заходи, організаційні структури, нарощування потенціалу та міжнародного співробітництва.

**Проекти Інтерполу**

Програма кіберзлочинності Інтерполу будується навколо підготовки та операцій і існує, щоб не відставати від нових загроз. Вона переслідує такі цілі:

- Сприяти обміну інформацією між країнами-членами в рамках регіональних робочих груп і конференцій;

- Давати навчальні курси для створення і підтримки професійних стандартів; ^ Координація та сприяння міжнародних операцій;

- Встановити глобальний список контактних офіцерів, доступний цілодобово для розслідування кіберзлочинів (список містив 134 контактів в кінці 2012 року);

- Надання допомоги країнам-членам у випадку кібер-атак або розслідуванні кіберзлочинів шляхом слідчих послуг і баз даних;

- Виявлення нових загроз і надання інформації розвідки країнам-членам;

- Забезпечити безпечний веб-портал для доступу до оперативної інформації і документів.

**Діяльність Європолу**

Європейський центр боротьби з кіберзлочинністю (ЕСЗ) почав свою діяльність в січні 2013 року з метою посилити реакції правоохоронних органів на боротьбу з кіберзлочинністю в Європейському союзі (ЄЄ) і допомогти захистити європейських громадян, бізнесу та уряду. Його створення є одним з пріоритетів в рамках стратегії внутрішньої безпеки ЄС.

Загроза з боку кіберзлочинів зростає, і ЄС є ключовим об'єктом, в основному завдяки своїй розвиненій інфраструктурі Інтернету, економіці і системі платежів, що від нього залежать.

Створюючи ЕСЗ в рамках Європолу Центр отримав можливість не тільки спиратися на існуючі потужності правоохоронних органів Європолу, а й істотно розширити інші можливості, зокрема, оперативну та аналітичну підтримку розслідувань держав-членів.

**6. Женевські домовленості щодо правового регулювання кіберзлочинів.**

Найбільш активним інститутом ООН в досягненні узгодженості в глобальній кібербезпеці і кіберзлочинності є Міжнародний союз електрозв'язку (МСЕ) в Женеві. Генеральна Асамблея ООН визнала в 2001 році потребу в багатофазних Всесвітніх самітах питань інформаційного суспільства (ВСЮ) і просила МСЕ взяти на себе провідну роль в координації надійної, багатосторонньої участі в цих заходах.

Перший етап ВСЮ відбувся у Женеві в грудні 2003 року , Другий етап відбувся в Тунісі в 2005 році. Після ВСЮ та Повноважної конференції МСЕ 2006 року, МСЕ взяв на себе важливу роль в координації зі зміцнення довіри і безпеки при використанні інформації та комунікаційних технологій (ІКТ).

На ВСЮ в Тунісі в 2005 році МСЕ була доручена роль посередника для : "Зміцнення довіри і безпеки при використанні інформаційно-комунікаційних технологій (ІКТ)".

Глобальна програма кібербезпеки була запущена в травні 2007 року Генеральним секретарем в якості глобальної основи для діалогу та міжнародного співробітництва, спрямованого на стратегії для пошуку рішень для підвищення рівня безпеки в інформаційному суспільстві. Програма складається з семи основних стратегічних цілей, в тому числі основної стратегічної мети для законодавчих заходів.

З метою надання допомоги Генеральному секретарю МСЕ в розробці стратегічних пропозицій для держав-членів, було створено групу експертів високого рівню в жовтні 2007 року. Це глобальна експертна група з більш ніж 100 експертів, що в червні 2008 року наддала поради щодо стратегії в наступних п'яти областях роботи: юридичні заходи, технічні та процедурні заходи, організаційні структури, нарощування потенціалу та міжнародного співробітництва.

Роль МСЕ полягає в пошуку консенсусу в рамках міжнародного співробітництва в області кібербезпеки, з тим щоб досягти загального розуміння загроз між країнами на всіх етапах економічного розвитку, яка включає в себе розробку і введення в дію рішень, спрямованих на вирішення глобальної проблеми в області кібербезпеки і кіберзлочинності. Програма є основою для пропозиції стратегій для рішень по зміцненню довіри і безпеки в інформаційному суспільстві, під егідою кібербезпеки.

Принципи цієї структури була прийняті в 2005 році в рамках Туніської програми ВСЮ. Туніська програма, пункт 42 і 40, свідчить про таке: Ми підтверджуємо, що заходи, прийняті для забезпечення стабільності і безпеки Інтернету, для боротьби з кіберзлочинністю і протидії спаму, повинні забезпечувати захист і дотримання положень про недоторканність приватного життя і свободу слова, які містяться у відповідних частини Загальної декларації прав людини (Пункт 42).

Ми закликаємо уряди у співпраці з іншими зацікавленими сторонами розробити необхідне законодавство для розслідування і судового переслідування кіберзлочинності, відзначаючи існуючі рамки, наприклад, Резолюції ГА ООН 55/63 та 56/121 «Боротьба з злочинним використанням інформаційних технологій» і регіональні ініціативи, в тому числі, але не обмежуючись цим, Конвенцію кіберзлочинності Ради Європи. (Пункт 40) Основна стратегічна мета Глобальної програми кібербезпеки для законодавчих заходів, є розробка стратегій для створення типового законодавства про кіберзлочинність.

Хоча члени експертної групи не змогли досягти повного консенсусу в кожній рекомендації, більшість експертів були в цілому згодні з багатьма рекомендаціями, які встановлюють чіткий напрямок для майбутньої роботи МСЕ в області кібербезпеки. Зокрема, члени групи були згодні, що життєво необхідно вжити заходів для сприяння забезпеченню кібербезпеки і МСЕ відіграє важливу роль.

**7. Додаткові джерела регулювання кіберзлочинності.**

Конгреси ООН із запобігання злочинності розглянули технічні питання і питання кримінального примусу щодо комп'ютерного зловживання на найближчі чотири з'їзди.

Організація Об'єднаних Націй у 1990 році прийняла резолюцію по законодавству про комп'ютерні злочини на 8-му з'їзді ООН щодо попередження злочинності та поводження з правопорушниками в Гавані, Куба.

Конгрес в Бангкоку, Таїланд, зосередився на питаннях комп'ютерної злочинності на спеціальному семінарі. Декларація Бангкоку №16 говорить: ми відзначаємо, що нинішній період глобалізації, інформаційних технологій і швидкого розвитку нових телекомунікаційних та комп'ютерних мережевих систем супроводжується зловживанням цими технологіями в злочинних цілях. Тому ми вітаємо зусилля щодо активізації та розширення існуючого співробітництва з метою запобігання, розслідування і кримінального переслідування злочинів з використанням високих технологій та пов'язаних з комп'ютерною злочинністю, в тому числі шляхом розвитку партнерських відносин з приватним сектором. Ми визнаємо важливий внесок Організації Об'єднаних Націй в регіональні та інші міжнародні форумів по боротьбі з кіберзлочинністю та пропонуємо Комісії з попередження злочинності та кримінального правосуддя, беручи до уваги цей досвід, вивчити питання про доцільність подальшого надання допомоги в цій галузі під егідою організації Об'єднаних Націй в партнерстві з іншими організаціями, що займаються аналогічними питаннями.

Програма кіберзлочинності Інтерполу будується навколо підготовки та операцій і існує, щоб не відставати від нових загроз. Вона переслідує такі цілі: сприяти обміну інформацією між країнами-членами в рамках регіональних робочих груп і конференцій; давати навчальні курси для створення і підтримки професійних стандартів; координація та сприяння міжнародних операцій; встановити глобальний список контактних офіцерів, доступний цілодобово для розслідування кіберзлочинів (список містив 134 контактів в кінці 2012 року); надання допомоги країнам-членам у випадку кібер-атак або розслідуванні кіберзлочинів шляхом слідчих послуг і баз даних; розробка стратегічних партнерських відносин з іншими міжнародними організаціями та органами приватного сектора; виявлення нових загроз і надання інформації розвідки країнам-членам; забезпечити безпечний веб-портал для доступу до оперативної інформації і документів.

Інтерпол організовує міжнародні конференції і семінари по боротьбіз кіберзлочинністю, щоб служити форумом для обміну знаннями і досвідом в розслідуванні кіберзлочинів. Ці події об'єднують зусилля експертів з правоохоронних органів, приватного сектора і наукових кіл, щоб представити і обговорити новітні технології в боротьбі з кіберзлочинністю.

У триденній міжнародній конференції під назвою Глобальне співробітництво сьогодні для боротьби з інформаційними ризиками завтра, взяли участь близько 300 делегатів з більш ніж 50 країн для пошуку шляхів запобігання та виявлення високотехнологічних злочинів. Відбулася вона в Гонконзі у вересні 2010 року.

**Діяльність Європолу.** Європейський центр боротьби з кіберзлочинністю (ЕСЗ) почав свою діяльність в січні 2013 року з метою посилити реакції правоохоронних органів на боротьбу з кіберзлочинністю в Європейському союзі (ЄЄ) і допомогти захистити європейськихгромадян, бізнесу та уряду. Його створення є одним з пріоритетів в рамках стратегії внутрішньої безпеки ЄС.

Загроза з боку кіберзлочинів зростає, і ЄС є ключовим об'єктом, в основному завдяки своїй розвиненій інфраструктурі Інтернету, економіці і системі платежів, що від нього залежать.

Створюючи ЕСЗ в рамках Європолу Центр отримав можливість не тільки спиратися на існуючі потужності правоохоронних органів Європолу, а й істотно розширити інші можливості, зокрема, оперативну та аналітичну підтримку розслідувань держав-членів.

ЕСЗ була поставлена задача зосередити увагу на наступних трьох областях: кіберзлочинність, здійснювана організованими групами, зокрема, щодо створення великих злочинних доходів, таких як онлайн-шахрайства; кіберзлочинність, яка завдає серйозної шкоди потерпілому, така як он-лайн сексуальна експлуатація дітей; кіберзлочинність (включаючи кібератаки), що впливають на критичні інфраструктури та інформаційні системи в Європейському Союзі.

**8. Взаємна допомога у розслідуванні кіберзлочинів.**

Бар'єри на шляху до співпраці: співробітники правоохоронних органів стикаються з перешкодами на шляху ефективного міжнародного співробітництва, включаючи:

1. Суверенітет

2. Правонаслідування і проблеми аутентифікації

3. Протоколи 19-го століття застосовуються для потреб 21-го століття

4. Невідповідність ресурсів

1. Видача, взаємна правова допомога та інші види формального співробітництва залежать від внутрішнього законодавства

а. Внутрішні закони формують основу для злочинів, що можуть в подальшому потребувати взаємної допомоги

б. Договір може обмежити співпрацю, щоб знайти підтвердження правопорушенню

с. Поведінки повинна бути кримінальною відповідно до законодавства обох запитуваних і запитуючих держав - "подвійна злочинність"

2. Міжнародні зусилля зосереджені на вдосконаленні внутрішніх законів про кіберзлочинність

а. Резолюція 55/63 Генеральної Асамблеї Організації Об'єднаних Націй: "Боротьба зі злочинним використанням інформаційних технологій" правові системи повинні захищати цілісність даних і комп'ютерних систем від знецінення та забезпечити, щоб злочинне зловживання було покаране

б. Конвенція Ради Європи про кіберзлочинність має суттєві, процесуальні положення та положення про співпрацю; підписана в 2001 році в Будапешті, Угорщина; вступила в силу в 2004 році; відома як "Будапештська конвенція", відкрита для всіх країн; 22 країни є учасниками (включаючи США).

Зобов'язує сторони:

1) створити суттєві внутрішні закони по боротьбі з кіберзлочинністю

2) Переконатися, що внутрішні співробітники правоохоронних органів мають процедурні повноваження з розслідування і судового переслідування кіберзлочинності

3) Забезпечити міжнародне співробітництво з Гншими сторонами в боротьбі з кіберзлочинністю

4) розглядати кримінальні злочини, встановлені в якості злочинів такими, що тягнуть за собою видачу відповідно до чинних договорах про видачу

ДВПП - двосторонні або багатосторонні договори, які можуть бути узгоджені, щоб забезпечити масив формалізованих заходів правової допомоги між країнами. Вони включають в себе пошук і вилучення даних, показання свідків, сприяння та конфіскацію доказів, а також екстериторіальну інформацію.

Вони є основною формою отримання міжнародної правової допомоги і були використані кілька разів, щоб розширити і отримати цифрові докази в розслідуванні кіберзлочинів. ДВПП потенційно може дозволити доступ до даних, які не можуть бути доступні у внутрішньому розслідуванні, так як вони можуть обійти національні засоби захисту, як судової системи, так і гарантій доступу.

Однак ДВПП не є єдиним засобом, за яким звертаються за допомогою, щоб отримати доступ до даних транскордонних. Країни часто змушені запросити певну форму міжнародного співробітництва правоохоронних органів і допомоги. Якщо у добровільній і неформальній допомозі відмовлено, країни можуть вдатися до ДВПП, листів-доручень або листи про видачу.

Такі листи є звичайними методами міжнародного співробітництва. Обмін відбувається між судовими органами, щоб звернутися за допомогою щодо розслідування поточних

**9. Європейська Судова Мережа з Кіберзлочинності та Євроюст.**

Європейське бюро судової співпраці (Євроюст «Eurojust»)

З метою посилення боротьби з тяжкими формами організованої злочинності Європейська рада, що засідала в м. Тампере 15 і 16 жовтня 1999 р., вирішила створити спеціальний підрозділ: Євроюст (Eurojust). Євроюст передбачалося заснувати як орган ЄС, наділений правами юридичної особи.

14 грудня 2000 року з ініціативи Португалії, Франції, Швеції та Бельгії заснували підготовчий орган Про-Євроюст (Pro-Eurojust), попередник Євроюсту, який мав стати форумом прокурорів з усіх держав-учасниць ЄС, сприяючи випробуванню принципів, на яких мав функціонувати Євроюст.

Про-Євроюст розпочав діяльність 1 березня 2001 року. Сучасний Євроюст був створений шляхом ухвалення рішень № 2002/187/JHA Ради ЄС від 28 лютого 2002 р., та № 2009/426/JHA від 16 грудня 2008 р. Ці рішення стали установчими актами нового органа Європейського Союзу.

Євроюст розташований в м. Гаага (Нідерланди). Діяльність Євроюста фінансується із загального бюджету ЄС, за винятком заробітної плати суддів, прокурорів і поліцейських, яка виплачується з бюджету держав, що входять в ЄС. До його складу входять прокурори, магістранти й інші посадові особи з кожної держави-учасниці ЄС, котрі мають подібний посадовий статус. В Єроюсті працює майже 200 співробітників, які забезпечують швидке реагування на прохання про допомогу з боку національних органів та інших органів ЄС.

Основними органами Євроюсту є Колегія та Адміністрація. Функціонуванням та організацією агенції керує Колегія, що складається із 28 членів (по одному від кожної країни ЄС) — прокурорів, суддів або співробітників поліції, що мають аналогічні повноваження. Членам Колегії допомагають заступники та асистенти, а також національні експерти, які входять до адміністрації Євроюсту. Колегія відповідальна за діяльність організації, затверджує проект бюджету й передає затверджений варіант до Єврокомісії.

СНО здійснює моніторинг діяльності Євроюсту, пов'язаної з обробкою персональних даних, і гарантує, що вона провадиться відповідно до Рішення про Євроюст. Для виконання своїх завдань СНО має повний доступ до всіх відповідних документів. Євроюст надає йому всю необхідну інформацію й допомагає цьому органові у виконанні завдань іншими способами. СНО є другою інстанцією для звернення офіцера Євроюсту із захисту даних у разі порушення, а Колегія не вирішила це питання протягом прийнятного періоду часу. Крім того, СНО розглядає звернення від осіб, щодо яких проводиться розслідування, і здійснює контроль. Комісія ЄС бере участь в роботі Євроюста без права голосу.

Завдання Євроюсту полягають у порушенні кримінальних розслідувань, зверненні з пропозиціями щодо порушення кримінальних переслідувань з боку національних органів стосовно фактів злочинних діянь, координації розслідувань і переслідувань, посилення судової співпраці, включно зі співпрацею з Європейською судовою мережею.

У Договорі про функціонування ЄС (ст. 85) передбачено: призначенням Євроюсту є підтримка та посилення координації і співробітництва національних органів, відповідальних за проведення розслідувань і кримінального переслідування за фактами тяжких злочинів, що зачіпають дві чи більше держав-учасниць або потребують проведення кримінального переслідування на загальних засадах — виходячи з операцій, які здійснюються органами держав-учасниць та Європолом, і на базі наданої ними інформації.

Відповідно до Консолідованої версії рішень про Євроюст від 15 липня 2009 року (ст. 3) перед Євроюст ставляться такі цілі:

а) розвивати й покращувати координацію між компетентними органами держав-учасниць щодо дій з розслідування і кримінального переслідування, які вони проводять на своїй території, з урахуванням будь-якого запиту, що надійшов від компетентного органу однієї з них, а також будь-якої інформації, наданої компетентним органом на підставі розпоряджень, виданих відповідно до установчих договорів;

b) зміцнювати співробітництво між компетентними органами держав-учасниць, зокрема, шляхом сприяння виконанню запитів у сфері судової співпраці, в тому числі щодо документів, котрі потребують взаємного визнання;

с) підтримувати іншими способами зусилля компетентних органів держав-учасниць для підвищення ефективності розслідувань та заходів із кримінального переслідування.

Повноваження Євроюсту, спрямовані на досягнення цих цілей.

По-перше, Євроюст може звертатися до компетентних органів відповідних держав-учасниць із запитами про: розслідування чи переслідування в судовому порядку конкретних дій; координацію між державами; визнання того, що одна країна перебуває в кращому становищі для кримінального переслідування, ніж інша; створення Спільної групи з розслідування; надання Євроюсту інформації, необхідної для виконання його завдань.

По-друге, Євроюст: забезпечує, щоб компетентні органи влади інформували один одного про розслідування і кримінальне переслідування, про які їх було поінформовано; сприяє компетентним органам у забезпеченні максимально ефективної координації розслідувань та судових переслідувань; надає допомогу для поліпшення співробітництва між компетентними національними органами влади; співпрацює і консультується з Європейською судовою мережею, а також використовує її базу даних і вдосконалює свою.

Також Євроюст може здійснювати координацію між компетентними органами і направляти запити про надання правової допомоги, якщо розслідування: (1) проводиться компетентним органом держави-учасниці, (2) стосується конкретної справи і (3) потребує його втручання для координації дій. Крім того, він може допомагати Європолу, зокрема, висновками, ґрунтованими на аналізі, проведеному Європолом, а також надавати матеріально-технічну підтримку, наприклад, у перекладі, тлумаченні та організації координаційних нарад.

Окрім Європолу, Євроюст активно співпрацює з такими організаціями як Європейська судова мережа (European judicial network, EJn), Європейське бюро з боротьби з шахрайством (European Anti-fraud Office, OLAF), Європейська агенція з управління оперативним співробітництвом на зовнішніх кордонах держав-учасниць Європейського Союзу (Frontex) та Європейський поліцейський коледж (European Police College, CEPOL).

Компетенція Євроюсту поширюється на два види правопорушень. По-перше, спочатку до них відносили ті види злочинних діянь та правопорушень, щодо яких компетенцією наділений Європол.

До відповідних злочинів почали зараховувати такі: організована злочинність, тероризм та інші форми тяжких злочинів (незаконний обіг наркотиків, незаконна діяльність з відмивання грошей, злочини, пов'язані з ядерними і радіоактивними речовинами, нелегальне перевезення іммігрантів, торгівля людьми, злочини, пов'язані із транспортними засобами, вбивство, завдання тяжких тілесних ушкоджень, незаконна торгівля органами людей, викрадення людей, незаконне позбавлення волі й захоплення заручників, расизм та ксенофобія, організовані крадіжки і грабіж тощо).

По-друге, компетенція Євроюсту поширюється на інші види злочинів, якщо вони вчинені разом з одним із названих вище, при цьому Євроюст може також допомагати у розслідуванні та кримінальному переслідуванні на прохання держав-учасниць ЄС.

Функції Євроюсту. Євроюст стимулює і покращує координацію розслідувань і судових переслідувань між компетентними органами в державах-учасницях ЄС і покращує співробітництво між компетентними органами держав-учасниць, зокрема шляхом сприяння виконанню міжнародних взаємної правової допомоги та здійснення запитів про екстрадицію.

Крім того, Євроюст може допомагати державам-учасницям ЄС у розслідуванні інших злочинів. Євроюст може просити компетентні органи зацікавлених держав-учасниць:

проводити розслідування або здійснювати конкретні дії; дозволу на координацію їх дій; створити спільну слідчу групу, або забезпечити Євроюст інформацією, необхідною для виконання певних завдань.

Крім того, Євроюст: повинен забезпечити, щоб компетентні органи інформували одне одного про розслідування та звинувачення злочинів, що стосуються іншої сторони;

сприяє компетентним органам у забезпеченні якомога більшої координації розслідувань і судових процесів.

Євроюст співпрацює з 24 країна, що не є членами ЄС: Албанією, Аргентиною, Боснією і Герцеговиною, Єгиптом, Канадою, Республікою Македонією, Ісландією, Ізраїлем, Японією, Кореєю, Ліхтенштейном, Молдовою, Монголією, Чорногорією, Норвегією, Російською Федерацією, Сербією, Сінгапуром, Швейцарією, Таїландом, Туреччиною, Україною і США.

**10. Захист прав й онлайн – завдання та дії.**

Закон про захист прав дітей в Інтернеті (СОРА) і Закон про захист конфіденційності дітей в Інтернеті (СОРРА) Закон про захист від 1998 року (СОРРА) є федеральним законом США прийнятим 21 жовтня 1998 року, 18 років тому.

Акт з 21 квітня 2000 року стосується збору особистої інформації фізичних або юридичних осіб он-лайн, які підпадають під юрисдикцію США дітей у віці до 13 років. У ньому детально вказано, що оператор веб-сайту повинен включити в політику конфіденційності положення про те, коли і як отримувати згоду батьків або опікунів, а також яку відповідальність оператор повинен нести за приватне життя дітей і безпеку в Інтернеті, включаючи обмеження на маркетинг для тих, хто молодше 13 років.

У той час як діти у віці до 13 років можуть легально видавати особисту інформацію за згодою їх батьків, багато веб-сайтів - зокрема, сайти соціальних медіа - забороняють малолітнім дітям використання їхніх послуг в цілому через високу вартість і роботу, пов'язану з дотримання закону.

Федеральна торгова комісія (FTC) має право видавати нормативні акти і забезпечувати дотримання СОРРА. Крім того, відповідно до умов СОРРА, положення "безпечної гавані" FTC призначені для того, щоб стимулювати саморегулювання галузі. Згідно з цим положенням, промислові групи та інші можуть запросити дозвіл Комісії на встановлення саморегулюючих керівних принципів.

У вересні 2011 року Федеральна торгова комісія оголосила пропоновані зміни до правил СОРРА, перші суттєві зміни в акті, оскільки його правила були випущені 2000 року. Запропоновані зміни правил розширили визначення того, що означає "збирати" дані від дітей. Пропоновані правила представили вимоги щодо зберігання і видалення даних, якою постановило, що дані, отримані від дітей, зберігаються лише на кількість часу, необхідного для досягнення мети, з якою вони були зібрана, а також додали вимогу, щоб оператори забезпечили, щоб будь-які треті особи, яким інформація дитини розкрита, мали адекватні засоби для захисту інформації.

Дія цього закону поширюється на веб-сайти і онлайн-сервіси, що працюють в комерційних цілях, або спрямовані на дітей у віці до 13 років або мають фактичне знання, що діти у віці до 13 років надають інформацію в Інтернеті.

Найбільш відомі некомерційні організації звільнені від більшості вимог СОРРА. Проте, Верховний суд постановив, що некомерційні організації, які діяли в інтересах комерційної діяльності своїх членів, підлягають регулюванню FTC і, отже, СОРРА. Та "підтверджена згода батьків", що потрібна перед збором та використанням інформації, наданої дітьми у віці до 13 років, заснована положеннях, викладених в регулюванні Федеральної торгової комісії, які беруть до уваги те, яким чином в даний час зібрано інформацію і шляхи використання даної інформації

Однією із найгостріших проблем взаємодії дитини з інтернетом є небезпека зіткнення з агресивними нападами, які називають кібер-булінгом.

**Кібербулінг** – це жорстокі дії з метою дошкулити, нашкодити, принизити дитину, в яких використовуються інформаційно-комунікаційні засоби: мобільні телефони, електронна пошта, соціальні мережі тощо. Діти часто не розповідають батькам про такі свої негаразди через страх батьківської заборони використання потрібних їм засобів зв’язку, і тому залишаються без необхідної підтримки і допомоги. Особливо небезпечною може стати ситуація, коли дитина потрапляє в ситуацію цькування і в реальному житті і у віртуальному середовищі. Ще недавно проблема кібер-булінгу стосувалась лише старших дітей, сьогодні вона охоплює і молодші класи, адже підвищилася доступність мобільного телефону для дітей, а педагогічних зусиль, спрямованих на підготовку дитячих колективів до конструктивної взаємодії з віртуальним світом, сьогодні явно бракує.

Рішенням уряду федеральної землі Баварія школярам не дозволяється користуватися стільниковим зв’язком на території шкіл – телефони мають бути вимкненими. І не лише під час занять, а й на перервах. У такий спосіб влада намагається стримати поширення серед підлітків матеріалів порнографічного характеру та з елементами насильства і жорстокості.

Міністр освіти Греції заборонив використовувати мобільні телефони у школах. Це обумовлене повальним захопленням учнів знімати на камеру сцени сексуального та хуліганського характеру. Більше того, у створенні відео вони влаштовували своєрідні «мистецькі» змагання.

Французька конституційна рада ухвалила новий закон, що передбачає суворе покарання – позбавлення волі, строком до п’яти років, і штраф у розмірі 75.000 євро – за зйомку реальних сцен насильства та поширення таких відеоматеріалів у мережі Інтернет. Закон стосується усіх, хто не пов’язаний з журналістською діяльністю.

Влада Італії наважилася на сміливий крок і заборонила школярам приносити з собою до школи мобільні телефони. Це було зроблено для того, аби унеможливити проведення відеозйомки ненормального змісту.

Про заборону мобільних телефонів у дитячих навчальних закладах активно заговорили у листопаді 2006 року, коли у Мережі виявився запис, де учні знущаються з однокласника. Невдовзі в Інтернеті почали з’являтися й інші, подібні, відеоролики.

Міністр освіти і науки України Станіслав Ніколаєнко видав наказ «Про використання мобільних телефонів під час навчального процесу» (№ 420 від 24.05.2007 року). Цей документ з 1 вересня 2007 року забороняє і дітям, і дорослим, котрі, відповідно, навчаються і працюють у загальноосвітніх школах та професійно-технічних навчальних закладах використовувати мобільні телефони під час занять. Наказ виданий відповідно до рішення колегій МОН України, МВС України, Міністерства України у справах сім’ї, молоді та спорту – з метою підвищення рівня організації навчально-виховного процесу.

Американський конгресмен від республіканської партії Пітер Кінг підготував законопроект, згідно з яким виробники мобільних телефонів зобов’язані прибрати з апаратів можливість вимкнення звуку під час зйомки фотографій. Кінг зазначив, що підлітки тишком-нишком роблять фотографії своїх друзів чи ворогів у шкільних роздягальнях та душових кімнатах, а потім розміщують цей матеріал в Інтернеті.

В Японії прогресує тенденція забороняти учням використовувати мобільні телефони у навчальних закладах. Взагалі, почалася тотальна боротьба за «мобільну культуру» – у громадських місцях, культурно-мистецьких закладах тощо.

**11. Блокування, фільтрування та видалення незаконного контенту в Інтернеті.**

В багатьох державах, як блокування так і видалення інтернет-матеріалу, часто розглядається аналогічним чином, а в країнах з цільовими законодавчими рамками, часто регулюється тими ж наборами правил.

Були визначені дві основні категорії моделей регулювання.

По-перше, є країни, які не мають конкретного законодавства з питання блокування, фільтрації іусунення незаконного контенту в Інтернеті: немає жодних законодавчих або іншої системи регулювання, введених в дію державою з метою визначення умов і процедур, які повинні дотримуватися тими, хто бере участь в блокуванні, фільтруванні або усуненні матеріалу. Аргумент в цьому контексті часто є неможливість для законодавця йти в ногу з темпами технологічних розробок. Глибинні причини для відсутності законодавчої діяльності також можуть бути знайдені в правових традиціях країни.

При відсутності конкретної або цілеспрямованої правової бази, країни покладаються на існуючі загальні правові рамки, що стосуються не лише Інтернету, щоб ввести обмежене блокування або видалення матеріалів незаконного інтернет-матеріалу. Такий процес діє в таких країнах як Німеччина, Австрія, Нідерланди, Великобританія, Ірландія, Польща, Чехія та Швейцарія.

Оскільки такі країни стають все частіше стикаються з реальністю суперечок щодо контенту в Інтернеті, пов'язаних з відсутністю законодавчого втручання, це представляє проблему. В останні роки використовувалися різні, щоб заповнити пробіл і врегулювати вирішення конкретних проблем. У деяких країнах навіть вирішили об'єднати підходи, зберігаючи в значній мірі нерегульовані рамки, але із законодавчим або політичним втручання в конкретних областях.

У деяких країнах, таких як Великобританія та Албанія, саморегулювання було прийнято приватним сектором, щоб доповнити порожнечу, залишену вибором законодавця не втручатися.

Інші країни, такі як Нідерланди і Німеччина, покладаються на національні суди, щоб забезпечити необхідний баланс між свободою вираження поглядів, з одного боку, і безпекою Інтернету і захистом інших основних прав в максимально можливій мірі.

По-друге, в багатьох країнах законодавець втрутився в цілях створення правової основи конкретно спрямованої на регулювання Інтернету та інших цифрових засобів масової інформації, в тому числі блокування, фільтрація і видалення контенту в Інтернеті. Фінляндія, Франція, Угорщина, Португалія, Росія, Іспанія і Туреччина є прикладами юрисдикцій, які вибрали використання цього нормативного підходу

Регулювання комунікацій і зв’язку в Великобританії і Північної Ірландії здійснює Офіс з комунікацій – орган, створений відповідно до Акту про комунікації 2003 року і діє на підставі національного і міжнародного законодавства, в функції якого входить ліцензування телерадіомовлення, забезпечення доступності в межах країни теле- і радіозв’язку, електронних комунікацій, розвиток конкуренції на ринку телекомунікаційних послуг і зв’язку.

Офіс з комунікацій здійснює розробку стандартів захисту суспільства від протиправної і шкідливої інформації, здатної спонукати до здійснення злочинів, приводити до безладів, тощо. Офіс публікує Кодекс мовлення, обов’язковий для дотримання всіма мовниками, які діють на підставі його ліцензії. Порушення Кодексу мовлення тягне за собою такі санкції, як офіційне попередження, вимога публічного вибачення з боку порушника, штраф.

Обмеження обігу дитячої порнографії та інших непристойних матеріалів в Великобританії здійснюється за допомогою блокування доступу до списку незаконних сайтів, у формуванні якого беруть участь провідні інтернет-провайдери, оператори мобільного зв’язку, правоохоронні органи і громадянське суспільство. Британські інтернет-провайдери передають інформацію про підозрілих користувачів в Фонд Інтернет Спостереження – національну “гарячу лінію” з моніторингу нелегального інтернет-контенту, яка приймає повідомлення про протизаконний інтернет-контент і формує “чорний список”, направляє його інтернет-провайдерам, які, в свою чергу, інформують спеціальні підрозділи поліції, зокрема національний відділ з криміналу (National Crime Squad, NCS).

Провайдерами інтернету блокується кримінальний контент. Наприклад, зображення сексуального насильства над дітьми, пропаганду екстремізму і тероризму, популяризацію наркотиків і анорексії. Також блокують матеріали, що порушують авторські права.

Якщо після проведення незалежної експертизи матеріал визнається незаконним, Фонд інформує інтернет-провайдера, який після видалення зазначеного матеріалу не піддається переслідуванню з боку поліції. З моменту свого створення Фонд видалив більше 26 тис. зображень дитячої порнографії з британських серверів і надав допомогу поліції в порушенні кримінальних справ.

Блокування та видалення матеріалів відбувається з різним ступенем прозорості. Наприклад, сайти, що розміщують в собі заборонений контент, є в чорному списку, з яким може ознайомитися кожен охочий.

Такі сайти блокуються спеціально налаштованими фільтрами, які працюють автономно, без втручання людини. Але є і сайти, які блокуються указом Верховного суду, і ця інформація залишається закритою.

У Франції Міністерством національної освіти здійснюється впровадження систем автоматичного контролю – централізованих фільтрів, які обмежують доступ школярів до сайтів расистської, антисемітської і неофашистською спрямованості.

У Франції діє ефективна система суспільно-державного партнерства для припинення дитячої порнографії. Крім інтернет-сайтів громадських організацій, які розповідають про інтернет-загрози, методах їх нейтралізації і містять “гарячі лінії” для прийому повідомлень про небезпечний контент, кібер-приниження, домаганнях і загрози (e-enfance.org, internetsanscrainte.fr, netecoute.fr, pointdecontact .net), “гаряча лінія” є також у МВС Франції.

У 1998 році Французькою асоціацією інтернет-провайдерів (AFA) був створений портал, який не тільки інформує про інтернет-загрози і способи їх нейтралізації, але також надає можливість залишити повідомлення про виявлені ресурсі, що містять, в тому числі, дитячу порнографію. Доступ до таких ресурсів блокується членами AFA, які отримують оброблену і перевірену інформацію від співробітників порталу.

В 2010 році у Франції було розпочато роботу зі зміни законодавства, спрямовану на вироблення дієвих механізмів припинення дитячої порнографії та кіберзлочинів.

У Канаді cписок матеріалів порнографічного характеру за участю неповнолітніх, поширення яких здійснювалося в рамках юрисдикції правоохоронних і судових органів влади країни відповідно до Кримінального кодексу, формується за результатами судової експертизи.

Блокування зарубіжних інтернет-ресурсів, розташованих поза юрисдикцією канадських правоохоронних органів здійснюється в рамках проекту “Клінфід/Канада” (“Чистий зв’язок”), реалізованого в листопаді 2006 року за сприяння провідних провайдерів Канади та Канадської лінії прийому повідомлень про сексуальну експлуатацію дітей.

Європейський поліцейський офіс (Європол) правоохоронна інституція Європейського Союзу, до сфери повноважень якої належать боротьба транснаціональною злочинністю, торгівлею людьми, нелегальною міграцією, тероризм, незаконною торгівлею автотранспортом, розповсюдженням порнографії, виготовленням фальшивих грошей та інших платіжних засобів, відмиванням грошей, кіберзлочинами.

4 грудня 2009 р. у м.Київ під час саміту Україна - ЄС була підписана Угода між Україною та Європолом про стратегічне співробітництво. Зазначена робота здійснюється у безпосередній взаємодії між Міністерством внутрішніх справ України та Секретаріатом Європолу. З Європолом також досягнуто домовленості щодо укладення Угоди про оперативне співробітництво, яка покликана поглибити відповідну взаємодію сторін. Угода зокрема передбачає налагодження співробітництва між Україною та Європолом з метою підтримки держав-членів Європейського Союзу в попередженні і боротьбі з організованою злочинністю, тероризмом та іншими формами міжнародної злочинності, зокрема шляхом обміну інформацією між Україною та Європолом.

Наразі сторони проводять переговори щодо проекту Угоди про оперативне співробітництво між Україною та Європолом. 11 березня 2015 р. у м.Київ, Європол - 19 березня 2015 р. у м.Гаага підписано Меморандум про взаєморозуміння між Україною та Європолом щодо встановлення захищеної лінії зв'язку. Це дасть можливість здійснювати обмін інформацією між Україною та країнами-членами ЄС через Європол в режимі реального часу та сприятиме поглибленню практичної взаємодії з інституціями ЄС та сприятиме зусиллям держави у боротьбі з транскордонною злочинністю на національному та міжнародному рівнях.

Європейська організація з питань юстиції (Євроюст) була створена рішенням Ради ЄС від 28 лютого 2002 р. з метою посилення боротьби з тяжкими злочинами. Завданням Євроюсту є сприяння органам кримінального переслідування держав-членів ЄС у боротьбі проти серйозної транскордонної злочинності, включаючи комп’ютерні злочини, шахрайство і корупцію, відмивання грошей та злочини проти довкілля. З цією метою Євроюст координує обмін інформацією, надання правової допомоги та процес видачі правопорушників.

Сторонами підготовлено проект Угоди між Україною і Євроюстом та завершено його погодження. Президент Петро Порошенко підписав Закон України "Про основні засади забезпечення кібербезпеки України", прийнятий Верховною Радою України 5 жовтня 2017 року. Закон створює засади національної системи кібербезпеки як сукупності політичних, соціальних, економічних та інформаційних відносин разом із організаційно-адміністративними та техніко-технологічними заходами державного і приватного секторів та громадянського суспільства.

Законом визначено правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, повноваження і обов'язки державних органів, підприємств, установ, організацій, осіб та громадян, основних засад координації їх діяльності, а також базових термінів у сфері кібербезпеки.

Документ також визначає основні об'єкти кіберзахисту, які в сукупності складають критичну інфраструктуру країни, принципи забезпечення кібербезпеки та національна система кібербезпеки. Згідно Закону, Президент України координує діяльність у сфері кібербезпеки через очолювану ним Раду нацбезпеки і оборони України.

Прийняття цього Закону дозволяє впровадити комплексний підхід під егідою держави і у тісному співробітництві з приватним сектором і громадянським суспільством та створює умови для забезпечення кіберзахисту критично важливих інфраструктурних об'єктів України. В Законі враховано низку пропозицій експертів НАТО і Євросоюзу.

Законодавчий акт було розроблено на виконання вимог Стратегії національної безпеки України, затвердженої Указом Президента України від 15.03.2016 № 96 "Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України".

Кіберполіція — структурний підрозділ Національної поліції України, що спеціалізується на попередженні, виявленні, припиненні та розкритті кримінальних правопорушень, механізмів підготовки, вчинення або приховування яких, передбачає використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних та комп'ютерних інтернет-мереж і системі.

10 жовтня 2015 року була створена нова Кіберполіція, як структурний підрозділ Національної поліції. Метою створення Кіберполіції в Україні було реформування та розвиток підрозділів МВС України, що забезпечило підготовку та функціонування висококваліфікованих фахівців в експертних, оперативних та слідчих підрозділах поліції, задіяних у протидії кіберзлочинності, та здатних застосовувати на високому професійному рівні новітні технології в оперативно-службовій діяльності.

Департамент кіберполіції Національної поліції України є міжрегіональним територіальним органом Національної поліції України, який входить до структури кримінальної поліції Національної поліції та відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність.

**Основні завдання Департаменту кіберполіції Національної поліції України:**

1) Участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку.

2) Сприяння у порядку, передбаченому чинним законодавством, іншим підрозділам Національної поліції у попередженні, виявленні та припиненні кримінальніх правопорушень.

**Кібербезпека —** це процес застосування заходів безпеки з метою забезпечення конфіденційності, цілісності та доступності даних.

Інформаційна безпека – це безпека інформації, зазвичай організації чи компанії, у тому числі в ІТ системах. Кібербезпека є частиною Інформаційної безпеки будь-якої організації.

На сьогоднішній день одним з найбільш ефективних методів боротьби з кіберсквотерами є звернення до одного з акредитованих центрів з вирішення доменних спорів Інтернет корпорації з присвоєння імен та номерів (англ. Internet Corporation for Assigned Names and Numbers, далі - «ICANN») .

Вичерпний перелік таких центрів міститься на сайті ICANN, на даний момент до нього входять: Asian Domain Name Dispute resolution Centre; National Arbitration Forum; WIPO; The Czech Arbitration Court Arbitration Center of Internet Disputes; Arab Center for Domain Name Dispute Resolution.

Кожен з цих центрів уповноважений застосовувати адміністративну процедуру згідно з Єдиною політикою вирішення доменних спорів (далі – «UDRP»). Рішення, які буде прийнято в порядку адміністративної процедури, є обов’язковими для акредитованих ICANN реєстраторів доменних імен, а це - всі домени gTLD рівня, тобто .com, .net, .org та інші, окрім того, деякі ccLTD, тобто домени з закінченням .us, co.uk..

UDRP являє собою звід правил, який був розроблений Всесвітньою Організацією Інтелектуальної Власності (далі – «ВОІВ») для швидкого вирішення спорів про доменні імена.

**12. Електронні докази**

У вітчизняному праві юридичну значущість електронного документа закріпили при прийнятті Цивільного кодексу, а також у законах «[Про електронні документи та електронний документообіг](http://zakon2.rada.gov.ua/laws/show/851-15" \t "_blank)» від 22.05.2003 № 851-IV та «[Про електронний цифровий підпис](http://zakon3.rada.gov.ua/laws/show/852-15" \t "_blank)» від 22.05.2003 № 852-IV.

Відповідно до ч.1 ст.5 закону № 851-IV електронним вважається документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов’язкові реквізити документа.

На практиці як такий вид доказів можуть використовуватись аудіо-, відеозаписи, документи бухгалтерської та податкової звітності, що створені, передані, отримані в електронній формі, роздруківки інтернет-сторінок, СМС-листування, листування електронною поштою, публікації в соціальних мережах тощо.

Характерними ознаками електронних доказів є:

1) існування у нематеріальному вигляді;

2) неможливість безпосереднього сприйняття інформації, що обумовлює необхідність використання технічних та програмних засобів для одержання відомостей;

3) наявність технічного носія інформації;

4) можливість копіювання або переміщення на інший носій без втрати своїх характеристик;

5) особливий статус «оригіналу», який може існувати в декількох місцях.

**Електронні засоби доказування —** це передбачені законом процесуальні форми текстової, звукової та візуальної інформації, яка створена та збережена за допомогою технічних та програмних засобів. Отже, до електронних доказів відносяться не лише електронні документи, а й відомості, отримані в мережі Інтернет, аудіо- та відеозаписи, електронні поштові повідомлення.

Подача електронних доказів. За проектом нового Кодексу учасники справи зобов’язані подавати наявні у них докази в порядку та строки, встановлені законом або судом, не приховуючи докази. Процесуальні документи в електронній формі мають подаватися учасниками справи до суду з використанням Єдиної судової інформаційно-телекомунікаційної системи шляхом заповнення форм процесуальних документів відповідно до Положення про Єдину судову інформаційно-телекомунікаційну систему. Проект КАС України врегульовує порядок огляду електронних доказів.

Так, згідно положень ст. 81 проекту КАС, письмові, речові і електронні докази, які не можна доставити в суд, оглядаються за їх місцезнаходженням. В порядку, визначеному цією статтею, суд за заявою учасника справи чи з власної ініціативи може оглянути веб-сайт (сторінку), інші місця збереження даних в мережі Інтернет з метою встановлення та фіксування їх змісту.

Електронний цифровий підпис за правовим статусом прирівнюється до власноручного підпису (печатки) у разі, якщо:

1) електронний цифровий підпис підтверджено з використанням посиленого сертифіката ключа за допомогою надійних засобів цифрового підпису;

2) під час перевірки використовувався посилений сертифікат ключа, чинний на момент накладення електронного цифрового підпису;

3) особистий ключ підписувача відповідає відкритому ключу, зазначеному у сертифікаті (ч. 1 ст. 3 Закону України «Про електронний цифровий підпис»).

В умовах цифрової епохи та швидкого розвитку сучасного світу адміністративне судочинство не може собі дозволити не відповідати реаліям часу, тому в найкоротшій термін наше законодавство повинно відреагувати на виклики реальності цифрового часу, розвиваючись разом зі світом.

**Лекція № 6**

Тема лекції: Захист авторського права в мережі Інтернет

**План лекції**

1. Проблематика визначення системи об’єктів авторського права в Україні.

2. Загальна характеристика розпорядження авторськими правами в мережі Інтернет та особливості їх захисту.

3.Проблемні питання захисту авторських прав в мережі Інтернет технічними засобами.

4. Особливості захисту авторських прав в мережі Інтернет правовими засобами: теорія та практика.

**Література**

* + 1. Закон України «Про інформацію» від 02.10.1992 року // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.
    2. Марущак А.І. Інформаційне право України. Підручник / Марущак А.І. – К.: Дакор, 2011. – 456 с.
    3. Сопілко І. М. Державна інформаційна політика України: стан та шляхи реалізації: монографія / І. М. Сопілко. – К. : МП «Леся», 2014. – 424 с.
    4. B.C.Цимбалюк Основи інформаційного права України / B.C.Цимбалюк, В.Д.Гавловський, В.В.Гриценко та ін. – К.: Видавництво "Знання", 2004
    5. Сопілко І.М. Захист авторських прав в мережі інтернет : монографія / І.М.Сопілко, О.В.Пономаренко. – К. : Комп’ютерпрес, 2013. – 247 с.
    6. [Кульчій](https://www.coursera.org/learn/r-programming/) О.О. Інформаційне право: навчально-методичний посібник для самостійного вивчення навчальної дисципліни підготовки бакалавра спеціальності 081 «Право» [Електронний ресурс] / О.О. Кульчій. – Полтава: ВНЗ Укоопспілки «ПУЕТ», 2015. – Режим доступу: <http://pravo.puet.edu.ua/files/lic2016bac/ip_03.pdf>
    7. Пазюк А.В. Правові засоби захисту та відновлення прав користувачів Інтернету в Україні в контексті застосування Посібника Ради Європи з прав людини для інтернет-користувачів [Електронний ресурс] / А.В. Пазюка. – К. : ФОП Клименко, 2015. – 128 с. – Режим доступу: <https://rm.coe.int/1680599465>
    8. Посібник з прав людини для інтернет-користувачів та пояснювальний меморандум [Електронний ресурс]. - Режим доступу: https://rm.coe.int/16802e3e96

**Зміст лекції**

**1. Проблематика визначення системи об’єктів авторського права в Україні.**

Інтелектуальна власність - це не лише приватноправова категорія, а й сфера, яка становить публічноправовий інтерес. Незважаючи на те, що права інтелектуальної власності відповідно до положень Загальної декларації прав людини, Міжнародного пакту про економічні, соціальні та культурні права розглядаються як основоположні немайнові права людини, все ж нарізі їх не можна сприймати як абсолют, що повною мірою вже підтверджено й судовою практикою.

Складною, але водночас багатогранною видається взаємодія системи права інтелектуальної власності як приватноправової категорії й сфери публічноправових інтересів - мережі Інтернет, управління яким здійснюється одразу на декількох рівнях за участі різних мультистейкхолдерів. Така взаємодія призводить до таких результатів:

- розвиток творчості та технологій, виникнення нових обєктів права

інтелектуальної власності;

- підвищення рівня загрози вчинення порушення прав інтелектуальної власності, виникнення «нетипового» місця вчинення порушення прав -мережа Інтернет;

- взаємопов’язаність прав інтелектуальної власності, інших немайнових прав фізичних та юридичних осіб в мережі Інтернет та особливості їх реалізації, зважаючи на принцип, відповідно до якого там, де закінчуються права на свободу слова й творчості одних осіб, починається право на гарантування поваги до честі, гідності йділової репутації інших осіб.

Незважаючи на відсутність конвенційного визначення «**Інтернет речей»,** дефініція представлена у Комюніке від 18.06.2009 Комісії ЄС до Європейського парламенту, Ради ЄС, Європейського соціально-економічного комітету та Комітету регіонів -«Інтернет речей: план дій для Європи»: інтернет речей - це серія нових незалежних систем, що діють на основі власної внутрішньої інфраструктури, яка частково базується на вже налагодженій інфраструктурі мережі Інтернет, а також може впроваджуватися у поєднанні із новими видами послуг.

Термін “Інтернет речей” (або англійською “Internet of Things”, скорочено – ІоТ) вперше було сформульовано в кінці ХХ-го століття, у 1999 році. Це концепція комунікації об’єктів (“речей”), які використовують технології для взаємодії між собою та з навколишнім середовищем. Також ця концепція передбачає виконання пристроями певних дій без втручання людини. Таким чином, всі пристрої в будинках, в автомобілях, на користувачеві виконують обробку інформації, її аналіз та обмін між собою та, залежно від результатів, приймають рішення і виконують певні дії.

**2. Загальна характеристика розпорядження авторськими правами в мережі Інтернет та особливості їх захисту.**

Особливості захисту авторського права і суміжних прав у мережі Інтернет полягають насамперед у контролі правовласників за використанням об’єктів, який полягає у такому:

– Обмежена функціональність. За такого підходу, власник авторського права надає користувачеві примірник твору, який має функціональні обмеження. Такий підхід є одним із шляхів упровадження в життя таких бізнес-моделей, як „спробуй, перед тим, як купити ” та „продавай поліпшені версії ”.

– „**Годинникова бомба”.** Аналогічно до прийому з функціональними обмеженнями, за цього підходу власник авторських прав розповсюджує функціонально повноцінний об’єкт інтелектуальної власності, але встановлює дату, після якої доступ до нього буде неможливим.

**– Захист від копіювання.** За цього підходу продавець обмежує кількість разів, коли комп’ютерний файл може бути скопійований.

**– Криптографічні конверти.** Це програмне забезпечення, яке зашифровує твори так, що доступ до них може бути отриманий лише із застосуванням належного ключа до шифру.

**– Контракти.** За умови правильного оформлення контракти можуть надати власникам авторського права і суміжних прав ширше повноваження щодо контролю за використанням їхніх творів ніж ті, що надаються їм відповідно до законодавства.

– Запобіжні заходи. Законодавством держав-членів Світової організації торгівлі (СОТ) мають бути передбачені процедури, які передбачають ефективні дії проти будь-якого порушення прав інтелектуальної власності, в тому числі термінові заходи, та способи захисту прав, які стримують від подальших порушень.

Загалом же українці розуміють важливість права інтелектуальної власності, хоча не зовсім готові дотримуватися його, перекладаючи усю відповідальність на владу.

**Завдання ж влади** – дати громадянам такі норми закону, які б відповідали реаліям сьогодення та зберігали такий хиткий баланс інтересів правовласників та користувачів.

**3. Проблемні питання захисту авторських прав в мережі Інтернет технічними засобами.**

З розвитком всесвітньої мережі Інтернет актуальним стає питання дотримання авторських прав користувачами. Враховуючи екстериторіальність мережі, технічний прогрес та динаміку збільшення кількості користувачів можна стверджувати, що міжнародне законодавство у сфері охорони авторського права неспроможне реально захистити права автора твору, розміщеного в мережі.

Що стосується національного законодавства, то воно досі не містить норм, які б відображали специфіку використання та захисту твору в Інтернеті. Це призводить до ще більшого загострення проблеми. Цікаво, що серед фахівців досі немає одностайності з приводу того, чи потрібне законодавче регулювання взагалі.

Тому цілком зрозумілим є факт, що все більшу роль в забезпеченні дотримання авторських прав в Інтернеті відіграє технологія. Автор статті ставить за мету провести аналіз технічних засобів, які дозволяють власникам авторських та суміжних прав ефективно захищати свої права на розміщені в Інтернеті твори до моменту порушення. Об’єктом дослідження є проблеми захисту авторського права в мережі Інтернет, предметом – технічні засоби захисту.

Найбільшої шкоди від порушень зазнають онлайнові бібліотеки з текстовими, музичними та відео файлами, а також веб-сторінки паперових періодичних видань з відкритим доступом до матеріалів номера.

Власники авторських прав мають вибір з широкого кола як технічних, так і правових засобів, контролю за розміщенням в Інтернеті творів до моменту порушення прав на них. Технічні способи захисту авторських прав в Інтернеті ми можемо умовно розподілити на способи ідентифікації об’єктів авторського права та суміжних прав, обмеження доступу, криптографічного перетворення тощо. Застосування способів захисту залежить від характеру твору, що захищається.

Ідентифікація об’єктів авторського права і суміжних прав здійснюється за допомогою ідентифікаційного коду ISBN, цифрового підпису, цифрової марки.

**Ідентифікаційний код ISBN** (Міжнародний стандартний книжковий номер) призначений для захисту фонограм; ISAN – номер, розроблений на Міжнародній конференції товариств авторів і композиторів (CISAC), і дозволяє ефективно захищати фільми та інші аудіовізуальні твори; цифровий ідентифікатор DOI супроводжує твори або їхні частини, дозволяючи у такий спосіб простежити „долю” об’єкта в торговельному обігу; існують й інші програмні коди, що дають можливість порушити цілісність твору при неправильному його використанні.

Що стосується цифрового підпису, то він дозволяє ідентифікувати справжнього автора того або іншого твору, таким чином знімаючи в контрагента будь-які сумніви про те, з ким він має справу.

Найпоширенішою є система так званих „цифрових водяних знаків”, впроваджуваних у твори (тексти, графічні зображення і тощо.) у мережі. Їх перевага полягає в тому, що при звичайному візуальному розгляді зображення користувач не бачить яких-небудь закодованих позначень – значка копірайта ©, імені автора, року видання. однак потім при застосуванні певного програмного засобу можна довести, що файли містять додаткову інформацію, що вказує на особу, яка її записала. Можливе і застосування спеціальних „відбитків”. Вони також дозволяють контролювати використання творів в інформаційних мережах, а при виявленні порушень авторського права і суміжних прав забезпечувати належну доказову базу в суді.

Серед способів захисту авторського права та суміжних прав у мережі Інтернет окремо можна казати на обмеження доступу до матеріалів, що розміщені в Інтернеті, надаючи доступ до Інтернет ресурсу за попередню плату. Можливе також застосування „цифрових конвертів”, що передбачають укладання угоди із власниками тих або інших ресурсів у мережі. Окрім того, можна застосувати методи криптографічного перетворення матеріалів такі, як шифрування, використання якого дозволяє обмежити або повністю виключити можливість копіювання творів (наприклад, система SCMS, що дозволяє виготовити одну копію документа й унеможливлює подальше копіювання цього примірника).

Захистити твір від копіювання можна шляхом встановлення технічної заборони робити копії. Або ж використовуючи метод антикопії, або антикопіювання. Їхній зміст полягає у тому, що на СD-ROM ставиться технічний бар’єр.

Ще одним способом захисту творів від неправомірного використання в Інтернеті є створення web-депозитаріїв, що дозволяють фіксувати об’єкти інтелектуальної власності у мережі Інтернет і закріплювати їх правовий статус, інакше кажучи, які визначають, що та кому належить.Власники авторського права і суміжних прав можуть контролювати використання об’єктів в мережі Інтернет з допомогою: обмеження функціональності. За такого підходу, власник авторського права надає користувачеві примірник твору, який має функціональні обмеження. Такий підхід є одним із шляхів впровадження в життя таких бізнес-моделей як „спробуй, перед тим, як купити” та „продавай поліпшені версії”; використання кодових слів. Оригінальний метод контролю за використанням об’єктів авторського права. Полягає у введенні у текст рідкісних та екзотичних слів за якими можна відстежити використання власного твору;

встановлення так званого ,,таймеру”. Аналогічно до прийому з функціональними обмеженнями, за цього підходу власник авторських прав розповсюджує функціонально повноцінний об’єкт інтелектуальної власності, але встановлює дату, після якої доступ до нього буде неможливим. Один з варіантів такого підходу передбачає закриття продавцем доступу до твору після певної кількості користувань (наприклад, після перегляду комп’ютерного файлу 10 разів його буде неможливо більше продивитися).

захисту від копіювання. За цього підходу продавець обмежує кількість разів, коли комп’ютерний файл може бути скопійований. Захист від копіювання був нормою в 1980-х роках, але пізніше вийшов з ужитку значною мірою тому, що користувачі скаржилися на незручність, а також тому, що захист копії можна було досить легко „зламати”.

Криптографічні конверти – це програмне забезпечення, яке зашифровує твори так, що доступ до них може бути отриманий лише із застосуванням належного ключа до шифру. Програми, що здійснюють таку операцію, часто називають торговою маркою фірми ІВМ “cryptolopes”. Власники прав можуть захищати свої права на твори, розповсюджуючи їх у криптографічних конвертах і вимагаючи від користувачів плати за ключі, за допомогою яких твір можна „вийняти” з „конверта” .

Отже, як ми бачимо, авторам доступне широке коло технічних засобів для захисту авторського права та суміжних прав в мережі Інтернет. Вибір того чи іншого способу залежить від характеру твору, об’єктивної форми існування та встановлених автором меж використання. Однак варто зазначити, що жоден із способів не є повністю ефективним, оскільки зростання комерційної цінності створеного продукту призводить до створення нових способів незаконного копіювання об’єктів авторського права та суміжних прав розміщених в Інтернеті.

Авторське право, як і право інтелектуальної власності в цілому, з огляду на завдання, які воно вирішує, має виключний характер і розглядається як сукупність немайнових (особистих) та майнових прав автора, що надаються йому законом, оголосити себе автором твору: доводити його до відома публіки, відтворювати та розповсюджувати або використовувати його будь-якими іншими способами і засобами, а також дозволяти іншим особам використовувати твір певними способами. В об’єктивному розумінні авторське право, як різновид права інтелектуальної власності, є цивільно-правовим інститутом, який регулює певну зовнішньо і внутрішньо споріднену категорію відносин, пов’язаних зі створенням і використанням творів науки, літератури і мистецтва. У суб’єктивному розумінні авторське право – це сукупність прав, які належать конкретному автору або його правонаступникам та іншим суб’єктам авторського права, у зв’язку зі створенням і використанням твору науки, літератури і мистецтва.

У законодавстві Україні не закріплено визначення поняття «авторське право». У ст. 433 ЦКУ ст. 8 ЗУ «Про авторське право і суміжні права», закріплено, що до об’єктів авторського права відносяться: літературні та художні твори (романи, поеми, статті, та інші письмові твори; лекції, промови,проповіді та інші усні твори; драматичні, музично – драматичні твори, пантоміми, хореографічні, інші сценічні твори; інші групи об’єктів); комп’ютерні програми; компіляції даних (бази даних), якщо вони за добором або упорядкуванням їх складових частин є результатом інтелектуальної діяльності; інші твори. Тобто об’єкти авторського право досить різноманітні і напевно, з розвитком культури і суспільства ще будуть з’являться нові об’єкти. Так з розвитком світової мережі Інтернет, з’явилися такі об’єкт як комп’ютерні програми і компіляції даних.

Відповідно до ст.434 ЦКУ та ст. 10 ЗУ «Про авторське право і суміжні права», не є об’єктом авторського права: а) повідомлення про новини дня або поточні події, що мають характер звичайної прес-інформації; б) твори народної творчості (фольклор); в) видані органами державної влади у межах їх повноважень офіційні документи політичного, законодавчого, адміністративного характеру (закони, укази, постанови, судові рішення, державні стандарти тощо) та їх офіційні переклади; г) державні символи України, державні нагороди; символи і знаки органів державної влади, Збройних Сил України та інших військових формувань; символіка територіальних громад; символи та знаки підприємств, установ та організацій; д) грошові знаки; е) розклади руху транспортних засобів, розклади телерадіопередач, телефонні довідники та інші аналогічні бази даних, що не відповідають критеріям оригінальності і на які поширюється право sui-generis (своєрідне право, право особливого роду).

Крім того, що об’єкти авторського права знаходяться в постійному розвитку, вони потребують якісної охорони. Особливо сильно це питання стало після розвитку і розповсюдження світової мережі Інтернет. Глобальна система стала невід’ємної частиною розвитку суспільства і світу. Насправді, з використанням Інтернету з’являються різноманітні види відносин. Але крім створення нових відносин, реалізацію ряду інших відносин і при всіх інших корисних напрямків, Інтернет став

У 2000 році був виданий Указ Президента України «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» від 31.07.2000 .року. Характеризуючи цей документ слід сказати, що він має декларативний характер, але при цьому визначає основні напрями правового регулювання Інтернет в Україні. Передовсім, це захист авторського права в глобальній мережі.

Найпоширенішими видами порушень в мережі Інтернет є: незаконне відтворення і копіювання музичних, художніх, літературних творів чи комп’ютерних програм без попереднього надання на це згоди автором чи правовласником. Це виражає порушення матеріальних прав авторів. Крім цього, все популярніше становиться такий вид порушень як плагіат. Такі порушення в мережі Інтернет порушують матеріальні і нематеріальні права авторів.

Франція, перша країна, яка оголосила боротьбу з піратством в мережі Інтернет, шляхом прийняття Закону «Про три кроки», який був розроблений за ініціативою президента Франції Ніколя Саркозі і вступив у дію з 1 жовтня 2010 року. Завдяки цьому влада отримала право на повне прослуховування трафіку, а також на сповіщення по електронній пошті тих, хто активно викачує з мережі піратські програми та мультимедійний контент у файлообмінних мережах. Закон передбачив, що «пірати», які ігнорують попередження електронною поштою, втрачають доступ до мережі терміном на рік, крім того в ряді випадків передбачений штраф до 300 тис євро або навіть тюремне ув’язнення. Закон також зобов’язав місцевих інтернет-провайдерів перехоплювати і передавати владі дані про людей, які займаються розповсюдженням піратських матеріалів. Щодо цих осіб в подальшому порушуються кримінальні справи.

Іван Римаренко у своїй роботі «Захист авторських прав та творів, розміщених в Інтернеті, визначає два шляхи для захисту авторський прав і мережі Інтернет.

Захист на етапі до порушення: 1) обмежена функціональність – автори розповсюджують програми, які не здатні друкувати документи або зберігати їх у пам’яті комп’ютера; 2) «годинникова бомба» – автор розповсюджує повноцінний об’єкт авторського права, але встановлює дату, після якої доступ до нього буде неможливим; 3) захист від копіювання, тобто автор встановлює кількість разів, коли файл може бути скопійований; 4) криптографічні конверти – твір зашифровано так, що доступ до нього можливий з використанням ключа до шрифту; 5)контракти-угоди «наскрізного клацання» укладені через Інтернет, це – дозволи автора на використання творів; 6) запобіжні заходи: попередня публікація матеріалу на традиційному матеріалі, підтвердження факту існування твору на певну дату, засвідчення в нотаріуса дати створення твору, запис на лазерному диску і поміщення в архів або веб-депозитарій; 7) клірингові центри – автор надає центру право ліцензувати свої права на твір, центр приймає плату від користувача і передає її володільцеві авторських прав.

Захист на етапі після порушення: 1) агенти – це комп’ютерні програми, які автоматично виконують попередньо визначені команди, наприклад, пошук у мережі контрафактних примірників творів; 2) стенографія – процес приховування інформації у файлах, наприклад «водяного знаку» автору твору, що буде доказом авторства цієї особи щодо цього твору; 3) «маячок» – це особлива мітка, яка розміщується в творі і спрацьовує під час несанкціонованого використання, надаючи можливість знайти порушника авторських прав; 4) використання кодових слів.

Застосування таких заходів захисту авторських прав в мережі Інтернет і справді зможе забезпечити належний захист, але для реалізації таких заходів необхідна підтримка з боку держави і ряд інших дій. Отже, сьогоднішні тенденції рухаються в бік саме мережі Інтернет, де зберігаються невизначена кількість об’єктів інтелектуальної власності, що потребують правової допомоги. Необхідно внести зміни в національне законодавство, а можливо і прийняття нового законодавчого акту з питань захисту авторських прав в мережі Інтернет. Більшість країн Європи вже займаються цими питаннями і частково можуть контролювати процеси і забезпечити захист прав авторів в мережі Інтернет.

**4. Особливості захисту авторських прав в мережі Інтернет правовими засобами: теорія та практика.**

Інтелектуальна власність - це не лише приватноправова категорія, а й сфера, яка становить публічноправовий інтерес. Незважаючи на те, що права інтелектуальної власності відповідно до положень Загальної декларації прав людини, Міжнародного пакту про економічні, соціальні та культурні права розглядаються як основоположні немайнові права людини, все ж нарізі їх не можна сприймати як абсолют, що повною мірою вже підтверджено й судовою практикою.

Складною, але водночас багатогранною видається взаємодія системи права інтелектуальної власності як приватноправової категорії й сфери публічно-правових інтересів - мережі Інтернет, управління яким здійснюється одразу на декількох рівнях за участі різних мультистейкхолдерів. Така взаємодія призводить до таких результатів: розвиток творчості та технологій, виникнення нових обєктів права інтелектуальної власності; підвищення рівня загрози вчинення порушення прав інтелектуальної власності, виникнення «нетипового» місця вчинення порушення прав -мережа Інтернет; взаємопов’язаність прав інтелектуальної власності, інших немайнових прав фізичних та юридичних осіб в мережі Інтернет та особливості їх реалізації, зважаючи на принцип, відповідно до якого там, де закінчуються права на свободу слова й творчості одних осіб, починається право на гарантування поваги до честі, гідності йділової репутації інших осіб.

Усвідомлюючи особливості такої взаємодії, держави вже сьогодні взялися до адаптації законодавства в сфері охорони та захисту прав інтелектуальної власності, зважаючи на виклики цифрового середовища.

Незважаючи на відсутність конвенційного визначення «Інтернет речей», дефініція представлена у Комюніке від 18.06.2009 Комісії ЄС до Європейського парламенту, Ради ЄС, Європейського соціально-економічного комітету та Комітету регіонів -«Інтернет речей: план дій для Європи»:

Незважаючи на різні форми використання знаків для товарів і послуг в мережі Інтернет, їх призначення залишається аналогічним - з метою ідентифікації та вирізнення товарів і послуг одних осіб від товарів і послуг інших осіб.

Використання знаків для товарів і послуг не врегульоване на універсальному рівні, а відповідні норми вміщені в національних законодавствах різних держав. У більшості юрисдикцій панує підхід, відповідно до якого знаки для товарів і послуг, які використовуються в кіберпросторі, отримують такий же рівень захисту, як і при їх використанні в реальному світі, що надає можливість споживачам зробити обміркований вибір товарів та послуг в мережі Інтернет. Зокрема, в національному законодавстві України: згідно з ч. 4 ст. 16 Закону України «Про охорону прав на знаки для товарів і послуг», використанням знака визнається, в тому числі, застосування його вділовій документації чи в рекламі та в мережі Інтернет. Використання знаку для товарів і послуг вякості елементу доменного імені Найрозповсюдженішим способом використання знаків для товарів і послуг в мережі Інтернет - це їх використання в якості елементів доменного імені.

**Домен** - це область простору ієрархічних імен мережі Інтернет, яка обслуговується набором серверів доменних імен (DNS) й централізовано адмініструється доменним ім’ям.

-**Доменне ім’я** - це адреса мережевого сполучення, яка ідентифікує власника адреси.

В національних законодавствах різних юрисдикцій вміщено дефініції «доменне ім’я». Відповідно до ст. 1 Закону України «Про охорону прав на знаки для товарів і послуг», доменне ім'я - це ім’я, що використовується для адресації комп'ютерів і ресурсів в Інтернеті. Згідно зі ст. 1 Закону України «Про телекомунікації» адреса мережі Інтернет - це визначений чинними в Інтернеті міжнародними стандартами цифровий та/або символьний ідентифікатор доменних імен в ієрархічній системі доменних назв.

Переважна більшість спорів, що стосуються захисту прав інтелектуальної власності в мережі Інтернет, вирішуються саме у досудовому порядку шляхом направлення декількох попереджувальних листів (C&D letters): лист на ім’я реєстранта веб-сайта; лист на ім’я реєстратора веб-сайта; лист на ім’я адміністратора публічного домену; лист на ім’я хостинг-провайдера.

Відомості, які зазначаються у попереджувальних листах: предмет (порушення прав інтелектуальної власності на об’єкти авторських прав/на знак для товарів і послуг); URL-адреса й матеріали сторінок, на яких вчинено порушення; докази наявності у особи авторських прав та/або прав власності на знак для товарів і послуг; формальні вимоги (засоби зв’язку, підпис, довіреність).

У випадку, якщо умови, зазначені у попереджувальних листах, не виконуються й порушення прав інтелектуальної власності не припиняється, правовласнику слід застосовувати судові механізми захисту порушених прав.

Найчастіше спори, що стосуються обєктів права в мережі Інтернет, між сторонами виникають з таких питань: спільні проекти; авторські договори; угоди про фінансування; дистриб’юторські угоди; угоди про сповіщення; ліцензійні договори; договори страхування; договори зі ЗМІ; договори про володіння і користування майном, що є спільною власністю; положення про конфіденційність і нерозголошення інформації.

З огляду на це, особливої ваги набуває діяльність Центру арбітражу й медіації ВОІВ. Обрання такого способу вирішення спорів став можливий, починаючи з 1994 року, коли за ініціативи ВОІВ було створено відповідний орган в Швейцарії.

Основними процедурами, доступними для сторін, які звертаються до Центру арбітражу й медіації ВОІВ, є: медіація (процедура, за якої незалежний посередник - медіатор - сприяє вирішенню спорів між сторонами); арбітраж (процедура, яка передбачає передачу спору на розгляд одного чи декількох арбітрів, які приймають рішення, яке є обов’язковим до виконання для сторін); пришвидшена процедура арбітражу (процедура вирішення спору відбувається значно швидше й є більш заощадливою з точки зору залучених коштів); тощо.

Особливості визначення міжнародної підсудності: Інтернет - глобальна мережа, виникнення порушення прав інтелектуальної власності можливе у будь-якій юрисдикції; Всесвітньою організацією інтелектуальної власності (WIPO) визначено ряд факторів, які впливають на визначення юрисдикції для вирішення спорів щодо порушення прав інтелектуальної власності в мережі Інтернет: обслуговування клієнтів на території держави; наявність інших комерційних відносин із третіми особам на території держави; фактичні відвідування веб-сайту, пов’язані із правопорушенням; - використання мови держави; зазначення цін в національній валюті держави; зазначення адреси чи контактного номера телефона у певній державі; - діяльність, яка не пов’язана із кіберсередовищі, на території держави.

**Механізм Notice-and-takedown** передбачає здійснення третьою особою повідомлення хостинг-провайдера (наприклад, соціальної мережі, певної торгівельної он-лайн платформи або просто компанії, яка надає послуги хостингу для певного веб-сайту) щодо наявності незаконно розміщеного контенту в мережі Інтернет, а також подальше вжиття заходів (блокування/видалення) хостінг-провайдером відповідного контенту, який є незаконним із тих чи інших причин (наприклад, порушення прав інтелектуальної власності, порушення прав дитини тощо).

Основна мета застосування механізму - швидка реакція на порушення прав та основоположних свобод (в тому числі, прав інтелектуальної власності, немайнових прав фізичної й юридичної особи); забезпечення принципу правової визначеності для надавачів послуг проміжного характеру.

**Лекція № 7**

Тема лекції: Право міжнародних комунікацій

**План лекції**

1. Поняття «комунікацій» і «телекомунікацій»: спільне та відмінне. 2. Комунікації як технологія й економічна діяльність.

3. Міжнародне право й міжнародні комунікації.

4. Пошта. Всесвітній поштовий союз.

5. Сучасні двосторонні угоди в поштовій сфері.

6. Підводні телекомунікаційні кабелі. Міжнародне право про підводні телекомунікаційні кабелі.

7. Світова організація торгівлі й телекомунікації.

8. Міжнародний союз електрозв’язку: загальний огляд. Регламент міжнародного електрозв’язку.

9. Радіочастотний ресурс і геостаціонарні орбіти.

10. Спеціалізовані й надзвичайні телекомунікації. Регулювання міжнародних (теле)комунікацій на регіональному та національному рівнях.

**Література**

* + 1. Закон України «Про інформацію» від 02.10.1992 року // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.
    2. Марущак А.І. Інформаційне право України. Підручник / Марущак А.І. – К.: Дакор, 2011. – 456 с.
    3. Сопілко І. М. Державна інформаційна політика України: стан та шляхи реалізації: монографія / І. М. Сопілко. – К. : МП «Леся», 2014. – 424 с.
    4. B.C.Цимбалюк Основи інформаційного права України / B.C.Цимбалюк, В.Д.Гавловський, В.В.Гриценко та ін. – К.: Видавництво "Знання", 2004
    5. [Кульчій](https://www.coursera.org/learn/r-programming/) О.О. Інформаційне право: навчально-методичний посібник для самостійного вивчення навчальної дисципліни підготовки бакалавра спеціальності 081 «Право» [Електронний ресурс] / О.О. Кульчій. – Полтава: ВНЗ Укоопспілки «ПУЕТ», 2015. – Режим доступу: <http://pravo.puet.edu.ua/files/lic2016bac/ip_03.pdf>
    6. Пазюк А.В. Правові засоби захисту та відновлення прав користувачів Інтернету в Україні в контексті застосування Посібника Ради Європи з прав людини для інтернет-користувачів [Електронний ресурс] / А.В. Пазюка. – К. : ФОП Клименко, 2015. – 128 с. – Режим доступу: <https://rm.coe.int/1680599465>
    7. Посібник з прав людини для інтернет-користувачів та пояснювальний меморандум [Електронний ресурс]. - Режим доступу: https://rm.coe.int/16802e3e96

**Зміст лекції**

**1. Поняття «комунікацій» і «телекомунікацій»: спільне та відмінне.**

В національних законодавствах різних юрисдикцій вміщено дефініції «доменне ім’я». Відповідно до ст. 1 Закону України «Про охорону прав на знаки для товарів і послуг», доменне ім'я - це ім’я, що використовується для адресації комп'ютерів і ресурсів в Інтернеті. Згідно зі ст. 1 Закону України «Про телекомунікації» адреса мережі Інтернет - це визначений чинними в Інтернеті міжнародними стандартами цифровий та/або символьний ідентифікатор доменних імен в ієрархічній системі доменних назв.

В основу систему доменних імен покладено винайдення мережі Інтернет, в якій замість складних для запам’ятовування IP-адрес почали використовуватися прості та зручні для використання посилання, які надавали можливість вміщувати позначення, зареєстроване в якості знаку для товарів і послуг. Таким чином, доменні імена почали вважатися одним із основних засобів для просування правовласниками власного бренду. Згодом з’являється ієрархічна система доменних імен (Domain Name System - DNS).

Інвестування в популяризацію доменного імені наразі є найбільш популярним способом збільшення вартості знаку для товарів і послуг в цілому.

**Телекомуніка́ції**([англ.](https://uk.wikipedia.org/wiki/%25D0%2590%25D0%25BD%25D0%25B3%25D0%25BB%25D1%2596%25D0%25B9%25D1%2581%25D1%258C%25) Telecommunications) - це передавання та/або приймання [знаків](https://uk.wikipedia.org/wiki/%D0%97%D0%BD%D0%B0%D0%BA), [сигналів](https://uk.wikipedia.org/wiki/%25), [письмового](https://uk.wikipedia.org/wiki/%D0%9F%D0%B8%D1%81%D1%8C%D0%BC%D0%BE) [тексту](https://uk.wikipedia.org/wiki/%D0%A2%D0%B5%D0%BA%D1%81%D1%82), [зображень](https://uk.wikipedia.org/wiki/%D0%97%D0%BE%D0%B1%D1%80%D0%B0%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F) та [звуків](https://uk.wikipedia.org/wiki/%D0%97%D0%B2%D1%83%D0%BA) або повідомлень будь-якого роду дротовими, [радіо](https://uk.wikipedia.org/wiki/%D0%A0%D0%B0%D0%B4%D1%96%D0%BE), [оптичними](https://uk.wikipedia.org/wiki/%D0%9E%D0%BF%D1%82%D0%B8%D0%BA%D0%B0) або іншими електромагнітними системами.

Телекомунікація виникає при обміні інформацією між учасниками з використанням технологій. Передача відбувається або за допомогою електрики, що проходить через фізичному носії, такий як кабель, або за допомогою електромагнітного випромінювання. Зазвичай, шляхи передачі розділяють на канали зв'язку, що дозволяє користуватись перевагами [мультиплексування](https://uk.wikipedia.org/wiki/%D0%9C%D1%83%D0%BB%D1%8C%D1%82%D0%B8%D0%BF%D0%BB%D0%B5%D0%BA%D1%81%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1). Термін часто використовується в множині, тобто телекомунікації, тому що для передачі використовуються багато різних технологій.

Ранні засоби зв'язку на відстані включали візуальні сигнали, такі як маяки, димові сигнали, [оптичний телеграф](https://uk.wikipedia.org/wiki/%D0%9E%D0%BF%D1%82%D0%B8%D1%87%D0%BD%D0%B8%D0%B9_%D1%82%D0%B5%D0%BB%D0%B5%D0%B3%D1%80%D0%B0%D1%84), сигнальні прапорці та [світлосигнальні геліографи](https://uk.wikipedia.org/wiki/%D0%93%D0%B5%D0%BB%D1%96%D0%BE%D0%B3%D1%80%D0%B0%D1%84_%D1%81%D0%B2%D1%96%D1%82%D0%BB%D0%BE%D1%81%D0%B8%D0%B3%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9). Іншими прикладами до-сучасних засобів зв'язку на відстані включали звукові повідомлення, такі як бій в [барабан](https://uk.wikipedia.org/wiki/%D0%91%D0%B0%D1%80%D0%B0%D0%B1%D0%B0%D0%BD), гра на [горні](https://uk.wikipedia.org/wiki/%D0%93%D0%BE%D1%80%D0%BD_(%D0%BC%D1%83%D0%B7%D0%B8%D1%87%D0%BD%D0%B8%D0%B9_%D1%96%D0%BD%D1%81%D1%82%D1%80%D1%83%D0%BC%D0%B5%D0%BD%D1%82)) або трембіті. У 20-му та 21-му століттях для телекомунікації на відстані зазвичай використовують електричні та електромагнітні технології, такі як [телеграф](%22ht), [телефон](https://uk.wikipedia.org/wiki/%D0%A2%D0%B5%D0%BB%D0%B5%D1%84%D0%BE%D0%BD%D0%BD%D0%B8%D0%B9_%D0%B7%D0%B2'%D1%8F%D0%B7%D0%BE%D0%BA%22%20%5Co%20%22), [телетайп](https://uk.wikipedia.org/wiki/%D0%A2%D0%B5%D0%BB%D0%B5%D1%82%D0%B0%D0%B9%D0%BF), [телекомунікаційні мережі](https://uk.wikipedia.org/wiki/%D0%A2%D0%B5%D0%BB%D0%B5%D0%BA%D0%BE%D0%BC%D1%83%D0%BD%D1%96%D0%BA%D0%B0%D1%86%D1), [радіозв'язок](https://uk.wikipedia.org/wiki/%D0%A0%D0%B0%D0%B4%D1%96%D0%BE%D0%B7%D0%B2'%D1%8F%D0%B7%D0%BE%D0%BA), [радіорелейний зв'язок](https://uk.wikipedia.org/wiki/%D0%A0%D0%B0%D0%B4%D1%96%D0%BE%D1%80%D0%B5%D0%BB%D0%B5%D0%B9%D0%BD%D0%B8%D0%B9_%D0%B7%D0%B2'%D1%8F%D0%B7%D0%BE%D0%BA), [оптоволоконний](https://uk.wiki) та [супутниковий зв'язок](https://uk.wikipedia.org/wiki/%25D0%25A1%25D1%2583%25D0%25BF%25D1%258).

**2. Комунікації як технологія й економічна діяльність.**

Менеджмент – це процес, який забезпечує виконання людьми певних дій, і основою цього процесу є комунікації.

Проблема ефективних комунікацій – одна з ключових у діяльності керівників, оскільки з їх допомогою здійснюється обмін повідомленнями, що виражені різними символами і мають певне смислове навантаження. Комунікації – це обмін інформацією, на основі якої керівник отримує дані, необхідні для прийняття рішень, і доводить їх до працівників організації.

**Ефективна комунікація (тобто така, яка приводить до бажаного типу поведінки адресата) має 4 стадії:**

1. Забезпечення уваги адресата (забезпечення готовності адресата до прийняття інформації). Процес комунікації може перерватися вже на першій стадії, якщо відправник не може подолати конкуренцію повідомлень, під якою розуміють одночасне дію на адресата кількох джерел інформації.

2. Забезпечення розуміння суті повідомлення. Багато комунікацій на цій стадії зазнають краху, тому менеджер, використовуючи канали зворотного зв'язку, повинен переконатися в розумінні підлеглими суті повідомлення.

3. Визнання. Цей етап передбачає забезпечення готовності адресата виконати те, що потрібно від нього у зв'язку з отриманим повідомленням.

4. Дія. Це останній етап ефективної комунікації. Він передбачає виконання адресатом певних дій на основі повідомлених вимог. Найбільш ефективним способом реалізації цього етапу є переконання підлеглих у наявності зв'язку між цілями організації і потребами працівників.

**Комунікація** – це процес обміну інформацією, що включає суб'єкти комунікації (відправника і одержувача), спосіб комунікації і об'єкт комунікації (передану інформацію).

Комунікаційні потреби організації залежать від: характеристик зовнішнього середовища організації (її динамічності, складності, невизначеності); завдань, що вирішуються організацією (наприклад, якщо ставиться завдання випустити якісно новий товар, захопити нові ринки збуту, здійснити модернізацію виробництва, диверсифікацію діяльності, то потреба в комунікаціях різко зростає); основних характеристик організації – масштабів, структури, сфери діяльності, характеру виробленої продукції (послуг), ступеня диверсифікації, позиції в галузі і т. д.

Засоби комунікації включають технічні засоби зв'язку (телефон, телефакс, телекс, пошту, електронну пошту), а також службові записки, звіти, довідкові та рекламні матеріали.

Класифікація комунікацій здійснюється залежно від: засобів комунікації; цілей і завдань, що вирішуються в процесі комунікацій; суб'єктів комунікації (зовнішніх і внутрішніх).

Виділяють два великі класи комунікації з подальшою деталізацією: комунікації між організацією та її зовнішнім середовищем (зовнішні комунікації); комунікації між рівнями і підрозділами організації (внутрішні комунікації).

До них відносяться комунікації по висхідній, між різними відділами, керівник-підпеглий, комунікації між керівником і працюючої групою, неформальні комунікації.

Зовнішні комунікації – це обміни інформацією між організацією та її зовнішнім середовищем. Будь-яка організація існує не ізольовано, а у взаємодії зі своєю зовнішнім середовищем.

Внутрішні комунікації поділяються на два типи комунікацій: формальні і неформальні. Формальні комунікації передбачені організаційною структурою. Під формальними комунікаціями розуміють інформаційний обмін, який здійснюється між елементами організації. Вони діляться на вертикальні, горизонтальні та діагональні.

До вертикальних комунікацій належать комунікації зверху вниз і знизу вгору, тобто інформація передається зверху від керівництва до підлеглих. Таким чином, працівникам організації повідомляють про нові стратегічні і тактичні цілі, конкретні завдання на певний період, зміни правил, інструкцій.

Якщо організація складається з декількох підрозділів, яким необхідно узгоджувати свої дії, то це викликає в них необхідність обмінюватися між собою інформацією. Таким чином, виникає необхідність у горизонтальних комунікаціях. Ці комунікації здійснюються між особами, які знаходяться на одному рівні ієрархії. Такий обмін інформацією забезпечує координацію діяльності (наприклад, між віце-президентами з маркетингу, фінансів, виробництва).

Діагональні комунікації здійснюються між особами, які перебувають на різних рівнях ієрархії (наприклад, між лінійними і штабними підрозділами, коли штабні служби керують виконанням певних функцій).

Комунікаційний процес – це обмін інформацією між двома або більшою кількістю людей.

**Основні функції комунікаційного процесу** полягають у досягненні соціальної спільності при збереженні індивідуальності кожного з її елементів.

**Основна мета комунікаційного процесу** – забезпечення розуміння інформації, яка є предметом обміну, тобто повідомлень. Однак сам факт обміну інформацією не гарантує ефективність спілкування людей, які брали участь в обміні. Процес комунікації представляє процес руху інформації в ланцюг "відправник – канал – одержувач".

**У процесі обміну інформацією можна виділити вісім базових елементів:**

1. Відправник – передавач, що генерує ідеї або збирає інформацію і передає її. Ним може бути індивід або група разом працюючих людей. Під час обміну інформацією відправник і одержувач проходять кілька взаємозалежних етапів: зародження ідеї, кодування і вибір каналу, передача, декодування. Обмін інформацією починається з формулювання ідеї або відбору інформації.

2. Кодування – це процес перетворення ідей у символи, зображення, малюнки, форми, звуки, мова тощо. Тобто, перш ніж передавати ідею, відправник повинен за допомогою символів закодувати її, використавши для цього слова, інтонації, жести (мова тіла) і надати ідеї гарну "упаковку". Таке кодування перетворює ідею в повідомлення.

3. Повідомлення – це сукупність символів, власне інформація, яка закодована за допомогою символів і передається одержувачу. Саме заради цього і здійснюється акт комунікації. Багато повідомлень передається у формі символів мови. Однак символи можуть бути і невербальними, наприклад, графічні зображення, жести, міміка та інші рухи тіла.

4. Канали передачі – засоби, за допомогою яких сигнал спрямовується від відправника до одержувача. Канапи поділяються на засоби масової інформації та міжособистісні канапи. Відправник повинен вибрати канал: передача промовою та письмові матеріали, електронні засоби зв'язку, електронна пошта, відеоплівки та відеоконференції.

5. Декодування – процес, за допомогою якого одержувач повідомлення переводить отримані символи в конкретну інформацію і інтерпретує її значення.

6. Одержувач – цільова аудиторія або особа, якій призначається інформація і яка її інтерпретує.

7. Відгук – сукупність реакції обмежувача повідомлення після ознайомлення з його змістом. Можна спостерігати три основні типи результатів комунікації: зміни в знаннях одержувача, зміна установок одержувача, зміни поведінки одержувача повідомлення. З точки зору керівника, обмін інформацією слід вважати ефективним, якщо одержувач продемонстрував розуміння ідеї, проводячи дії, яких очікував відправник.

8. Зворотний зв'язок – частина відгуку одержувача, який надходить відправнику. Характеризує ступінь розуміння або нерозуміння інформації. Зворотний зв'язок може бути вербальний і невербальний (усмішка, кивок, потиск руки, негативний жест і т.п.).

**3. Міжнародне право й міжнародні комунікації.**

Міжнародно-правове регулювання телекомунікацій сильно залежить не лише від їхніх технологічних параметрів (дротові, бездротові, супутникові, підводні тощо), але й від економічних умов їхнього функціонування й експлуатації

Як розвиток (теле)комунікацій вливає на міжнародне право за межами норма, що їм безпосередньо присвячені.

З метою надання офіційного статусу взаємодії підрозділів між країнами СНД підписана і є чинною Угода про співробітництво держав - учасниць Співдружності Незалежних Держав у боротьбі зі злочинами у сфері комп'ютерної інформації від 1 червня 2001 року.

Правопорушниками, викритими на території України, використовувалися підроблені банківські платіжні картки, окрім українських, ще й банківських установ Російської Федерації, країн Балтії, США, Великої Британії, Італії, Франції та інших. З відповідними правоохоронними підрозділами поліції цих країн маємо контакти.

Протягом 2002-2005 років наші підрозділи проводили перевірки щодо протиправних дій з використанням комп'ютерних та інтернет-технологій за запитами Польщі, Італії, Білорусії, Великої Британії, Греції, Ірландії, Латвії, Німеччини, Норвегії, Російської Федерації та США.

Підрозділами було ініційовано та направлено запити на проведення перевірок чи оперативних заходів до Австралії, Великої Британії, Латвії, Російської Федерації, США, Швеції та Японії. Повні відповіді отримано від правоохоронних органів Австралії, Великої Британії та Швеції. Часткові відповіді - від США та Японії.

**4. Пошта. Всесвітній поштовий союз.**

**По́шта (від**[**лат.**](https://uk.wikipedia.org/wiki/%D0%9B%D0%B0%D1%82%D0%B8%D0%BD%D1%81%D1%8C%D0%BA%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0)**posta)**— установа для транспортування повідомлень (наприклад [листів](https://uk.wikipedia.org/wiki/%D0%9B%D0%B8%D1%81%D1%82_(%D0%BF%D0%BE%D1%88%D1%82%D0%BE%D0%B2%D0%B5_%D0%B2%D1%96%D0%B4%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F)), [листівок](https://uk.wikipedia.org/wiki/%D0%9F%D0%BE%D1%88%D1%82%D0%BE%D0%B2%D0%B0_%D0%BB%D0%B8%D1%81%D1%82%D1%96%D0%B2%D0%BA%D0%B0)), дрібних товарів, частково людей. Найчастіше вона є державною установою. Більшість поштових організацій перебувають у [Всесвітньому поштовому союзі](https://uk.wikipedia.org/wiki/%D0%92%D1%81%D0%B5%D1%81%D0%B2%D1%96%D1%82%D0%BD%D1%96%D0%B9_%D0%BF%D0%BE%D1%88%D1%82%D0%BE%D0%B2%D0%B8%D0%B9_%D1%81%D0%BE%D1%8E%D0%B7).

[**Всесвітній Поштовий Союз**](http://www.upu.int/en.html%22%20%5Ct%20%22_blank) (анг. Universal Postal Union, UPU) є спеціалізованою установою ООН.

Метою діяльності є організація та поліпшення діяльності поштової служби в усьому світі та забезпечення міжнародного співробітництва у цій сфері з тією метою, щоб полегшити спілкування між людьми по всьому світу.

ВПС об’єднує країни-члени в єдину поштову територію і є головним форумом для співпраці між поштовими службами, на якому виробляються принципи організації і функціонування міжнародного поштового обміну.

Всесвітній Поштовий Конгрес як правило збирається кожні чотири роки, а його основною функцією є законодавча, а також розгляд загальних політичних питань. До інших функцій Конгресу належить вибір Генерального Директора та його заступника, так само, як і членів Виконавчої Ради та Ради Поштових Операцій; Конгрес також встановлює бюджет на наступні п’ять років.

Адміністративна рада (анг. Council of Administration) складається з Голови та представників 40 країн-членів та збирається щороку у штаб-квартирі ВПС у Берні.

Вона забезпечує безперервність роботи ВПС між Конгресами, здійснює нагляд над діяльністю ВПС та вивчає регулятивні, законні, адміністративні, та законодавчі питання роботи Союзу. Адміністративна рада також має право здійснювати дії в межах своєї компетенції, які, на її думку, необхідні для вирішення тимчасових справ. Рада затверджує бюджет та рахунки ВПС, а також щорічно доповнює Програму діяльності Союзу. Вона також відповідальна за сприяння та координацію технічної допомоги між країнами-членами. Обов’язки голови Адміністративної Ради автоматично надаються країні, де проходив останній Конгрес.

**5. Сучасні двосторонні угоди в поштовій сфері.**

оловним документом Всесвітнього Поштового Союзу є його Конституція ВПС, який містить мету діяльності та загальні положення. Він є дипломатичним документом, який має бути ратифікований компетентними органами кожної країни-члена ВПС. Доповнення до Статуту можуть вноситись лише Конгресом, і також підлягають ратифікації.

Загальні правила, що регулюють міжнародні поштові послуги, а також положення, що стосуються відправки листів, втілені у Всесвітній Поштовій Конвенції. Цей документ, так само, як і Статут, має обов'язкову юридичну силу для всіх країн-членів ВПС. З метою чіткого, простого та гнучкого регулювання діяльності у сфері міжнародних поштових послуг, на Сеульському Конгресі у [1994](https://uk.wikipedia.org/wiki/1994%22%20%5Co%20%221994) році було внесено доповнення до двох головних документів. Тепер дозволяється вносити зміни до положень щодо міжнародних поштових послуг, не звертаючись до Конгресу.

Окремі угоди, які є обов'язковими лише для країн, що їх уклали або приєднались, регулюють операції з поштовими посилками та поштовими фінансовими службами.

У 2013 році Україна є членом наступних керівних органів ООН та спеціалізованих установ системи ООН: Комісії ООН з права міжнародної торгівлі (ЮНСІТРАЛ) (2010-2014 рр.), Комісії із соціального розвитку (2012-2015 рр.), Комісії з наркотичних засобів (2012-2015 рр.), Комітету з внесків (2013-2015 рр.), Виконавчої ради Структури ООН з питань гендерної рівності та розширення прав і можливостей жінок «ООН-Жінки» (2011-2013 рр.), Комітету з інформації (2013-2014 рр.), Ради Організації ООН з промислового розвитку (ЮНІДО) (2010-2013 рр.), Адміністративної ради та Ради поштової експлуатації Всесвітнього поштового союзу (2013-2016 рр.), Програмного та бюджетного комітетів Всесвітньої організації інтелектуальної власності (ВОІВ). Постійний представник України при ООН обраний Головою Шостого комітету (правові питання) 67-ї сесії ГА ООН (2012-2013 рр.), Україна Віце-головує в Асамблеї Міжнародної морської організації, представник нашої держави входить до складу Міжнародного трибуналу з морського права (2011-2021 рр.).

**6. Підводні телекомунікаційні кабелі. Міжнародне право про підводні телекомунікаційні кабелі.**

Історія підводних кабелів починається в середині 19-го століття, коли почали прокладатися перші телеграфні кабелі по дну річок і гаваней, що стало можливим завдяки винайденню ізоляційних матеріалів. Перший великий телеграфний кабель між Англією та Францією прокладено 1851 року. 1858-го прокладено перший трансатлантичний кабель. Перший тихоокеанський — 1902-го. 1884 — перший телефонний підводний кабель між Сан-Франциско й Оклендом. У 20-х роках 20 століття короткохвильове радіо перехопило першість у морських кабелів, ставши основним носієм інформації на далекі відстані і зберігаючи цю нову роль практично до 50-х років. Справжній прорив стався 1956-го року, коли було прокладено трансатлантичний телефонний кабель ТАТ-1. Але в 70-х і 80-х основним інструментом передачі інформації через океани були космічні супутники, аж поки не настала ера оптичного волокна, яку позначив перший підводний оптоволоконний кабель, прокладений 1985-го року.375 На сьогодні 99% всього міжнародного трафіку проходить через підводні кабелі, і значна частина цього трафіку.

Найперший багатосторонній договір, що стосувався кабелів, укладено 1884 року. Це досі чинна Паризька конвенція про захист підводних телеграфних кабелів,380381 Попри слово «телеграфний» у назві перша стаття передбачає, що “ця Конвенція застосовується за межами територіальних вод до всіх правомірно прокладених підводних морських кабелів [a tous les cables sous-marins legalement etablis] з виходом на суходіл на територіях, в колоніях або інших володіннях однієї чи декількох Високих Договірних Сторін». Тобто уточнення про функціональне призначення кабелів у тексті відсутнє. Як буде показано далі, Женевські конвенції 1958 року та Конвенція ООН з морського права 1982 також юридично не розрізняють підводні морські кабелі за функціями: так що телекомунікаційні кабелі мають такий самий міжнародно-правовий режим, що й високовольтні електричні. Така байдужість загалом раціональна, адже сьогодні трапляються швидкісні оптоволоконні кабелі, що паралельно використовуються для передачі електроенергії.

У найзагальніших рисах Паризьку конвенцію можна класифікувати як класичну кримінально-правову конвенцію, адже її ключовий метод правового регулювання й основне зобов’язання — криміналізувати умисне пошкодження підводних морських кабелів: «Є караним діянням поламка чи пошкодження підводного морського кабелю, умисні чи внаслідок злочинної недбалості [negligence coupable], у такий спосіб, що може перервати чи перешкодити телеграфному зв’язку повністю або частково, причому таке покарання застосовується без шкоди для будь-якого цивільного позову про компенсацію заподіяної шкоди» (Пункт 1 статті 2). Згадка саме про «телеграфний зв’язок» створює сьогодні певну амбівалентність, утім загалом є тенденція тлумачити Конвенцію як застосовну до кабельного зв’язку будь-якого типу, включно з передачею голосу й цифрових даних у вигляді електричних або оптичних сигналів.

**7. Світова організація торгівлі й телекомунікації.**

Світова організація торгівлі (СОТ) – єдина міжнародна організація, що опікується глобальними правилами торгівлі між країнами. Її головна функція – забезпечувати, щоб торговельні обміни відбувалися настільки легко, передбачувано і вільно, наскільки можливо. СОТ стала наступницею Генеральної угоди з тарифів і торгівлі (ҐАТТ), укладеної після Другої світової війни.Тож попри те, що СОТ – одна з наймолодших міжнародних організацій, багатосторонній торговельній системі, початково закладеній ҐАТТ, вже понад 50 років.

Протягом минулих 50 років світова торгівля зростала надзвичайно швидко. Торгівля товарами збільшувалась у середньому на 6% щорічно. 2000 року загальний торговельний обіг у 22 рази перевищив рівень 1950 року.

СОТ об’єднує 160 членів, які здійснюють понад 95% світового торговельного обігу. Ще близько 25 країн ведуть переговори про вступ до організації.

Рішення ухвалюють всі члени, зазвичай одностайно. Ухвалення рішення більшістю також можливе, але голосування ніколи не застосовувалось в СОТ. Угоди СОТ ратифікували всі парламенти країн-членів.

Найвищий орган ухвалювання рішень в СОТ – Міністерська конференція – збирається щонайменше раз на два роки.

На рівень нижче – Генеральна рада (зазвичай до її складу входять посли і глави делегацій в Женеві, та іноді – чиновники, спеціально відряджені зі столиць країн-членів). Вона збирається кілька разів на рік у штаб-квартирі СОТ у Женеві. Генеральна рада виконує також функції нагляду за торговельною політикою та врегулювання суперечок.

На наступному рівні – Рада з торгівлі товарами, Рада з торгівлі послугами і Рада з торговельних аспектів інтелектуальної власності, підзвітні Генеральній раді.

Численні спеціальні комітети, підкомітети й робочі групи опікуються окремими угодами та іншими галузями, як-от, довкілля, розвиток, заявки на вступ і реґіональними торговельними угодами.

**8. Міжнародний союз електрозв’язку: загальний огляд. Регламент міжнародного електрозв’язку.**

Міжнародний союз електрозв’язку (МСЕ) – спеціалізована установа ООН у сфері глобального електрозв’язку, покликана здійснювати законодавчі, управлінські, виконавчі та консультативні функції, надавати технічну підтримку, розробляти стандарти і правила у сфері електрозв’язку та формулювати рекомендації, спрямовані на активізацію розвитку телекомунікацій та підвищення якості послуг.

Основною метою співробітництва України у рамках МСЕ залишається вдосконалення та раціональне використання інформаційно-комунікаційної інфраструктури, а також долання «цифрового розриву» в телекомунікаційних технологіях на національному та міжнародному рівнях. Супутньою метою співпраці з МСЕ залишається спільна діяльність з розробки та використання відкритих, функціонально сумісних, недискримінаційних міжнародних стандартів, що визначаються споживчим попитом.

Важливого значення для України також набуває діяльність дослідних комісій МСЕ, яка охоплює сферу технічного прогресу і міжнародної стандартизації в області мовлення, а також споріднених йому аудіовізуальних та мультимедійних застосувань, заснованих на використанні радіотехнологій. На сьогодні робота національних делегацій зосереджується на питаннях подальшого технічного прогресу телевізійного, звукового та мультимедійного мовлення, створення нових методів цифрової обробки, передавання та відтворення аудіовізуальної інформації, прогресу методів оцінки якості аудіовізуальної інформації, планування частотно-територіального ресурсу для наземних та супутникових мовленнєвих служб, використання нових підходів до стиснення аудіовізуальної інформації для подальшого підвищення ефективності її обробки та передачі.

Супутньою метою сучасного етапу співробітництва України у рамках МСЕ у галузі міжнародної стандартизації мовлення є забезпечення міжнародного правового захисту сумісного використання в Україні радіомовних аналогових і цифрових систем, служб і технологій на весь перехідний період від аналогового до цифрового мовлення, врахування національних інтересів України під час розроблення міжнародних нормативних документів, що стосуються стратегії впровадження цифрового мовлення, подолання цифрового розриву, а також створення цифрових служб нових поколінь.

Генеральним секретарем МСЕ є представник Китаю Хоулінь Чжао (2015-2018 рр.).

Керівний орган – Повноважна конференція, яка скликається раз на чотири роки і обирає Раду МСЕ в складі 46 членів, яка проводить свої засідання щорічно.

Міжнародний комітет захисту кабелів (International Cable Protection Committee — ICPC) — це неурядова організація, що об’єднує компанії в галузі прокладання й експлуатації підводних кабелів, а також інших зацікавлених осіб, практична робота якої полягає головно в поширенні навігаційних мап із попередженнями про ймовірність пошкодження підводного кабеля (також оновлення навігаційних мап світу в цьому відношенні), а також у підготовці керівництв для допомоги як власникам кабелів, так і офіційним органам.

**9. Радіочастотний ресурс і геостаціонарні орбіти.**

Відповідно до Декларації керівних засад використання мовлення через супутники для вільного поширення інформації, розвитку освіти і розширення культурних обмінів (Париж, 15 листопада 1972 року) і ч. 2 ст. 44 Статуту Міжнародного союзу електрозв'язку, радіочастоти і орбіта геостаціонарних супутників є обмеженими природними ресурсами, що належать усім народам і їх використання регулюється Конвенцією Міжнародного союзу електрозв'язку та її Регламентом радіозв'язку. Статут Міжнародного союзу електрозв'язку і Конвенція Міжнародного союзу електрозв'язку (Женева, 22 грудня 1992 року) ратифіковані Законом України від [15 липня](https://uk.wikipedia.org/wiki/15_%D0%BB%D0%B8%D0%BF%D0%BD%D1%8F) [1994](https://uk.wikipedia.org/wiki/1994%22%20%5Co%20%221994) року.

Положення міжнародно-правових актів відображені у п. 4 Концепції розвитку зв'язку України до 2010 року, затвердженої постановою Кабінету Міністрів України від [9 грудня](%22htt) [1999](https://uk.wikipedia.org/wiki/1999%22%20%5Co%20%221999) року № 2238, згідно з яким, радіочастотний ресурс є обмеженим природним ресурсом, ефективність використання якого впливає на економічне становище країни та на стан довкілля.

Законодавство: Стаття 1 Закону України «Про радіочастотний ресурс України» у редакції від 24 червня 2004 року); [Закон України «Про радіочастотний ресурс України», стаття 10](http://zakon2.rada.gov.ua/laws/show/1770-14); [Постанова КМУ від 15 грудня 2005 р. № 1208 «Про затвердження Національної таблиці розподілу смуг радіочастот України»](http://zakon2.rada.gov.ua/laws/show/1208-2005-%D0%BF); [Закон України «Про радіочастотний ресурс України», стаття 21, пункт 3](http://zakon2.rada.gov.ua/laws/show/1770-14); [Постанова КМУ від 9 червня 2006 р. № 815 «Про затвердження Плану використання радіочастотного ресурсу України»](http://zakon2.rada.gov.ua/laws/show/815-2006-%D0%BF)

**10. Спеціалізовані й надзвичайні телекомунікації. Регулювання міжнародних (теле)комунікацій на регіональному та національному рівнях.**

Використання телекомунікацій часто становить важливу складову загального зусилля з подолання наслідків природних і рукотворних катастроф. Наявність таких комунікацій забезпечує швидшу реакцію на надзвичайні події та вищу ефективність у застосуванні рідкісних ресурсів.

З іншого боку, самі умови широкомасштабного лиха часто означають, що нормальні (тобто зазвичай залежні від мережі — дротової чи стільникової) комунікації або недоступні, або марні, через що постає потреба в спеціальній апаратурі (супутниковій або портативній). Катастрофи вимагають швидкого розгортання спеціальних телекомунікацій, що нормально не використовуються широким загалом, у зонах, що постраждали. Доставка такого обладнання в такі зони часто саме по собі непроста задача, однак юридичний і регуляторний бік справи можуть іще більше все ускладнити. Зазвичай країни встановлюють різноманітні правила для імпортування пристроїв, що емітують радіохвилі. Наприклад, в Україні навіть такі поширені девайси як мобільні телефони вимагають сертифікації. Правила ввезення можуть бути доволі заплутаними, тож імовірність ненароком щось порушити буває достатньо високою, особливо коли рідкісне професійне іноземне обладнання експлуатується іноземними фахівцями, запрошеними постраждалою країною лише задля допомоги в подоланні наслідків лиха. Нарешті, навіть достатньо прості імпортні правила можуть скласти серйозну перешкоду, навіть стандартна вимога заплатити (високі чи навіть помірні) мита на ввезену апаратуру.

Вочевидь, можна придумати ще проблеми. Вищевказані взято лише тому, що саме на них було дано юридичну відповідь у тексті Конвенції Тампере про надання телекомунікаційних ресурсів для пом’якшення наслідків лих і операції з подання допомоги, укладеної Міжурядовою конференцією з надзвичайних телекомунікацій (ІСЕТ-1998) у Тампере, Фінляндія, 18 червня 1998 року. Хоча сам договір закриває ширше коло питань, перераховані вище видаються ключовими з обмеженої точки зору міжнародного права телекомунікацій, радше ніж права боротьби з лихами взагалі.