

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ В. Н. КАРАЗІНА

Кафедра міжнародних відносин, міжнародної інформації та безпеки

КОМПЛЕКС НАВЧАЛЬНО-МЕТОДИЧНОГО ЗАБЕЗПЕЧЕННЯ
з дисципліни
«ЗАХИСТ НАЦІОНАЛЬНОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ»

рівень вищої освіти: другий (магістерський)
галузь знань: 29 «Міжнародні відносини»
спеціальність: 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
освітня програма: «Міжнародна інформаційна безпека»
вид дисципліни: за вибором
факультет міжнародних економічних відносин та туристичного бізнесу

Укладач: канд. юрид. наук, доц. Доценко О. М.

1. НАВЧАЛЬНИЙ КОНТЕНТ (РОЗШИРЕНИЙ ПЛАН ЛЕКЦІЙ)

РОЗДІЛ 1. ЗАГАЛЬНІ ЗАСАДИ ЗАХИСТУ НАЦІОНАЛЬНОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ

Тема 1. Загальні засади інформаційного суспільства

ЛЕКЦІЯ 1. Загальні засади інформаційного суспільства

Мета:

- **навчальна:** формування у студентів базових знань щодо характеристики інформації як стратегічної сировини ХХІ століття, концепції інформаційного суспільства та типів і моделей його побудови, стану та стратегії розвитку інформаційного суспільства в Україні, а також практичних умінь та навичок правильного тлумачення та застосування заходів інформаційної протидії, необхідних для їх майбутньої трудової діяльності як фахівців у сфері міжнародної інформаційної безпеки;
- **розвиваюча:** розвинути у студентів уміння визначати концепцію інформаційного суспільства та характеризувати стан розвитку інформаційного суспільства в Україні, а також навички роботи з міжнародними та національними нормативно-правовими актами та документами у сфері інформаційної безпеки;
- **виховна:** викликати у студентів зацікавленість до вивчення даної теми.

Час проведення – 2 год.

Навчальні питання:

1. Інформація – стратегічна сировина ХХІ століття.
2. Концепція інформаційного суспільства.
3. Стан розвитку інформаційного суспільства в Україні.

Ключові поняття: інформація, інформаційне суспільство, інформаційна продукція, інформаційна послуга, принципи побудови інформаційного суспільства, персональні дані, інформація з обмеженим доступом, ІКТ, стратегія розвитку інформаційного суспільства, електронне урядування.

Література:

Основна: 5, 7, 13, 14, 16, 18, 21, 27, 28, 31.
Додаткова: 2, 3, 10, 11, 12.

Хід заняття:

1. Організаційний момент.
2. Актуалізація опорних знань.

Оскільки дана тема є першою в семестрі, викладач сам наголошує на актуальності питання побудови інформаційного суспільства в умовах глобалізації та необхідності захисту національного інформаційного простору від потенційних та реальних загроз.

3. Виклад нової інформації.

ПИТАННЯ № 1. Інформація - стратегічна сировина XXI століття.

Закон України «Про інформацію» від 02.10.1992 № 2657-ХІІ. Поняття інформації. Види інформації. Право на інформацію. Інформаційні відносини. Інформаційний ресурс. Інформаційна продукція та інформаційна послуга.

Інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

За змістом інформація поділяється на такі види:

1. інформація про фізичну особу;
2. інформація довідково-енциклопедичного характеру;
3. інформація про стан довкілля (екологічна інформація);
4. інформація про товар (роботу, послугу);
5. науково-технічна інформація;
6. податкова інформація;
7. правова інформація;
8. статистична інформація;
9. соціологічна інформація;
10. інші види інформації.

Інформація про фізичну особу (персональні дані) – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини. До конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження. Кожному забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законом.

Інформація довідково-енциклопедичного характеру – систематизовані, документовані, публічно оголошені або іншим чином поширені відомості про суспільне, державне життя та навколишнє природне середовище.

Інформація про стан довкілля (екологічна інформація) – відомості та/або дані про:

стан складових довкілля та його компоненти, включаючи генетично модифіковані організми, та взаємодію між цими складовими;

фактори, що впливають або можуть впливати на складові довкілля (речовини, енергія, шум і випромінювання, а також діяльність або заходи,

включаючи адміністративні, угоди в галузі навколишнього природного середовища, політику, законодавство, плани і програми);

стан здоров'я та безпеки людей, умов життя людей, стан об'єктів культури і споруд тією мірою, якою на них впливає або може вплинути стан складових довкілля;

інші відомості та/або дані.

Інформація про товар (роботу, послугу) – відомості та/або дані, які розкривають кількісні, якісні та інші характеристики товару (роботи, послуги).

Науково-технічна інформація – будь-які відомості та/або дані про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Податкова інформація – сукупність відомостей і даних, що створені або отримані суб'єктами інформаційних відносин у процесі поточної діяльності і необхідні для реалізації покладених на контролюючі органи завдань і функцій у порядку, встановленому Податковим кодексом України.

Правова інформація – будь-які відомості про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо.

Статистична інформація – документована інформація, що дає кількісну характеристику масових явищ та процесів, які відбуваються в економічній, соціальній, культурній та інших сферах життя суспільства.

Соціологічна інформація – будь-які документовані відомості про ставлення до окремих осіб, подій, явищ, процесів, фактів тощо.

Доступ до інформації.

За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.

Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.

Інформація з обмеженим доступом

Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація.

Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

До інформації з обмеженим доступом не можуть бути віднесені такі відомості:

- 1) про стан довкілля, якість харчових продуктів і предметів побуту;
- 2) про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей;

3) про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

4) про факти порушення прав і свобод людини, включаючи інформацію, що міститься в архівних документах колишніх радянських органів державної безпеки, пов'язаних з політичними репресіями, Голодомором 1932–1933 років в Україні та іншими злочинами, вчиненими представниками комуністичного та/або націонал-соціалістичного (нацистського) тоталітарних режимів;

5) про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб;

5⁻¹) щодо діяльності державних та комунальних унітарних підприємств, господарських товариств, у статутному капіталі яких більше 50 відсотків акцій (часток) належать державі або територіальній громаді, а також господарських товариств, 50 і більше відсотків акцій (часток) яких належать господарському товариству, частка держави або територіальної громади в якому становить 100 відсотків, що підлягають обов'язковому оприлюдненню відповідно до закону;

6) інші відомості, доступ до яких не може бути обмежено відповідно до законів та міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України.

Закон України «Про національну програму інформатизації» від 4 лютого 1998 року № 74/98-ВР надає наступні визначення:

інформаційна послуга – дії суб'єктів щодо забезпечення споживачів інформаційними продуктами;

інформаційний продукт (продукція) – документована інформація, яка підготовлена і призначена для задоволення потреб користувачів;

інформаційний ресурс – сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо);

Закон України «Про інформацію»:

Інформаційна продукція – матеріалізований результат інформаційної діяльності, призначений для задоволення потреб суб'єктів інформаційних відносин. **Інформаційною послугою** є діяльність з надання інформаційної продукції споживачам з метою задоволення їхніх потреб.

Інформаційна продукція та інформаційні послуги є об'єктами цивільно-правових відносин, що регулюються цивільним законодавством України.

Інформаційні відносини – відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації.

Основними принципами інформаційних відносин є: гарантованість права на інформацію; відкритість, доступність інформації, свобода обміну інформацією; достовірність і повнота інформації; свобода вираження поглядів і переконань; правомірність одержання, використання, поширення, зберігання та захисту інформації; захищеність особи від втручання в її особисте та сімейне життя.

Суб'єктами інформаційних відносин є: фізичні особи; юридичні особи; об'єднання громадян; суб'єкти владних повноважень.

Об'єктом інформаційних відносин є інформація.

Основними напрямками державної інформаційної політики є:

забезпечення доступу кожного до інформації;

забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації;

створення умов для формування в Україні інформаційного суспільства;

забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень;

створення інформаційних систем і мереж інформації, розвиток електронного урядування;

постійне оновлення, збагачення та зберігання національних інформаційних ресурсів;

забезпечення інформаційної безпеки України;

сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору.

Право на інформацію. Кожен має право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів. Реалізація права на інформацію не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб.

Гарантії права на інформацію. Право на інформацію забезпечується:

створенням механізму реалізації права на інформацію;

створенням можливостей для вільного доступу до статистичних даних, архівних, бібліотечних і музейних фондів, інших інформаційних банків, баз даних, інформаційних ресурсів;

обов'язком суб'єктів владних повноважень інформувати громадськість та засоби масової інформації про свою діяльність і прийняті рішення;

обов'язком суб'єктів владних повноважень визначити спеціальні підрозділи або відповідальних осіб для забезпечення доступу запитувачів до інформації;

здійсненням державного і громадського контролю за додержанням законодавства про інформацію;

встановленням відповідальності за порушення законодавства про інформацію.

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

Охорона права на інформацію.

1. Право на інформацію охороняється законом. Держава гарантує всім суб'єктам інформаційних відносин рівні права і можливості доступу до інформації.

2. Ніхто не може обмежувати права особи у виборі форм і джерел одержання інформації, за винятком випадків, передбачених законом. Суб'єкт інформаційних відносин може вимагати усунення будь-яких порушень його права на інформацію.

3. Забороняється вилучення і знищення друкованих видань, експонатів, інформаційних банків, документів з архівних, бібліотечних, музейних фондів, крім встановлених законом випадків або на підставі рішення суду.

4. Право на інформацію, створену в процесі діяльності фізичної чи юридичної особи, суб'єкта владних повноважень або за рахунок фізичної чи юридичної особи, Державного бюджету України, місцевого бюджету, охороняється в порядку, визначеному законом.

Основними видами інформаційної діяльності є створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації.

Відповідальність за порушення законодавства про інформацію. Порушення законодавства України про інформацію тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність згідно із законами України.

Неприпустимість зловживання правом на інформацію. Інформація не може бути використана для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання міжетнічної, расової, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини.

Поширення суспільно необхідної інформації. Інформація з обмеженим доступом може бути поширена, якщо вона є суспільно необхідною, тобто є предметом суспільного інтересу, і право громадськості знати цю інформацію переважає потенційну шкоду від її поширення.

Предметом суспільного інтересу вважається інформація, яка свідчить про загрозу державному суверенітету, територіальній цілісності України; забезпечує реалізацію конституційних прав, свобод і обов'язків; свідчить про можливість порушення прав людини, введення громадськості в оману, шкідливі екологічні та інші негативні наслідки діяльності (бездіяльності) фізичних або юридичних осіб тощо.

Звільнення від відповідальності. Ніхто не може бути притягнутий до відповідальності за висловлення оціночних суджень.

Оціночними судженнями, за винятком наклепу, є висловлювання, які не містять фактичних даних, критика, оцінка дій, а також висловлювання, що не можуть бути витлумачені як такі, що містять фактичні дані, зокрема з огляду на характер використання мовно-стилістичних засобів (вживання гіпербол, алегорій, сатири). Оціночні судження не підлягають спростуванню та доведенню їх правдивості.

Якщо особа вважає, що оціночні судження або думки принижують її гідність, честь чи ділову репутацію, а також інші особисті немайнові права, вона вправі скористатися наданим їй законодавством правом на відповідь, а також на власне тлумачення справи у тому самому засобі масової інформації з метою обґрунтування безпідставності поширених суджень, надавши їм іншу оцінку. Якщо суб'єктивну думку висловлено в брутальній, принизливій чи непристойній формі, що принижує гідність, честь чи ділову репутацію, на особу, яка таким чином та у такий спосіб висловила думку або оцінку, може бути покладено обов'язок відшкодувати завдану моральну шкоду.

Суб'єкти інформаційних відносин звільняються від відповідальності за розголошення інформації з обмеженим доступом, якщо суд встановить, що ця інформація є суспільно необхідною.

Відшкодування матеріальної та моральної шкоди. У разі якщо порушенням права на свободу інформації особі завдано матеріальної чи моральної шкоди, вона має право на її відшкодування за рішенням суду.

Суб'єкти владних повноважень як позивачі у справах про захист честі, гідності та ділової репутації вправі вимагати в судовому порядку лише спростування недостовірної інформації про себе і не мають права вимагати відшкодування моральної (немайнової) шкоди. Це не позбавляє посадових і службових осіб права на захист честі, гідності та ділової репутації в суді.

ПИТАННЯ № 2. Концепція інформаційного суспільства.

Окінавська хартія глобального інформаційного суспільства від 22.07.2000 року: мета, основні положення.

Використання можливостей цифрових технологій.

Потенційні переваги ІТ, які стимулюють конкуренцію, сприяють розширенню виробництва, створюють і підтримують економічне зростання і зайнятість, мають значні перспективи. Наше завдання полягає не тільки в стимулюванні та сприянні переходу до інформаційного суспільства, але також і в повній реалізації його економічних, соціальних і культурних переваг. Для досягнення цих цілей важливо будувати роботу на наступних ключових напрямках:

- проведення економічних і структурних реформ з метою створення умов відкритості, ефективності, конкуренції та використання нововведень, які доповнювалися б заходами по адаптації на ринках праці, розвитку людських ресурсів та забезпечення соціальної злагоди;

- раціональне управління макроекономікою, що сприяє більш точному плануванню з боку ділових кіл та споживачів, і використання переваг нових інформаційних технологій;

- розробка інформаційних мереж, що забезпечують швидкий, надійний, безпечний і економічний доступ за допомогою конкурентних ринкових умов і відповідних нововведень до мережевих технологій, їх обслуговування та застосування;

- розвиток людських ресурсів, здатних відповідати вимогам століття інформації, за допомогою освіти та довічного навчання і задоволення

зростаючого попиту на фахівців в області ІТ у багатьох секторах нашої економіки;

- активне використання ІТ в державному секторі і сприяння наданню в режимі реального часу послуг, необхідних для підвищення рівня доступності влади для всіх громадян.

Приватний сектор відіграє життєво важливу роль в розробці інформаційних і комунікаційних мереж в інформаційному суспільстві. Однак завдання створення передбачуваної, відкритості і недискримінаційної політики і нормативної бази, необхідної для інформаційного суспільства, лежить на урядах. Нам необхідно подбати про те, щоб правила і процедури, що мають відношення до ІТ, відповідали корінним змінам в економічних угодах з урахуванням принципів ефективного партнерства між державним і приватним сектором, а також транспарентності та технологічної нейтральності. Такі правила повинні бути передбачуваними і сприяти зміцненню ділової і споживчої довіри.

Подолання електронно-цифрового розриву. Стратегія розвитку інформаційного суспільства повинна супроводжуватися розвитком людських ресурсів, можливості яких відповідали б вимогам інформаційного століття. Ми зобов'язуємося надати всім громадянам можливість освоїти і отримати навички роботи з ІТ за допомогою освіти, довічного навчання і підготовки. Ми будемо і далі прагнути до здійснення цієї масштабної мети, надаючи школам, класам і бібліотекам комп'ютерне обладнання, здатне працювати в режимі реального часу, а також направляти туди викладачів, що мають навички роботи з ІТ та мультимедійними засобами. Крім того, ми будемо здійснювати заходи щодо підтримки і стимулювання малих і середніх підприємств, а також людей, які працюють не за наймом, надаючи їм можливість підключатися до мережі Інтернет та ефективно нею користуватися. Ми також будемо заохочувати використання ІТ з метою надання громадянам можливості довічного навчання з застосуванням передових методик, особливо тим категоріям громадян, які в іншому випадку не мали б доступу до освіти та професійної підготовки.

Сприяння загальній участі. ІТ відкриває перед країнами, що розвиваються чудові можливості. Країни, яким вдалося направити свій потенціал в потрібне русло, можуть сподіватися на подолання перешкод, які традиційно виникають в процесі розвитку інфраструктури, більш ефективного вирішення своїх насущних завдань в області розвитку, таких як скорочення бідності, охорона здоров'я, поліпшення санітарних умов і освіти, а також використання переваг швидкого зростання глобальної електронної торгівлі.

Подальший розвиток. Зусилля щодо подолання міжнародної роз'єднаності в вирішальною мірою залежать від ефективної співпраці між усіма учасниками. Для створення рамкових умов для розвитку ІТ важливу роль і в подальшому буде грати двостороннє і багатостороннє співробітництво. Міжнародні фінансові інститути, включаючи багатосторонні банки розвитку (МБР), особливо Всесвітній банк, вельми придатні для цієї

мети і можуть розробляти і здійснювати програми, які сприятимуть зростанню і боротьбі з бідністю, а також розширювати зв'язки, доступ і навчання.

Міжнародна мережа телекомунікацій, ЮНКТАД і ЮНДП і інші відповідні міжнародні фонди також можуть зіграти важливу роль. Центральною залишається роль приватного сектора в просуванні ІТв країнах, що розвиваються. Він може також істотно сприяти міжнародним зусиллям з подолання цифрового розриву. НВО, що володіють унікальними можливостями донести ідеї до громадськості, також можуть сприяти розвитку людських і суспільних ресурсів. ІТ глобальна по своїй суті і вимагає глобального підходу.

Декларація принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті» 12 грудня 2003 року.

Слід зазначити, що Декларація принципів з питань інформаційного суспільства встановлює головні принципи та напрямки побудови інформаційного суспільства на глобальному рівні.

В. Інформаційне суспільство для всіх: ключові принципи:

1) Роль державних органів і всіх заінтересованих сторін у сприянні використанню ІКТ для цілей розвитку.

Державні органи, а також приватний сектор, громадянське суспільство, *Організація Об'єднаних Націй* та інші міжнародні організації відіграють важливу роль і несуть відповідальність за розвиток інформаційного суспільства і, в належних випадках, за процеси прийняття рішень. Побудова інформаційного суспільства, орієнтованого на інтереси людей, є спільним зусиллям, що вимагає співробітництва і партнерства між усіма заінтересованими сторонами.

2) Інформаційна і комунікаційна інфраструктура: необхідний фундамент відкритого для всіх інформаційного суспільства.

Документи, що визначають політику, які створюють сприятливі умови для стабільності, передбачуваності і добросовісної конкуренції на всіх рівнях, повинні розроблятися і впроваджуватися так, щоб не лише залучати більше приватних інвестицій у розвиток інфраструктури ІКТ, але й забезпечувати виконання зобов'язань із надання загальнодоступних послуг в тих областях, де не діють традиційні ринкові механізми. У районах, що знаходяться в несприятливих умовах, створення публічних пунктів доступу до ІКТ у таких структурах, як поштові відділення, школи, бібліотеки та архіви, може надати ефективні засоби для забезпечення загального доступу до інфраструктури і послуг інформаційного суспільства.

3) Доступ до інформації та знань.

Велике публічне надбання – необхідний елемент для зростання інформаційного суспільства, що створює такі численні блага, як освічене населення, нові робочі місця, інновації, можливості для бізнесу і розвиток науки. Інформація, що є публічним надбанням, повинна бути легкодоступною для підтримки інформаційного суспільства і захищеною від незаконного привласнення. Публічні установи, такі як бібліотеки й архіви, музеї, колекції культурних цінностей та інші суспільні пункти доступу слід зміцнювати для

того, щоб сприяти збереженню документальних записів і вільному та рівноправному доступу до інформації.

Доступу до інформації і знань можна сприяти, підвищуючи рівень інформованості всіх заінтересованих сторін про можливості, які надають різні моделі програмного забезпечення, у тому числі власницьке, з відкритими кодами і безплатне програмне забезпечення, для того, щоб підвищити конкуренцію, доступ користувачів, різноманітність вибору, а також надати можливість усім користувачам знаходити рішення, які найкраще задовольняють їхні запити. Прийнятний за ціною доступ до програмного забезпечення є важливим компонентом насправді відкритого для всіх інформаційного суспільства.

4) Підвищення компетентності.

Для забезпечення сталого розвитку інформаційного суспільства слід нарощувати національні можливості науково-дослідних і конструкторських робіт у сфері ІКТ. Крім цього, партнерства, зокрема між і серед розвинутих країн та країн, що розвиваються, включаючи країни з перехідною економікою, у сфері науково-дослідних і конструкторських робіт, передачі технологій, виробництва і використання продуктів і послуг ІКТ, є вирішальними для сприяння підвищенню компетентності і глобальної участі в інформаційному суспільстві. Виробництво ІКТ відкриває широку можливість для створення добробуту.

5) Підвищення довіри і безпеки при використанні ІКТ.

Зміцнення основи для довіри, включаючи інформаційну безпеку і безпеку мереж, підтвердження достовірності, захист недоторканості приватного життя і прав споживачів, є передумовою розвитку інформаційного суспільства і підвищення довіри з боку користувачів ІКТ. Необхідно формувати, розвивати і впроваджувати глобальну культуру кібербезпеки в співробітництві з усіма заінтересованими сторонами і компетентними міжнародними органами. Ці зусилля повинні спиратися на все ширше міжнародне співробітництво. У рамках цієї глобальної культури кібербезпеки важливо підвищувати безпеку і забезпечувати захист даних і недоторканості приватного життя, розширюючи при цьому доступ і торгівлю. Окрім цього, необхідно брати до уваги рівень соціального й економічного розвитку кожної країни і враховувати аспекти інформаційного суспільства, пов'язані з орієнтацією на розвиток.

6) Сприятливе середовище.

Динамічне і сприятливе міжнародне середовище, що сприяє залученню прямих іноземних інвестицій, передачі технологій і міжнародному співробітництву, зокрема у сферах фінансів, заборгованості і торгівлі, а також повна й ефективна участь країн, що розвиваються, у прийнятті рішень на світовому рівні є життєво важливими додатковими компонентами національних зусиль в області розвитку, що стосуються ІКТ. Розширення глобальної, прийнятної за ціною можливості з'єднання значно сприяло б ефективності цих зусиль в області розвитку.

7) Прикладення ІКТ: вигоди в усіх аспектах життя.

Використання і розгортання ІКТ слід спрямовувати на створення вигод у всіх аспектах нашого повсякденного життя. Прикладення ІКТ потенційно важливі для урядової діяльності і послуг, охорони здоров'я та інформації про здоров'я, освіти і професійної підготовки, зайнятості, створення робочих місць, підприємництва, сільського господарства, транспорту, захисту довкілля й управління природними ресурсами, запобігання катастрофам, культури, для сприяння подоланню бідності та для інших погоджених цілей розвитку. ІКТ повинні також сприяти моделям сталого виробництва і споживання і зменшенню традиційних бар'єрів, даючи можливість усім одержати доступ на місцеві і світові ринки більш справедливим способом. Прикладення повинні бути дружніми для користувачів, доступними для всіх, прийнятними за ціною, пристосованими до місцевих мовних і культурних потреб та підтримувати сталий розвиток. Для цього місцеві органи влади повинні відігравати основну роль у наданні послуг ІКТ на благо свого населення.

8) Культурне різноманіття та ідентичність, мовне різноманіття і місцевий контент.

При побудові відкритого для всіх інформаційного суспільства повинен надаватися високий пріоритет створенню, поширенню і збереженню контенту на різних мовах і в різних форматах, звертаючи окрему увагу на різноманіття пропозицій творчих робіт і належне визнання прав авторів і митців. Необхідно сприяти виробництву і забезпеченню доступності всього контенту – освітнього, наукового, культурного і розважального – на різних мовах і в різних форматах. Створення місцевого контенту, пристосованого до внутрідержавних або регіональних потреб, буде сприяти соціальному і економічному розвитку та стимулювати участь усіх заінтересованих сторін, у тому числі жителів сільських, віддалених і маргінальних районів.

9) Засоби масової інформації.

Ми знову підтверджуємо наше зобов'язання дотримуватися принципів свободи друку і свободи інформації, а також принципів незалежності, плюралізму і різноманіття засобів масової інформації, які є необхідними для інформаційного суспільства. Свобода шукати, одержувати, передавати і використовувати інформацію для створення, нагромадження і поширення знань є важливою для інформаційного суспільства. Ми закликаємо до відповідального використання і трактування інформації засобами масової інформації відповідно до найвищих етичних і професійних стандартів. Традиційні засоби масової інформації в усіх їхніх формах відіграють важливу роль в інформаційному суспільстві й ІКТ повинні відігравати підтримуючу роль стосовно цього. Слід заохочувати різноманітність форм власності на засоби масової інформації, згідно з національним законодавством і з урахуванням відповідних міжнародних конвенцій. Ми знову підтверджуємо необхідність скорочення міжнародних диспропорцій, які впливають на засоби масової інформації, зокрема стосовно інфраструктури, технічних ресурсів і розвитку навичок і вмінь.

10) Етичні сторони інформаційного суспільства.

Інформаційне суспільство повинне поважати мир і дотримуватися основних цінностей свободи, рівності, солідарності, терпимості, колективної відповідальності і збереження природи.

11) Міжнародне і регіональне співробітництво.

Інформаційне суспільство є по-справжньому глобальним за природою, і національні зусилля потребують підтримки ефективним міжнародним і регіональним співробітництвом між державними органами, приватним сектором, громадянським суспільством та іншими заінтересованими сторонами, включаючи міжнародні фінансові установи.

Щодо **Женевського Плану дій**, то керівні принципи Декларації принципів з питань інформаційного суспільства перенесені в цьому документі у конкретні напрямки дій для досягнення погоджених на міжнародному рівні цілей розвитку, впровадження, сприянням використанню продуктів, мереж, послуг і стосунків на базі інформаційно-комунікаційних технологій, а також для допомоги країнам у подоланні цифрової нерівності.

Одним з головних питань, зазначених у обох вищезазначених документах було прохання до Генерального секретаря ООН створити Робочу групу з управління Інтернетом в рамках відкритого для всіх процесу, що буде забезпечувати механізм для повної і активної участі органів державного управління, приватного сектору та громадянського суспільства як із країн, так і з розвинутих країн, в тому числі відповідних міжурядових та міжнародних організацій і форумів, з метою вивчення питання про управління використанням Інтернету. Робочій групі з управління Інтернетом було доручено вивчити «питання про управління використанням Інтернет і надати пропозиції для прийняття рішення відносно організації управління використанням Інтернет».

Крім того, перед Робочою групою, як координатором робіт щодо управління Інтернетом, були поставлені наступні завдання: запропонувати робоче визначення «управління використанням Інтернет», підготувати аналітику та основні принципи даної дефініції; дослідити та визначити основні питання державної політики, які відносяться до управління використанням Інтернет; сформулювати єдиний підхід, щодо розуміння ролі та сфери відповідальності органів державного управління, існуючих міжнародних організацій, а також приватного сектору та суспільних організацій.

Робочою групою управління Інтернетом було визначено основні напрями роботи, та згруповано основні проблемні питання за напрямками: справедливий розподіл ресурсів; доступ для всіх; стабільне та надійне функціонування Інтернет; багатомовність і контент.

Підсумовуючи вищесказане, можна сказати, що Женевський Етап став початком для створення першої діючої моделі управління Інтернетом, та видав перші міжнародні документи універсального характеру, які стали базовими для вирішення першочергових питань та проблем у створенні єдиного механізму з управління Інтернетом.

У листопаді 2005 р в Тунісі проходив туніський етап Зустрічі WSIS, у якому йшла мова про реалізацію Женевського Плану дій, та вироблення

рішень та домовленостей з приводу управління Інтернетом, виходячи з підсумків роботи Групи WGIG. В кінці даної зустрічі було прийнято два документи, перший який мав назву «**Туніське зобов'язання з питань інформаційного суспільства**», а другий «**Туніська програма для інформаційного суспільства**».

У Туніському зобов'язанні з питань інформаційного суспільства, було ще раз переглянуто базові засади та принципи, які були введені ще у Декларації принципів з питань інформаційного суспільства, але потрібно, сказати, що у цьому документі містяться положення, щодо реалізації та розвитку інформаційного суспільства, та ІКТ, яке прямим чином пов'язано з розвитком управління Інтернетом.

Щодо «Туніського зобов'язання з питань інформаційного суспільства», можна сказати, що він показав усю недосконалість участі держав в управлінні Інтернетом, із за нечітко виписаних правил поведінки у тих чи інших питаннях в сфері розвитку інформаційного суспільства, ІКТ, чи управління Інтернетом державної політики».

Туніська програма для інформаційного суспільства підтвердила принципи, проголошені під час Женевського етапу WSIS та відзначила «потребу в активізації співробітництва в майбутньому, щоб надати можливість урядам, на рівноправній основі, відігравати свої ролі й виконувати свої зобов'язання в питаннях міжнародної державної політики, що стосуються Інтернету, а не в повсякденних технічних і експлуатаційних справах, що не впливають на питання міжнародної державної політики».

З приводу цього можна сказати, що на другому етапі Зустрічі WSIS, було вирішено, багато важливих питань пов'язаних з управлінням Інтернету, адже другий етап став, став як способом, виправлення помилок після першого етапу. Тобто усі недоліки та прогалини, які виникли на Женевській зустрічі, було виправлено та доповнено ідеями на Туніській зустрічі.

Типи і моделі побудови інформаційного суспільства.

На основі ключових чинників, до яких відносять макроекономічну політику держав у контексті формування інформаційного суспільства, особливості ідеології переходу до нової фази розвитку, специфіку законодавства, характеристики національної культури і менталітету, виділяють дві моделі становлення інформаційного суспільства - західну і азійську. Національні моделі відзначаються політичними стратегіями, специфікою національних ринків, законодавчими традиціями, розвитком інфраструктури, економічними ресурсами. Проте незалежно від національних особливостей простежуються дві основні тенденції:

- 1) поєднання (злиття) державних і суспільних інтересів з приватною ініціативою з метою фінансування нового гармонійного суспільства;
- 2) розвиток міжнародної конкуренції для трансформації ринкових структур і подальшої конвергенції комунікаційної сфери.

Західний тип становлення інформаційного суспільства узагальнює стратегії і програми індустріально розвинених країн – США, Канади, Великої

Британії, ФРН, Франції, країн Північної Європи. У рамках цієї моделі своєю специфікою вирізняються американо-англійська та європейська моделі.

Американо-англійська модель визначається загальною концепцією соціально-економічного розвитку, яка передбачає переваги приватного сектору над функціями держави в усіх напрямках розвитку суспільства. Американський вплив у галузі комунікаційних технологій та інформаційної сфери відчутний в глобальних процесах, міжнародній політиці, світовій економіці. Ідея побудови інформаційних супермагістралей, створення національної і глобальної інфраструктури з метою зростання і динаміки економічного розвитку, запропонована 1993 року як президентська стратегія США, покладена в основу всіх існуючих національних моделей становлення інформаційного суспільства. Англійська модель максимально близька до американської:

- роль держави обмежується створенням умов для ринкової конкуренції в інформаційній сфері;

- стратегія розвитку суспільства визначається як приватна ініціатива, лібералізація ринку телекомунікацій, створення мереж та інформаційних супермагістралей, захист нових структур на інформаційних ринках.

Американо-англійська модель передбачає інтенсивний розвиток електронних комунікацій для встановлення соціальних, політичних, культурних зв'язків у суспільстві. Проблема поширення універсальних послуг має важливе значення в програмах інформаційного суспільства США та Великої Британії, вона вирішується за допомогою стратегії поліпшення якості інформаційних послуг, виваженої цінової політики, соціальної орієнтації суспільства. Специфічною рисою американо-англійської моделі інформаційного суспільства є вплив чинного законодавства на розвиток перспективних галузей економіки. Замовлення інформаційного суспільства обумовлює і диференціює трудове право, авторське право, право інтелектуальної власності, соціальний захист населення. У США спостерігається вичерпність трудових ресурсів (з одночасним поширенням сфери використання інформаційних послуг) і потребами поповнення їх зарахунок нової "інтелектуальної" хвилі імміграції. У культурній сфері США і Велика Британія мають різні стратегії. Північноамериканська модель (США, І Канада) стимулює діяльність аудіовізуальної промисловості і ринку і розважальних відеопослуг за запитами населення. У Великій Британії Поділяють культурну стратегію континентальної Європи – збереження і культурної ідентичності і самобутності націй, створення європейської і культурної спадщини, забезпечення культурних прав національних.

Європейська модель інформаційного суспільства вирізняється стратегією європейської інтеграції, поняттям «об'єднаної Європи», пуками рівноваги між контролем держави і стихією ринку, динамічним поєднанням державних інтересів і прагнень приватного та корпоративного бізнесу. Характерними рисами європейської моделі є варіативність і політична спрямованість програм побудови інформаційного суспільства для різних країн, обумовлених новою європейською геополітикою, становленням

інформаційної (інтелектуальної) економіки, різними можливостями постіндустріального розвитку. У рамках європейської моделі виділяють західноєвропейську, скандинавську, центральноєвропейську, східноєвропейську стратегії.

В основу класифікації моделей інформаційного суспільства покладено в основному соціально-економічні показники різних країн, тобто макропоказники, що вирішальним чином впливають на динаміку процесів у міжнародному інформаційному полі. При цьому не беруться до уваги інші критерії інформаційного розвитку, які впливають на перспективи країн, що розвиваються. Врахування таких критеріїв підкоригувало б запропоновані моделі відповідно до специфіки економічної бази, національних пріоритетів та попиту на інформаційні технології в інших регіонах світу.

Європейський план інформаційного суспільства містить також концепцію розвитку універсальних послуг, яка має політичні, економічні, соціальні і технологічні ознаки. До політичних ознак відносять протидію монополій конкуренції (побудова нових магістралей здійснюється обмеженим колом операторів у більшості європейських країн), до економічних – створення ринку інформаційних послуг, до соціальних – недискримінацію за інформаційною ознакою (нерівність у доступі до універсальних інформаційних послуг, обумовлену рівнем доходів і платоспроможністю населення), до технологічних – першочерговий розвиток магістралей. Відмінність європейської моделі від американської полягає і в створенні інформаційного законодавства; адекватної законодавчої бази, яка враховує як національні, так і міжнародні принципи регулювання інформаційних відносин, вважається Головним чинником зростання прибутку країни від потенціалу інформаційно-комунікаційних технологій.

Азійський тип інформаційного суспільства реалізує ідеологічну доктрину країн Азійсько-Тихоокеанського регіону, побудовану на філософських принципах конфуціанства, діяльності держави щодо інституціоналізації цих принципів, взаєморозуміння і взаємодопомоги в суспільстві для досягнення мети. В основі азійського типу – альтернативний соціально-економічний розвиток регіону, конкуренція із Заходом, утвердження власних ціннісних орієнтацій, зв'язок між культурними традиціями (освіта, виробнича дисципліна, відданість корпорації, довіра, сімейна гармонія) і соціальними трансформаціями. У рамках азійської моделі виділяють японську, індійську та младазійську.

Японська модель постіндустріального розвитку спрямована на вдосконалення системи корпоративного управління за принципом ієрархічної піраміди, в основі якої три складові чинники: он (вдячність), гігі (відповідальність), ва (гармонія). Вони виражають угоду про взаєморозуміння і взаємодопомогу вищого і нижнього рівнів управління в державі і якості цієї угоди, тобто розуміння статусу кожної групи відповідно до спільної мети.

Японська модель інформаційного суспільства використовує пріоритетний розвиток інформаційних технологій і впровадження інформаційних послуг у всі сфери життєдіяльності країни. У ХХІ столітті

стратегічна політика японського уряду полягає у стимулюванні інтелектуального розвитку нації, провідної ролі бізнесу для інформаційної економіки, розумінні інформаційного (інтелектуального) блага як спільного надбання суспільства. Для розвинутої інформаційної цивілізації характерними є підвищення рівня ефективності усіх суспільних процесів, зростання комфортності життя, доступність використання цифрової техніки, її адаптація до потреб споживачів. Для впровадження моделі інтелектуального суспільства прийнято політичні рішення про національну мету Японії в галузі високих технологій, інтенсифікацію діяльності у сфері інформаційної науки і техніки, інтелектуальної власності, ноу-хау як пріоритетних напрямів розвитку.

Младоазійська модель передбачає стратегію регіону Східної і Південно-Східної Азії – епіцентру індустріального та інформаційного розвитку, до якого належать Південна Корея, Тайвань, Сінгапур і Гонконг, а в останні роки наближаються Таїланд, Малайзія, В'єтнам. Ця модель – трансформована японська ідея, успіх якої пов'язується з підтриманням сталого макроекономічного і політичного середовища та співробітництва держави з приватним капіталом. Уряди приймають рішення щодо вагомих інвестицій приватного сектору в інформаційну сферу, стимулюють створення матеріальної і соціальної інфраструктури (тобто, порушується фундаментальний принцип невтручання держави у ринкові відносини). Державний контроль, його форми і методи можуть бути різними, але дилема «держава-ринок» виступає як соціально-політична, а не суто економічна. Младоазійська модель характеризується як політичне і економічне співробітництво держави і приватного сектору.

У країнах, що розвиваються, визначають дві моделі становлення інформаційного суспільства – **латиноамериканську і азійську**, які відрізняються напрямками і масштабами трансформації. Стратегія реформування включає приватизацію (передачу державних підприємств і видів діяльності у повну або часткову приватну власність чи контроль), лібералізацію (розширення конкуренції на ринку товарів і послуг). Азійська модель характеризується пріоритетним розвитком лібералізації, впровадженням конкуренції і відкритості ринків, а латиноамериканська починається з приватизації з метою різкого зростання якості телекомунікаційних послуг, поступового впровадження конкуренції і вважається більш ефективною.

Індійську модель визначають як комбінований варіант, що за масштабами і ефективністю трансформацій наближається до латиноамериканської моделі, а за прогресивністю впровадження – до азійської. Акцент зроблено на ресурсах народонаселення, науково-технічному потенціалі (третьому у світі після США та Росії), чинному законодавстві, державному контролі у сфері виробництва інформаційних послуг (крім ринку місцевих послуг, де допускається 49% іноземних капіталовкладень). Специфіка ідеології інформаційного суспільства в Індії – поступова динаміка, опора на національні культурні традиції. Урядова політика визначає головним чинником становлення інформаційного суспільства – вдосконалення системи

телекомунікацій, розвиток універсальних послуг на рівні світових стандартів, експорт програмного забезпечення у розвинуті країни світу. Індійська стратегія реформування передбачає інтенсивну інтеграцію азійської країни в глобальне інформаційне співтовариство.

ПИТАННЯ № 3. Стан розвитку інформаційного суспільства в Україні.

Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 09.01.2007 № 537-V.

Завдання, цілі та напрями розвитку інформаційного суспільства в Україні.

Основним завданням розвитку інформаційного суспільства в Україні є сприяння кожній людині на засадах широкого використання сучасних ІКТ можливостей створювати інформацію і знання, користуватися та обмінюватися ними, виробляти товари та надавати послуги, повною мірою реалізуючи свій потенціал, підвищуючи якість свого життя і сприяючи сталому розвитку країни на основі цілей і принципів, проголошених Організацією Об'єднаних Націй, Декларації принципів та Плану дій, напрацьованих на Всесвітніх зустрічах на вищому рівні з питань інформаційного суспільства (Женева, грудень 2003 року; Туніс, листопад 2005 року) та Постанови Верховної Ради України від 1 грудня 2005 року «Про Рекомендації парламентських слухань з питань розвитку інформаційного суспільства в Україні».

Основні стратегічні цілі розвитку інформаційного суспільства в Україні:
прискорення розробки та впровадження новітніх конкурентоспроможних ІКТ в усі сфери суспільного життя, зокрема в економіку України і в діяльність органів державної влади та органів місцевого самоврядування;

забезпечення комп'ютерної та інформаційної грамотності населення, насамперед шляхом створення системи освіти, орієнтованої на використання новітніх ІКТ у формуванні всебічно розвиненої особистості;

розвиток національної інформаційної інфраструктури та її інтеграція із світовою інфраструктурою;

державна підтримка нових "електронних" секторів економіки (торгівлі, надання фінансових і банківських послуг тощо);

створення загальнодержавних інформаційних систем, насамперед у сферах охорони здоров'я, освіти, науки, культури, охорони довкілля;

збереження культурної спадщини України шляхом її електронного документування;

державна підтримка використання новітніх ІКТ засобами масової інформації;

використання ІКТ для вдосконалення державного управління, відносин між державою і громадянами, становлення електронних форм взаємодії між органами державної влади та органами місцевого самоврядування і фізичними та юридичними особами;

досягнення ефективної участі всіх регіонів у процесах становлення інформаційного суспільства шляхом децентралізації та підтримки регіональних і місцевих ініціатив;

захист інформаційних прав громадян, насамперед щодо доступності інформації, захисту інформації про особу, підтримки демократичних інститутів та мінімізації ризику "інформаційної нерівності";

вдосконалення законодавства з регулювання інформаційних відносин;

покращення стану інформаційної безпеки в умовах використання новітніх ІКТ.

Основними напрямками розвитку інформаційного суспільства в Україні визначити:

формування та впровадження правових, організаційних, науково-технічних, економічних, фінансових, технологічних, методичних умов розвитку інформаційного суспільства в Україні з урахуванням світових тенденцій;

всебічний розвиток загальнодоступної інформаційної інфраструктури на засадах сприяння вітчизняному виробництву новітніх ІКТ та інформаційно-телекомунікаційних систем, подолання технічної і технологічної залежності від зарубіжних виробників;

забезпечення вільного доступу населення до телекомунікаційних послуг, зокрема до мережі Інтернет, ІКТ та інформаційних ресурсів;

збільшення різноманітності та кількості послуг населенню та бізнесу, що надаються за допомогою ІКТ;

створення загальнодоступних електронних інформаційних ресурсів на основі врахування національних, світоглядних, політичних, економічних, культурних та інших аспектів розвитку України;

надання кожній людині можливості для здобуття знань, умінь і навичок з використанням ІКТ під час навчання, виховання та професійної підготовки;

створення умов для забезпечення комп'ютерної та інформаційної грамотності усіх верств населення, створення системи мотивацій щодо впровадження і використання ІКТ для формування широкого попиту на такі технології в усіх сферах життя суспільства;

забезпечення участі громадськості в побудові інформаційного суспільства, забезпечення конституційних прав людини, суспільства та держави в інформаційній сфері;

розробку та впровадження системи індикаторів розвитку інформаційного суспільства в Україні з внесенням відповідних змін у систему державних статистичних спостережень з узгодженням їх з міжнародними стандартами і методологією та щорічним їх оприлюдненням.

Запровадження засад взаємодії учасників побудови інформаційного суспільства передбачає, що це суспільство розбудовується за умови співпраці і солідарності громадян, приватного сектору економіки, органів державної влади та органів місцевого самоврядування, відповідних об'єднань громадян, коли:

органи державної влади визначають пріоритети розвитку, забезпечують їх досягнення і всебічну підтримку, координують та стимулюють виконання завдань, формують законодавчу базу і контролюють її виконання всіма учасниками побудови інформаційного суспільства;

приватний сектор економіки, здебільшого, забезпечує впровадження та використання ІКТ у всіх сферах життя, вдосконалює інформаційну інфраструктуру, надає інформаційні та комунікаційні послуги тощо;

об'єднання громадян взаємодіють з органами державної влади, органами місцевого самоврядування і приватним сектором економіки у питаннях забезпечення справедливого та рівного доступу до інформаційних і комунікаційних послуг, формують громадську думку щодо пріоритетів та перспектив розвитку інформаційного суспільства;

державна, приватний сектор економіки та об'єднання громадян сприяють встановленню і розширенню взаємовигідних відносин з міжнародними організаціями, в тому числі з міжнародними фінансовими установами, які відіграють провідну роль у розвитку інформаційного суспільства та оцінці прогресу в цій сфері.

Національна політика розвитку інформаційного суспільства в Україні ґрунтується на засадах: пріоритетності науково-технічного та інноваційного розвитку держави; формування необхідних для цього законодавчих і сприятливих економічних умов; всебічного розвитку загальнодоступної інформаційної інфраструктури, інформаційних ресурсів та забезпечення повсюдного доступу до телекомунікаційних послуг та ІКТ; сприяння збільшенню різноманітності та кількості електронних послуг, забезпеченню створення загальнодоступних електронних інформаційних ресурсів; поліпшення кадрового потенціалу; посилення мотивації щодо використання ІКТ; широкого впровадження ІКТ в науку, освіту, культуру, охорону здоров'я, охорону навколишнього середовища; забезпечення інформаційної безпеки.

Така політика передбачає:

1. Перехід до пріоритетного науково-технічного та інноваційного розвитку.
2. Законодавче забезпечення розвитку інформаційного суспільства.
3. Формування сприятливих економічних умов розвитку інформаційного суспільства.
4. Розвиток загальнодоступної інформаційної інфраструктури.
5. Забезпечення повсюдного доступу до телекомунікаційних послуг та інформаційних ресурсів.
6. Сприяння збільшенню різноманітності та кількості електронних послуг.
7. Забезпечення створення загальнодоступних електронних інформаційних ресурсів.
8. Підготовка людини для роботи в інформаційному суспільстві.
9. Створення системи мотивацій щодо впровадження і використання ІКТ.

10. Наука та культура в інформаційному суспільстві.
11. Охорона здоров'я в інформаційному суспільстві.
12. Охорона навколишнього природного середовища.
13. Інформаційна безпека в інформаційному суспільстві.

Організаційно-правові основи розвитку інформаційного суспільства в Україні включають: інституційне, організаційне та ресурсне забезпечення; відповідні об'єднання громадян; механізми інтеграції України у світовий інформаційний простір та механізми реалізації Основних засад розвитку інформаційного суспільства в Україні на 2007-2015 роки.

Стратегія розвитку інформаційного суспільства в Україні: мета, принципи, завдання, етапи та основні напрями реалізації.

Розпорядження Кабінету Міністрів України «Про схвалення Стратегії розвитку інформаційного суспільства в Україні» від 15 травня 2013 року № 386-р.

Метою реалізації Стратегії є формування сприятливих умов для розбудови інформаційного суспільства, соціально-економічного, політичного і культурного розвитку держави з ринковою економікою, що керується європейськими політичними та економічними цінностями, підвищення якості життя громадян, створення широких можливостей для задоволення потреб і вільного розвитку особистості, підвищення конкурентоспроможності України, вдосконалення системи державного управління за допомогою інформаційно-комунікаційних технологій.

Для розвитку інформаційного суспільства необхідно застосовувати **принципи:**

- рівноправного партнерства державних органів, громадян і бізнесу;
- прозорості та відкритості діяльності державних органів;
- гарантованості права на інформацію, вільного отримання та поширення інформації, крім обмежень, установлених законом;
- свободи вираження поглядів і переконань;
- правомірності одержання, використання, поширення, зберігання та захисту інформації;
- інформаційної безпеки;
- постійного навчання;
- підконтрольності та підзвітності державних органів громадськості;
- сприяння пріоритетному розвитку інформаційно-комунікаційних технологій;

- чіткого розмежування повноважень і скоординованої взаємодії державних органів;

- гарантованості повного ресурсного забезпечення національних програм та проектів розвитку інформаційного суспільства.

Основні **стратегічні цілі** розвитку інформаційного суспільства та суспільства знань визначено в Законі України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки”, які з урахуванням сучасного стану та тенденцій розвитку України включають:

прискорення процесу розроблення та впровадження сучасних інформаційно-комунікаційних технологій у державне управління, охорону здоров'я, культуру, освіту, науку, охорону навколишнього природного середовища, бізнес тощо;

розвиток електронної економіки;

забезпечення комп'ютерної та інформаційної грамотності громадян насамперед шляхом створення системи освіти, орієнтованої на використання новітніх інформаційно-комунікаційних технологій у формуванні всебічно розвиненої особистості, та забезпечення неперервності навчання;

розвиток національної інформаційної інфраструктури та її інтеграція до світової інфраструктури;

підвищення якості та доступності адміністративних послуг, спрощення процедур їх надання і скорочення відповідних витрат, деперсоніфікація надання адміністративних послуг як інструмент зниження рівня корупції;

розвиток електронної демократії;

збереження культурної спадщини України шляхом документування її об'єктів на цифрових носіях, забезпечення накопичення і збереженості електронних документів та електронних інформаційних ресурсів;

досягнення ефективної участі регіонів України у процесах становлення інформаційного суспільства, підтримку регіональних і місцевих ініціатив;

захист інформаційних прав громадян та організацій, авторського права, підтримку демократичних інститутів та мінімізацію ризиків "інформаційної нерівності";

захист персональних даних;

забезпечення відкритості інформації про діяльність державних органів та органів місцевого самоврядування, розширення доступу до неї та надання можливості безпосередньої участі як інститутів громадянського суспільства, так і громадян у процесах підготовки і проведення експертизи проектів актів законодавства, здійснення контролю за результативністю і ефективністю діяльності органів державної влади та органів місцевого самоврядування;

удосконалення інформаційного законодавства;

поліпшення стану інформаційної безпеки.

Основними завданнями розвитку інформаційного суспільства в Україні є:

сприяння кожному громадянину на засадах широкого використання сучасних інформаційно-комунікаційних технологій у створенні інформації і знань, їх використанні та обміні ними, виробництві товарів та наданні послуг;

забезпечення гарантій волевиявлення і самореалізації громадянина в інформаційному суспільстві, а також вільного доступу до інформації та знань, крім установлених законом обмежень;

повномасштабне входження України до глобального інформаційного простору;

прискорений розвиток інформаційного сектору економіки, який активно взаємодіє з іншими секторами економіки з метою підвищення темпів економічного зростання;

впровадження новітніх інформаційно-комунікаційних технологій в усі сфери суспільного життя, діяльність державних органів та органів місцевого самоврядування, у тому числі в процесі реалізації Ініціативи “Партнерство “Відкритий уряд” та електронного урядування;

гармонізація національного законодавства з європейським, дотримання цілей і принципів, проголошених Організацією Об’єднаних Націй, Декларацією принципів та Плану дій, напрацьованих на Всесвітніх зустрічах на вищому рівні з питань інформаційного суспільства.

Етапи та основні напрями реалізації.

Реалізація Стратегії передбачається у 2013–2020 роках.

На першому етапі реалізації Стратегії (2013–2015 роки) необхідно досягти цілей та виконати завдання, що визначені Законом України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки”, внести зміни до плану заходів з виконання завдань, передбачених Законом України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки”, затвердженого розпорядженням Кабінету Міністрів України від 15 серпня 2007 р. № 653, з метою його актуалізації. Необхідно забезпечити розроблення та прийняття Інформаційного кодексу України, Закону України “Про електронну комерцію”, внести зміни до нормативно-правових актів щодо Національної програми інформатизації, розробити базові норми, правила і регламенти створення, впровадження, модернізації та експлуатації інформаційних ресурсів, інформаційних, інформаційно-аналітичних, інформаційно-телекомунікаційних систем та засобів інформатизації органів державної влади, а також визначити порядок здійснення контролю за дотриманням таких правил, норм та регламентів.

На другому етапі (2016–2020 роки) передбачається гармонізувати досягнення розвитку інформаційного суспільства в Україні із загальносвітовими та досягти:

розбудови інформаційної інфраструктури для забезпечення доступу громадян до інформаційних послуг та інформаційно-комунікаційних технологій;

спрощення процедури доступу громадян до інформації та знань за допомогою інформаційно-комунікаційних технологій, крім обмежень, установлених законом;

забезпечення сталого розвитку національної економіки за допомогою новітніх інформаційно-комунікаційних технологій, насамперед е-економіки та е-комерції з використанням інформаційно-комунікаційних технологій;

підвищення ефективності та якості державного управління з надання адміністративних послуг в електронній формі, прозорості та відкритості діяльності державних органів, активності громадян та організацій у формуванні та реалізації державної політики, здійснення контролю за діяльністю державних органів;

широке впровадження інформаційно-комунікаційних технологій в освіту, культуру, архівну справу, охорону здоров’я, охорону навколишнього природного середовища тощо;

посилення мотивації до використання інформаційно-комунікаційних технологій;

забезпечення інформаційної безпеки;

запровадження системи індикаторів розвитку інформаційного суспільства в Україні;

забезпечення подальшого розвитку Національної системи конфіденційного зв'язку як інтегрованої основи для загальнодержавних інформаційних систем електронної взаємодії державних органів;

поліпшення кадрового потенціалу у сфері інформаційно-комунікаційних технологій.

Основними напрямками реалізації Стратегії за зазначеними етапами є розвиток таких сфер суспільного життя: інформаційна інфраструктура, доступ до інформації та знань, е-економіка, електронне урядування, е-демократія, е-освіта, наука та інновації, е-культура, е-медицина, охорона навколишнього природного середовища, інформаційна безпека, міжнародне співробітництво.

4. Підведення підсумків.

Таким чином, на сьогоднішній лекції ми надали характеристику інформації як стратегічної сировини XXI століття, визначили концепцію інформаційного суспільства та типи і моделі його побудови, стратегії розвитку інформаційного суспільства в Україні, а також оволоділи практичними вміннями та навичками правильного тлумачення та застосування заходів інформаційної протидії, необхідних для майбутньої трудової діяльності як фахівців у сфері міжнародної інформаційної безпеки.

Тема 2. Інформаційна безпека в контексті національної безпеки держави

ЛЕКЦІЯ 2. Інформаційна безпека в контексті національної безпеки держави (ч. 1)

Навчальні питання:

1. Засади національної безпеки України.

Закон України «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII.

Національна безпека України – захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз;

Національні інтереси України – життєво важливі інтереси людини, суспільства і держави, реалізація яких забезпечує державний суверенітет України, її прогресивний демократичний розвиток, а також безпечні умови життєдіяльності і добробут її громадян;

Основними принципами, що визначають порядок формування державної політики у сферах національної безпеки і оборони, є:

1) верховенство права, підзвітність, законність, прозорість та дотримання засад демократичного цивільного контролю за функціонуванням сектору безпеки і оборони та застосуванням сили;

2) дотримання норм міжнародного права, участь в інтересах України у міжнародних зусиллях з підтримання миру і безпеки, міждержавних системах та механізмах міжнародної колективної безпеки;

3) розвиток сектору безпеки і оборони як основного інструменту реалізації державної політики у сферах національної безпеки і оборони.

Фундаментальними національними інтересами України є:

1) державний суверенітет і територіальна цілісність, демократичний конституційний лад, недопущення втручання у внутрішні справи України;

2) сталий розвиток національної економіки, громадянського суспільства і держави для забезпечення зростання рівня та якості життя населення;

3) інтеграція України в європейський політичний, економічний, безпековий, правовий простір, набуття членства в Європейському Союзі та в Організації Північноатлантичного договору, розвиток рівноправних взаємовигідних відносин з іншими державами.

Основні цілі Стратегії національної безпеки України:

мінімізація загроз державному суверенітету та створення умов для відновлення територіальної цілісності України у межах міжнародно-визнаного державного кордону України, гарантування мирного майбутнього України як суверенної і незалежної, демократичної, соціальної, правової держави;

утвердження прав і свобод людини і громадянина, забезпечення нової якості економічного, соціального і гуманітарного розвитку, забезпечення інтеграції України до Європейського Союзу та формування умов для вступу в НАТО.

Актуальні загрози національній безпеці України: агресивні дії Росії, що здійснюються для виснаження української економіки і підриву суспільно-політичної стабільності з метою знищення держави Україна і захоплення її території; неефективність системи забезпечення національної безпеки і оборони України; корупція та неефективна система державного управління; економічна криза, виснаження фінансових ресурсів держави, зниження рівня життя населення; загрози енергетичній безпеці; загрози інформаційній безпеці; загрози кібербезпеці і безпеці інформаційних ресурсів; загрози безпеці критичної інфраструктури; загрози екологічній безпеці.

Основні напрями державної політики національної безпеки України: 1. Відновлення територіальної цілісності України; 2. Створення ефективного сектору безпеки і оборони; 3. Підвищення обороноздатності держави; 4. Реформування та розвиток розвідувальних, контррозвідувальних і правоохоронних органів; 5. Реформування системи державного управління, нова якість антикорупційної політики; 6. Інтеграція в Європейський Союз; 7. Особливе партнерство з НАТО; 8. Забезпечення національної безпеки у зовнішньополітичній сфері; 9. Забезпечення економічної безпеки; 10. Забезпечення енергетичної безпеки; 11. Забезпечення інформаційної безпеки;

12. Забезпечення кібербезпеки і безпеки інформаційних ресурсів; 13. Забезпечення безпеки критичної інфраструктури; 14. Забезпечення екологічної безпеки.

2. Національний інформаційний простір.

Поняття інформаційного простору та інформаційної сфери.

На сьогодні існує безліч наукових підходів до тлумачення інформаційного простору. Як синонім застосовується поняття «інформаційна сфера». Термін «інформаційний простір» застосовують, як правило, для позначення системи зовнішніх та внутрішньоорганізаційних потоків інформації, які, у свою чергу, можуть мати різні характеристики з погляду змісту, методів, передачі та інтенсивності обміну інформацією. «Сукупність інформації, інформаційної інфраструктури, суб'єктів, що здійснюють збір, формування, поширення і використання інформації, а також системи регулювання відповідних суспільних відносин, розглядається як інформаційна сфера».

Структура інформаційного простору. Інформаційні поля та інформаційні потоки є основними структурними складовими інформаційного простору.

Інформаційне поле – це сукупність усієї зосередженої в просторі інформації, безвідносно до її форми і стану, що знаходиться у відриві як від об'єкта відображення, так і від суб'єкта сприйняття. Рух інформації в інформаційному полі здійснюється за допомогою фізичного зв'язку між одержувачем і джерелом інформації, що матеріалізується в інформаційному потоці.

Інформаційний потік – це сукупність інформації, що переміщується в інформаційному просторі через канали комунікації. Інформаційні потоки можуть протікати як усередині окремих інфосфер, так і між ними, залежно від наявності каналів комунікації.

До складу технологічних та організаційних компонентів інформаційного простору відносять **інформаційну інфраструктуру** – середовище, яке забезпечує можливість збору, передачі, зберігання, автоматизованої обробки і розповсюдження інформації в суспільстві..

Функції інформаційного простору.

інтегруюча;

комунікативна;

актуалізуюча;

геополітична.

Співвідношення понять «інформаційний простір» та «кіберпростір».

Інформаційний простір – глобальне інформаційне середовище, яке в реальному масштабі часу забезпечує комплексну обробку відомостей про протидію сторони та їх навколишнє оточення в інтересах підтримки прийняття рішень по створенню оптимального, для досягнення поставлених цілей, складу сил і засобів та їх ефективного застосування в різних умовах обстановки.

Кіберпростір – середовище, яке виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних (автоматизованих), телекомунікаційних та інформаційно-телекомунікаційних систем.

Поняття та основні характеристики національного інформаційного простору.

Історично склалося так, що інформаційний простір володіє національно-специфічними способами побудови. Тому в контексті нашої держави застосовується категорія «Національного інформаційного простору України». Національний інформаційний простір України – сфера (об’ємний простір), у якій здійснюються інформаційні процеси і на яку поширюється юрисдикція України». Національний інформаційний простір – сукупність всіх інформаційних потоків як національного, так й іноземного походження, які доступні на території держави.

Основні характеристики національного інформаційного простору: територія, на яку державою безпосередньо, чи опосередковано поширюється інформаційний вплив; структурованість інформаційного простору; інтенсивність інформаційних потоків.

Мета формування і розвитку національного інформаційного простору України полягає у формуванні сучасної моделі державної інформаційної політики, а також створенні політико-правових, економічних, організаційних та матеріально-технічних умов забезпечення розвитку та захисту національного інформаційного простору.

Інформаційний простір у мережі Інтернет: правове регулювання та контроль. Питання адміністрування адресного простору українського сегмента мережі Інтернет, реєстру домену.UA в координації з міжнародною системою адміністрування мережі Інтернет урегульовано нормами Закону України від 18.11.2003 № 1280-IV “Про телекомунікації” (ст. 56), у якому на Національну комісію, що здійснює державне регулювання у сфері зв’язку та інформатизації, покладено функцію контролю за дотриманням умов застосування технічних засобів у телекомунікаційних мережах загального користування (п. 7 ст. 24).

У цьому зв’язку в Україні створені та діють суб’єкти таких адміністративно-правових відносин, пов’язаних із контролем інформаційного простору, зокрема: Національна комісія, що здійснює державне регулювання у сфері зв’язку та інформатизації, Національна рада України з питань телебачення і радіомовлення, Державний комітет телебачення та радіомовлення України. Діяльність названих органів та виконувані ними функції регулюються численними законодавчими і нормативно-правовими актами.

Щодо контролю інформаційного простору в мережі Інтернет, то детальне вивчення наукових джерел і зарубіжного досвіду дозволяє зробити висновки щодо методів контролю інформаційного простору в мережі Інтернет, до яких належать:

- 1) блокування або заборона доступу до сайтів, що містять інформацію,

яка порушує чинне в тій чи іншій країні законодавство (застосовується в Австралії, Азербайджані, Алжирі, Бахреїні, Білорусі, Бельгії, Бірмі, В'єтнамі, Німеччині, Данії, Єгипті, Зімбабве, Індії, Йорданії, Іраку (під контролем США), Ірані, Італії, Казахстані, Канаді, Киргизії, Китаї, Кубі, Малайзії, ОАЕ, Пакистані, Саудівській Аравії, Південній Кореї, Північній Кореї, Сінгапурі, Сирії, Таїланді, Тунісі, Туркменістані, Туреччині, Узбекистані);

2) фільтрування інформаційного потоку в місцях загального користування (інтернет-кафе, навчальні заклади, підприємства) – передбачає обмеження доступу до інформації на основі “чорних списків” – заборони доступу до адрес, що містяться в списку (Китай, Російська Федерація) чи “білих списків” – дозволу доступу тільки до конкретних адрес (Північна Корея), а також за ключовими словами;

3) відстеження активності інтернет-користувачів (Російська Федерація), перлюстрація повідомлень;

4) авторизація користувачів при доступі в інтернет із застосуванням провайдерів програмних чи апаратних засобів (Білорусь, Алжир, Іран).

ЛЕКЦІЯ 3. Інформаційна безпека в контексті національної безпеки держави (ч. 2)

Навчальні питання:

3. Поняття та зміст інформаційної безпеки держави.

Підходи до визначення поняття «інформаційна безпека».
Співвідношення понять «інформаційна безпека» та «кібернетична безпека (кібербезпека)». **Інформаційна безпека** – стан та умови захищеності інформаційного середовища суспільства, який забезпечує його формування, використання та розвиток в інтересах громадян, організацій, держави, включених у це інформаційне середовище.

У проекті Концепції інформаційної безпеки України **інформаційна безпека** – стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоечасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій.

Кібернетична безпека (кібербезпека) – стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі.

Пріоритети забезпечення інформаційної безпеки відповідно до Закону України «Про Національну безпеку»:

забезпечення наступальності заходів політики інформаційної безпеки на основі асиметричних дій проти всіх форм і проявів інформаційної агресії;

створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них;

протидія інформаційним операціям проти України, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації, захист національних цінностей та зміцнення єдності українського суспільства;

розробка і реалізація скоординованої інформаційної політики органів державної влади;

виявлення суб'єктів українського інформаційного простору, що створені та/або використовуються Росією для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності;

створення і розвиток інститутів, що відповідають за інформаційно-психологічну безпеку, з урахуванням практики держав-членів НАТО;

удосконалення професійної підготовки у сфері інформаційної безпеки, упровадження загальнонаціональних освітніх програм з медіакультури із залученням громадянського суспільства та бізнесу.

Суб'єкти та механізми забезпечення інформаційної безпеки України. Суб'єктами забезпечення інформаційної безпеки є: громадяни України, об'єднання громадян, громадські організації та інші інститути громадянського суспільства; Президент України, Верховна Рада України, Кабінет Міністрів України, інші центральні органи виконавчої влади та органи сектору безпеки і оборони України; засоби масової інформації та комунікації різних форм власності, підприємства, заклади, установи та організації різних форм власності, що здійснюють інформаційну діяльність; наукові установи, освітні і навчальні заклади України, які, зокрема, здійснюють наукові дослідження та підготовку фахівців за різними напрямками інформаційної діяльності, в галузі інформаційної безпеки.

2. Доктрина інформаційної безпеки України.

Мета та принципи Доктрини інформаційної безпеки України. Метою Доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни.

Доктрина базується на **принципах** додержання прав і свобод людини і громадянина, поваги до гідності особи, захисту її законних інтересів, а також законних інтересів суспільства та держави, забезпечення суверенітету і територіальної цілісності України.

Національні інтереси України в інформаційній сфері:

1) життєво важливі інтереси особи: забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; забезпечення конституційних прав людини на захист приватного життя; захищеність від руйнівних інформаційно-психологічних впливів;

2) життєво важливі інтереси суспільства і держави.

Актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері:

здійснення спеціальних інформаційних операцій, спрямованих на підриив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів,

підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні;

проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі;

інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах;

інформаційне домінування держави-агресора на тимчасово окупованих територіях;

недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України;

неефективність державної інформаційної політики, недосконалість законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіа-культури суспільства;

поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні.

Пріоритети державної політики в інформаційній сфері:

створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них;

удосконалення повноважень державних регуляторних органів, які здійснюють діяльність щодо інформаційного простору держави, з метою досягнення адекватного рівня спроможності держави відповідати реальним та потенційним загрозам національним інтересам України в інформаційній сфері;

законодавче врегулювання механізму виявлення, фіксації, блокування та видалення з інформаційного простору держави, зокрема з українського сегмента мережі Інтернет, інформації, яка загрожує життю, здоров'ю громадян України, пропагує війну, національну та релігійну ворожнечу, зміну конституційного ладу насильницьким шляхом або порушення територіальної цілісності України, загрожує державному суверенітету, пропагує комуністичний та/або націонал-соціалістичний (нацистський) тоталітарні режими та їхню символіку;

визначення механізмів регулювання роботи підприємств телекомунікацій, поліграфічних підприємств, видавництв, телерадіоорганізацій, телерадіоцентрів та інших підприємств, установ, організацій, закладів культури та засобів масової інформації, а також використання місцевих радіостанцій, телевізійних центрів та друкарень для військових потреб і проведення роз'яснювальної роботи серед військ та населення; заборони роботи приймально-передавальних радіостанцій особистого та колективного користування і передачі інформації через комп'ютерні мережі в умовах запровадження правового режиму воєнного стану та ін.

Механізм реалізації Доктрини інформаційної безпеки України.
Визначення повноважень таких органів, як: Рада національної безпеки і оборони України, Кабінет Міністрів України, Міністерство інформаційної політики України, Міністерство інформаційної політики України, Міністерство закордонних справ України, Міністерство оборони України, Міністерство культури України, Державне агентство України з питань кіно, Національна рада України з питань телебачення і радіомовлення, Державний комітет телебачення і радіомовлення України, Служба безпеки України, Розвідувальні органи України, Державна служба спеціального зв'язку та захисту інформації України, Національний інститут стратегічних досліджень.

Тема 3. Основні поняття інформаційного протиборства

ЛЕКЦІЯ 4. Основні поняття інформаційного протиборства

Навчальні питання:

1. Види загроз інформаційній безпеці України.

Загрози комунікативного характеру в сфері реалізації потреб людини і громадянина, суспільства та держави щодо продукування, споживання, розповсюдження та розвитку національного стратегічного контенту та інформації:

1) зовнішні негативні інформаційні впливи на свідомість людини та спільноти через засоби масової інформації, а також мережу Інтернет, що здійснюються на шкоду державі;

2) інформаційний вплив на населення України, у тому числі на особовий склад військових формувань, мобілізаційний резерв, з метою послаблення їх готовності до оборони держави та погіршення іміджу військової служби;

3) поширення суб'єктами інформаційної діяльності викривленої, недостовірної та упередженої інформації для дискредитації органів державної влади, дестабілізації суспільно-політичної ситуації, що значно ускладнює прийняття політичних рішень, завдає шкоди національним інтересам України чи створює негативний імідж України;

4) загрози свободі слова;

5) створення, розповсюдження, передача та зберігання інформації з метою підтримки, супроводження чи активізації злочинної та терористичної діяльності.

Загрози технологічного характеру в сфері функціонування та захищеності кібернетичних, телекомунікаційних та інших автоматизованих систем, що формують матеріальну (технічну, інструментальну) основу внутрішньодержавного інформаційного простору:

1) використання іноземними державами кібервійськ, кіберпідрозділів, нових видів інформаційної зброї та зброї кібернетичного характеру на шкоду Україні;

2) прояви кіберзлочинності, кібертероризму чи кібернетичної військової агресії, що загрожують сталому та безпечному функціонуванню національних інформаційно- телекомунікаційних систем, шляхом втручання, не

санкціонованого доступу або порушення функціонування телекомунікаційних, кібернетичних, автоматизованих комп'ютерних систем, незалежно від форми власності;

3) недостатній рівень розвитку національної інформаційної інфраструктури;

4) порушення порядку доступу, поводження та встановлених регламентів збору, обробки, зберігання, поширення чи передачі інформації, яка захищається державою (державна таємниця, конфіденційна інформація, персональні дані, авторські права чи інтелектуальна власність), або роботи з інформаційними ресурсами, що її містять;

5) відсутність громадського контролю за діяльністю суб'єктів забезпечення інформаційної безпеки, захищеністю національної інформаційної інфраструктури та інформаційного простору України.

Інформаційний тероризм – злиття фізичного насильства зі злочинним використанням інформаційних систем, а також умисне зловживання цифровими інформаційними системами, мережами або їх компонентами з метою сприяння здійсненню терористичних операцій або акцій.

2. Поняття та зміст інформаційного протиборства.

Інформаційне протиборство – суперництво соціальних систем (країн, блоків країн) в інформаційній сфері з приводу впливу на ті або інші сфери соціальних відносин і встановлення контролю над джерелами стратегічних ресурсів, у результаті якого одна група учасників суперництва отримує переваги, необхідні їм для подальшого розвитку.

За інтенсивністю, масштабами та засобами, які використовуються, виділяють наступні **ступені інформаційного протиборства**: інформаційна експансія, інформаційна агресія та інформаційна війна.

Інформаційна експансія – діяльність із досягнення національних інтересів методом безконфліктного проникнення в інформаційну сферу а метою: поступової, плавної, непомітної для суспільства зміни системи соціальних відносин за зразком системи джерела експансії; витіснення положень національної ідеології і національної системи цінностей і заміщення їх власними цінностями й ідеологічними установками; збільшення ступеня свого впливу та присутності, встановлення контролю над стратегічними інформаційними ресурсами, інформаційно-телекомунікаційною структурою і національними ЗМІ; нарощування присутності власних ЗМІ в інформаційній сфері об'єкта проникнення і т.п.

Інформаційна агресія – незаконні дії однієї зі сторін в інформаційній сфері, спрямовані на нанесення супротивнику конкретної, відчутної шкоди в окремих областях його діяльності шляхом обмеженого та локального по своїх масштабах застосування сили.

Інформаційна війна – це найвищий ступінь інформаційного протиборства, спрямований на розв'язання суспільно-політичних, ідеологічних, а також національних, територіальних та інших конфліктів між державами, народами, націями, класами й соціальними групами шляхом широкомасштабної реалізації засобів і методів інформаційного насильства

(інформаційної зброї).

Основними **формами інформаційного протидорства** на державному рівні є: політичні, дипломатичні й економічні акції; інформаційні та психологічні операції; підривні та деморалізуючі пропагандистські дії; сприяння опозиційним і дисидентським рухам; надання усебічного впливу на політичне і культурне життя з метою розвалу національно-державних підвалин суспільства; проникнення в систему державного керування.

Основним завданням інформаційної боротьби є: отримання розвідувальної інформації шляхом перехоплення та розшифрування інформаційних потоків, що передаються по каналах зв'язку, а також по побічним випромінюванням, а також за рахунок спеціального втілення технічних засобів перехоплення інформації; отримання потрібної інформації шляхом перехоплення й обробки відкритої інформації, що передається через незахищені канали зв'язку, циркулює в інформаційних системах, а також опублікованої у відкритих джерелах та ЗМІ; електромагнітний вплив на елементи інформаційних і телекомунікаційних систем; психологічний вплив, спрямований проти персоналу та осіб, що приймають рішення; формування і масоване розповсюдження через інформаційні канали противника та глобальні мережі дезінформації та тенденційної інформації; вогневе придушення (у воєнний час) елементів інфраструктури державного і воєнного управління; здійснення несанкціонованого доступу до інформаційних ресурсів з подальшим їх викривленням, знищенням або викраденням, або порушенням нормального функціонування таких систем; захист від аналогічних впливів з боку противника.

До **основних форм ведення інформаційної боротьби** звичайно відносять наступні: інформаційна операція; інформаційна битва; інформаційна дія (акція); інформаційний удар.

Усі **способи інформаційної боротьби** можна поділити на три основні категорії: силові, інтелектуальні і комбіновані, а також за аналогією із збройною боротьбою виділити дві основні групи способів: наступальні і оборонні.

Інформаційна зброя та її особливості. **Інформаційна зброя** – це сукупність засобів і технологій, призначених для ведення інформаційної боротьби.

За об'єктами впливу інформаційну зброю можна поділити на два основних класи:

1. Інформаційно-технічна зброя, що впливає на інформаційні ресурси, інформаційну інфраструктуру збройних сил, держави в цілому.

2. Інформаційно-психологічна зброя, що впливає на морально-психологічний стан людини, соціальних та інших груп населення, суспільства в цілому.

Особливості інформаційної зброї: скритність; масштабність; універсальність; економічність.

Завдання захисту національного інформаційного простору за досвідом ведення гібридної війни на сході України:

- розроблення нормативно-правової бази стосовно засад державної політики у сфері інформаційної безпеки, яка б визначала взаємодію силових структур України з місцевими органами самоврядування, державними (недержавними) установами, громадсько-політичними організаціями, ЗМІ тощо;
- створення єдиного міжвідомчого органу, який здійснюватиме керівництво, координацію та контроль заходів інформаційної безпеки, зокрема інформаційного протидіювання (наприклад, міжвідомча комісія при РНБО);
- завершення формування національної системи забезпечення інформаційної безпеки, адекватної масштабам і спрямованості загроз;
- створення системи комплексного моніторингу матеріалів популярних аудіовізуальних та друкованих ЗМІ, а також популярних Інтернет-ресурсів;
- створення нової комунікаційної стратегії, здатної швидко й ефективно реагувати на сучасні виклики та загрози, а також визначити та оцінити їх характер і значущість;
- формування державної програми, спрямованої на підвищення в суспільстві рівня медіаграмотності (розуміння небезпеки від негативного інформаційного впливу);
- узаконення діяльності, використання за єдиним замислом ресурсу працівників недержавних установ, звичайних громадян України для виконання завдань захисту інформаційного простору та протидії інформаційним і кібернетичним заходам;
- продовження створення системи національного інформування для формування об'єктивної думки про події в Україні, зокрема за кордоном;
- забезпечення специфічними засобами, які б сприяли на сучасному рівні розвитку інформаційних технологій вирішенню завдання захисту об'єктів інформаційної інфраструктури держави та вжиттю превентивних заходів;
- удосконалення системи наукових досліджень у сфері інформаційної безпеки.

Тема 4. Досвід захисту національного інформаційного простору в інших країнах

ЛЕКЦІЯ 5. Досвід захисту національного інформаційного простору в інших країнах

Навчальні питання:

1. Захист національного інформаційного простору в США. У значній кількості офіційних документів США, зокрема в Доповіді комісії з національної оборони, констатується, що «проблеми ХХІ століття будуть якісно і кількісно відмінними від тих, які були характерними для періоду холодної війни, у зв'язку з чим стануть необхідними докорінні зміни інститутів національної безпеки, воєнної стратегії та підходів до питань оборони до 2020 року».

У США в процесі виникнення та розвитку новітніх інформаційних технологій, формування та становлення інформаційного суспільства було сформульовано декілька підходів щодо захисту інформаційного простору держави.

Одна з моделей передбачала створення значної переваги держави в наступальних видах озброєнь, у знешкодженні систем захисту держави-супротивника засобами інформаційного впливу, координації дій із союзними державами з використаннями визначених засобів інформаційної зброї для ідентифікації будь-яких джерел і типів інформаційних загроз.

Практичне втілення цієї моделі спостерігалось під час проведення інформаційної операції "Союзницька сила" (1999 р.), яку США та інші держави-члени НАТО здійснили проти Союзної Федеративної Республіки Югославія.

Інша модель, яка розглядалась в політичних колах США, передбачала наявність кількох держав-інфолідерів та потенційного протистояння між ними, визначення фактору стримування експансії інформаційних загроз, а в перспективі – забезпечення домінування США у сфері міжнародної ІБ з можливостями значного впливу на глобальну інфосферу та переважного права вирішення проблем глобального світового порядку.

2. Принципи та особливості системи інформаційної безпеки Японії.

Згідно з даними про кількість користувачів кіберпростору в Азіатсько-Тихоокеанському регіоні, Японія займає третє місце – в країні офіційно налічується понад 117,6 млн користувачів мережі при населенні 126 млн. У світовому кіберпросторі Японія сьогодні являє собою мету високо рівня важливості- у військовому, економічному і технологічному плані.

Традиційно Японія займає високі місця за кількістю кіберінцидентів і зараз знаходиться на 11 місці в списку країн світу серед джерел кібератак і на 16 серед реципієнтів кібератак. При цьому високі місця у всіх рейтингах хакерської активності займають сусідній Китай і основний союзник Японії – Сполучені Штати.

Уряд Японії постійно оновлює свою стратегію кібербезпеки. З моменту публікації в 2006 р «Першої національної стратегії інформаційної безпеки» в неї кілька разів вносилися зміни і доповнення. У Стратегії-2015 уряд підходить до забезпечення безпеки критично важливих елементів інфраструктури – електромережі, водопровід, інформаційно-комунікаційні послуги, фінансові послуги та ін.

У серпні 2016 японський Національний центр готовності до надзвичайних ситуацій та стратегії в сфері кібербезпеки (NISC) опублікував документ під назвою «Загальні рамкові положення безпеки систем «інтернету речей» який є додатком до Національної стратегії кібербезпеки.

У той час, як в стратегії визнається важливість сталого економічного розвитку за допомогою ІКТ інновацій і забезпечення безпеки в цій галузі, вищевказаний документ постановляє, що Японія буде прагнути забезпечувати безпеку навіть в не критично важливих елементах інфраструктури, включаючи промислових виробників, враховуючи при цьому інтереси всіх зацікавлених

сторін в досягненні безпеки. З середини 90-х років XX століття в Японії створений цілий ряд організацій, відповідальних за реагування на інциденти і виникають кризові ситуації в області кібербезпеки.

3. Захист національного інформаційного простору у Великій Британії. У 2011 р. уряд Великобританії прийняв національну програму з інформаційної безпеки (Cyber Security Strategy) терміном дії до 2015 р. На цю програму витрачається 650 млн фунтів стерлінгів, тобто близько 1 млрд дол. за поточним курсом. Підсумки першого року дії програми, а також аналіз і рекомендації на майбутнє опубліковані у звіті Національного департаменту аудиту (National Audit Office) – незалежної організації, яка має дати об’єктивну оцінку роботи уряду у сфері інформаційної безпеки. Аудитори відзначають конкретні результати щодо захисту інформаційного простору. Наприклад, підрозділ по боротьбі з організованою злочинністю SOCA припинив діяльність 36 веб-сайтів, які продавали інформацію про платіжні карти, запобігши завданню матеріальної шкоди державі на півмільярда фунтів стерлінгів. Національний інформаційний центр Action Fraud громадяни повідомили про більш ніж 46000 випадків потенційного шахрайства, запобігши завданню матеріальної шкоди державі на чверть мільярда фунтів.

У Британії дуже чітко визначено цілі та проблеми в мережі Інтернет. Це трапилося після терористичних атак на Всесвітній торговий центр і Пентагон США 11 вересня 2001 р., коли фільтрація Інтернету стала головним завданням створеного у тому самому році Національного відділення по боротьбі зі злочинністю у сфері високих технологій. Скарги щодо використання контентів в Інтернеті розслідує Internet Watch Foundation. Після визнання контенту незаконним провайдеру повідомляють про це, а інформація видаляється. У свою чергу британська поліція стежить за чатами з метою недопущення дітей до порносайтів.

Загальна мета інформаційної стратегії Великобританії полягає в удосконаленні умов конкуренції на інформаційному ринку, зростанні ефективності інформаційних послуг і впровадження ІТ в державне управління. Характерною рисою інформаційної політики Великобританії є створення регіональних мереж і супермагістралей для оптимізації та підвищення ефективності міжрегіонального і міжнародного науково-технічного співробітництва.

4. Інформаційна безпека держави в національному законодавстві європейських країн (на прикладі Естонії, Литви, Бельгії та Туреччини).

Естонія була однією з перших країн, яка розробила національну стратегію кібербезпеки (2008 р.), а потім опублікувала оновлену стратегію у 2014 році. 10 травня 2018 року набув чинності Закон про кібербезпеку (Cybersecurity Bill). Він спрямований на зміцнення структур, що надають важливі послуги суспільству, та захист державних та муніципальних мереж та інформаційних систем.

Стратегія кібербезпеки Литви була прийнята в 2011 році: це Програма розвитку електронної інформаційної безпеки (кібербезпеки) на 2011-2019 роки. Перший закон про кібербезпеку був ухвалений у грудні 2014 року. У

вересні 2016 року Литва офіційно запустила свій Національний центр кібербезпеки. Цей центр було створено шляхом трансформації Служби зв'язку та інформаційних систем Міністерства оборони Литви. Основна мета Центру – консолідувати зусилля державних установ, поширити ідеї кіберінформованості та надати допомогу у попередженні кіберінцидентів урядових мереж. У липні 2015 року був створений Литовський Центр кібербезпеки з метою забезпечення централізації захисту кіберпростору на національному рівні. У квітні 2015 року уряд Литви прийняв рішення створити Раду з питань кібербезпеки, щоб забезпечити тіснішу співпрацю між державою, бізнесом та академічними організаціями.

Орган, що контролює інформаційний простір Бельгії – Аудіовізуальна вища рада (CSA) був створений 1987 році і був виключно консультативним, організований в незалежній адміністративну одиницю Указом від 24 липня 1997; Постанова від 27 лютого 2003 року надала цьому органу статус юридичної особи та контрольних повноважень в діяльності ЗМІ.

28 березня 2009 року набув чинності новий наказ про аудіовізуальні медіа-послуги (транспонування в нормативно-правову базу Бельгії Європейської директиви про аудіовізуальні медіа-послуги).

Туреччина, як і більшість розвинених держав, опинившись у трійці з найбільшою кількістю кібератак, сформувала у 2012 році стратегію кібербезпеки, яка на сьогодні є однією з найбільш повних та точних, адже вона включає в себе одразу всі види основних загроз у кіберпросторі та методи протидії ним. Вона була розроблена за такими основними напрямками: а) операції з кіберзахисту та кіберстримування; б) боротьба з кіберзлочинністю та кібертероризмом; в) розвідувальна діяльність і кібершпіонаж; г) кризове управління; ґ) управління мережею Інтернет і кібердипломатія. Стратегія кібербезпеки Туреччини направлена на захист громадянина, бізнесу та держави в цілому. Вона також визначає перелік критичної інфраструктури держави, виділяючи при цьому, що кібертерористичних атак зазнають переважно банківські та фінансові, енергетичні, транспортні, інформаційні та комунікаційні, електронні комунікації, таких секторів, як охорона здоров'я, оборона, а також основні державні послуги та їх інфраструктура.

Передбачаючи можливі загрози національній безпеці, в 2012 році було прийнято рішення про створення Командного центру кіберзахисту, який 30 серпня 2013 року був перетворений в Командування кіберзахисту Збройних Сил Туреччини. Центр діє цілодобово, і робить цілий ряд дій при виявленні загроз і атак на систему Збройних сил Туреччини. Центр кіберзахисту тісно взаємодіє з іншими військовими структурами країни. Діяльність центру ставитися до всіх видів військ Туреччини. Збройні Сили Туреччини є лідерами у сфері розробок турецьких кібертехнологій.

Ще одним значним кроком у реформуванні системи безпеки Туреччини було проведення на державному рівні навчань щодо забезпечення національної кібербезпеки, з 2011 по 2013 роки були двічі проведені навчання щодо забезпечення національної кібербезпеки.

2. ПЛАНИ ПРАКТИЧНИХ (СЕМІНАРСЬКИХ) ЗАНЯТЬ, ЗАВДАННЯ ДЛЯ САМОСТІЙНОЇ РОБОТИ ТА ПОТОЧНОГО КОНТРОЛЮ ЗНАНЬ, УМІНЬ ТА НАВИЧОК СТУДЕНТІВ

РОЗДІЛ 1. ЗАГАЛЬНІ ЗАСАДИ ЗАХИСТУ НАЦІОНАЛЬНОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ

Тема 1: Загальні засади інформаційного суспільства

Семінарське заняття 1: Загальні засади інформаційного суспільства

Навчальна мета заняття: формування у студентів базових знань щодо характеристики інформації як стратегічної сировини XXI століття, концепції інформаційного суспільства та типи і моделі його побудови, стан та стратегію розвитку інформаційного суспільства в Україні, а також практичних умінь та навичок визначати концепцію інформаційного суспільства та характеризувати стан розвитку інформаційного суспільства в Україні, працювати з міжнародними та національними нормативно-правовими актами та документами у сфері інформаційної безпеки.

Час проведення – 2 год.

Ключові поняття: інформація, інформаційне суспільство, інформаційна продукція, інформаційна послуга, принципи побудови інформаційного суспільства, персональні дані, інформація з обмеженим доступом, ІКТ, стратегія розвитку інформаційного суспільства, електронне урядування.

Навчальні питання:

1. Інформація – стратегічна сировина XXI століття.
2. Концепція інформаційного суспільства.
3. Стан розвитку інформаційного суспільства в Україні.

Література:

Основна: 5, 7, 13, 14, 16, 18, 21, 27, 28, 31.

Додаткова: 2, 3, 10, 11, 12.

Самостійна робота – 20 год.

Питання для контролю засвоєння знань:

- 1) Назвіть види інформації з обмеженим режимом.
- 2) Дайте визначення інформаційної продукції та інформаційної послуги.
- 3) Дайте загальну характеристику Окінавської хартії глобального інформаційного суспільства від 22.07.2000 року.
- 4) У чому полягає значення Всесвітнього саміту з питань інформаційного суспільства WSIS (Женева, 2003 – Туніс, 2005) для побудови

глобального інформаційного суспільства?

5) Назвіть головні принципи побудови інформаційного суспільства відповідно до Декларації принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті» від 12.12.2003 року.

6) У чому полягає зміст принципу побудови інформаційного суспільства «Підвищення довіри і безпеки при використанні ІКТ»?

7) Охарактеризуйте американо-англійську модель побудови інформаційного суспільства.

8) Охарактеризуйте європейську модель побудови інформаційного суспільства.

9) Визначте завдання, цілі та напрями розвитку інформаційного суспільства в Україні.

10) Визначте етапи та основні напрями реалізації Стратегії розвитку інформаційного суспільства в Україні.

Завдання:

1. Підготувати доповіді / презентації з наступних тем:

1) Право на інформацію відповідно до чинного законодавства України.

2) Принципи побудови інформаційного суспільства відповідно до Декларації принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті» від 12.12.2003 року.

3) Загальна характеристика Туніської програми для інформаційного суспільства від 18.12.2005 року.

4) Електронне урядування в Україні.

5) Західний тип побудови інформаційного суспільства.

6) Азійський тип побудови інформаційного суспільства.

2. Ознайомитися із Женевським планом дій від 12 грудня 2003 року <http://old.apitu.org.ua/ws/pd> та вміти визначати та характеризувати напрями побудови інформаційного суспільства.

3. Ознайомитися із Розпорядженням Кабінету міністрів України від 15 травня 2013 року № 386-р «Про схвалення Стратегії розвитку інформаційного суспільства в Україні» <https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80/ed20130515#n21> та вміти характеризувати сучасний стан розвитку інформаційного суспільства в Україні, визначати оціночні (контрольні) показники та індикатори інформаційного суспільства в Україні.

Тема 2. Інформаційна безпека в контексті національної безпеки держави

Семінарське заняття 2, 3: Інформаційна безпека в контексті національної безпеки держави

Навчальна мета заняття: формування у студентів базових знань щодо поняття та основних засад національної безпеки України, стратегії національної безпеки України, поняття, структури та основних характеристики національного інформаційного простору, особливостей регулювання та контролю інформаційного простору в мережі Інтернет,

поняття та змісту інформаційної безпеки держави, доктрини інформаційної безпеки держави та пріоритети державної політики і інформаційній сфері, а також практичних умінь та навичок розкривати поняття та зміст інформаційної безпеки в контексті національної безпеки держави, визначати пріоритети забезпечення інформаційної безпеки України, аналізувати та професійно давати оцінку сучасним міждержавним відносинам у світлі політики інформаційної безпеки держави, обґрунтовувати та висловлювати свою точку зору з проблем, пов'язаних з міжнародною інформаційною безпекою.

Час проведення – 4 год.

Ключові поняття: національна безпека України, національні інтереси України, національний інформаційний простір, інформаційна сфера, інформаційна інфраструктура, інформаційне поле, інформаційний потік, кіберпростір, кібербезпека, доктрина інформаційної безпеки України, державна політика в інформаційній сфері, інформаційна безпека, доктрина інформаційної безпеки України.

Навчальні питання:

1. Засади національної безпеки України.
2. Національний інформаційний простір.
3. Поняття та зміст інформаційної безпеки держави.
4. Доктрина інформаційної безпеки України.

Література:

Основна: 1, 6, 8, 9, 11, 15, 17, 19, 20, 23, 24, 30, 33, 35.

Додаткова: 1, 4, 5, 6, 7, 8, 10, 11, 12, 14, 16, 20.

Самостійна робота – 40 год.

Питання для контролю засвоєння знань:

- 1) Дайте визначення національної безпеки України.
- 2) Назвіть основні цілі Стратегії національної безпеки України.
- 3) Назвіть функції інформаційного простору.
- 4) Дайте характеристики співвідношення понять «інформаційний простір» та «кіберпростір».
- 5) Дайте визначення національного інформаційного простору.
- 6) Дайте визначення інформаційної безпеки.
- 7) Дайте характеристику співвідношення понять «інформаційна безпека» та «кібербезпека».
- 8) Визначте національні інтереси України в інформаційній сфері.
- 9) Визначте актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері.
- 10) Розкрийте пріоритети державної політики в інформаційній сфері.

Завдання:

1. Підготувати доповіді / презентації з наступних тем:

1) Основні напрями державної політики національної безпеки України відповідно до Закону України «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII.

2) «Інформаційний простір» та «кіберпростір».

3) Поняття та основні характеристики національного інформаційного простору.

4) Поняття та зміст інформаційної безпеки держави.

5) «Інформаційна безпека» та «кібербезпека».

6) Суб'єкти та механізми забезпечення інформаційної безпеки України.

2. Ознайомитися з Указом Президента України від 25 лютого 2017 року № 247/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» <https://zakon.rada.gov.ua/laws/show/47/2017> та вміти визначати національні інтереси України в інформаційній сфері та актуальні загрози їм, а також пріоритети державної політики в інформаційній сфері.

3. Ознайомитися зі статтею Солдатенко О. «Інформаційний простір у мережі Інтернет: правове регулювання та контроль» <http://pgp-journal.kiev.ua/archive/2018/5/27.pdf> та бути готовими до дискусії та обґрунтування своєї точки зору щодо інформації, наведеної у статті.

4. Ознайомитися зі статтею Шевченко О. М. «Поняття національного інформаційного простору та його характеристики» http://nbuv.gov.ua/UJRN/ukrinfsp_2018_1_12 та бути готовими до дискусії та обґрунтування своєї точки зору щодо інформації, наведеної у статті.

5. Ознайомитися зі статтею Ткачук Т. «Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз» <http://pgp-journal.kiev.ua/archive/2017/10/38.pdf> та бути готовими до дискусії та обґрунтування своєї точки зору щодо інформації, наведеної у статті.

Тема 3. Основні поняття інформаційного протиборства

Семінарське заняття 4: **Основні поняття інформаційного протиборства**

Навчальна мета заняття: формування у студентів базових знань щодо видів загроз інформаційній безпеці України, поняття та змісту інформаційного протиборства, основних завдань, форм та засобів ведення інформаційної війни, а також практичних умінь та навичок характеризувати види загроз інформаційній безпеці України та розкривати основні категорії інформаційного протиборства, орієнтуватися в способах протидії інформаційному вторгненню, вирішувати аналітичних завдань та практичні казуси відповідно до програми курсу на підставі аналізу нормативних документів, а також навчальної та монографічної літератури.

Час проведення – 2 год.

Ключові поняття: інформаційне протиборство, загрози інформаційній безпеці, інформаційна злочинність, кіберзлочинність, інформаційний тероризм, національна інформаційна інфраструктура, інформаційна експансія, інформаційна агресія, інформаційна війна, інформаційна зброя, інформаційна боротьба.

Навчальні питання:

1. Види загроз інформаційній безпеці України.
2. Поняття та зміст інформаційного протиборства.

Література:

Основна: 4, 10, 11, 12, 17, 20, 26, 29, 32.

Додаткова: 5, 7, 9, 13, 15, 16, 17, 18, 19.

Самостійна робота – 20 год.

Питання для контролю засвоєння знань:

- 1) Назвіть види загроз інформаційній безпеці України.
- 2) Дайте визначення інформаційного тероризму.
- 3) Дайте визначення інформаційного протиборства.
- 4) Назвіть ступені інформаційного протиборства.
- 5) Дайте визначення інформаційної війни.
- 6) Назвіть форми інформаційного протиборства.
- 7) Визначте завдання інформаційної боротьби.
- 8) Розкрийте форми ведення інформаційної боротьби.
- 9) Дайте визначення інформаційної зброї.
- 10) Назвіть класи інформаційної зброї.

Завдання:

1. Підготувати доповіді / презентації з наступних тем:

1) Загрози комунікативного характеру в сфері реалізації потреб людини і громадянина, суспільства та держави щодо продукування, споживання, розповсюдження та розвитку національного стратегічного контенту та інформації.

2) Загрози технологічного характеру в сфері функціонування та захищеності кібернетичних, телекомунікаційних та інших автоматизованих систем, що формують матеріальну (технічну, інструментальну) основу внутрішньодержавного інформаційного простору.

3) Ступені інформаційного протиборства.

4) Способи інформаційної боротьби.

5) Інформаційні війни в сучасному світі.

6) Інформаційна зброя та її особливості.

2. Ознайомитися зі статтею Косогова О. М., Сірик А. О. «Завдання

захисту національного інформаційного простору за досвідом ведення гібридної війни РФ на сході України» http://nbuv.gov.ua/UJRN/soivt_2017_1_7 та бути готовими до дискусії та обґрунтування своєї точки зору щодо інформації, наведеної у статті.

Тема 4. Досвід захисту національного інформаційного простору в інших країнах

Семінарське заняття 5: Досвід захисту національного інформаційного простору в інших країнах

Навчальна мета заняття: формування у студентів базових знань щодо досвіду захисту національного інформаційного простору в інших країнах, а також практичних умінь та навичок визначати позитивні та негативні тенденції досвіду захисту національного інформаційного простору в інших країнах та можливість його застосування в Україні, готувати рекомендації та пропозиції до проектів керівних документів у сфері забезпечення захисту національного інформаційного простору, спрямованих на адекватну відповідь загрозам національній безпеці України.

Час проведення – 2 год.

Ключові поняття: національний інформаційний простір, інформаційна безпека, кібербезпека, кіберінцидент, веб-сайт, національна стратегія кібербезпеки, кіберзахист, США, Японія, Велика Британія.

Навчальні питання:

1. Захист національного інформаційного простору в США.
2. Принципи та особливості системи інформаційної безпеки Японії.
3. Захист національного інформаційного простору у Великій Британії.
4. Інформаційна безпека держави в національному законодавстві європейських країн.

Література:

Основна: 2, 3, 22, 25, 26, 34.

Додаткова: 4, 5, 10, 15, 16, 18.

Самостійна робота – 20 год.

Питання для контролю засвоєння знань:

- 1) Розкрийте моделі захисту національного інформаційного простору в США.
- 2) Дайте характеристику Першій національній стратегії інформаційної безпеки Японії 2006 року.
- 3) Дайте характеристику Національній стратегії кібербезпеки Японії

2015 року.

- 4) Дайте характеристику Національної програми з інформаційної безпеки Великобританії 2011 року.
- 5) Розкрийте характерні риси інформаційної політики Великої Британії.
- 6) Дайте характеристику Національної стратегії кібербезпеки Естонії 2008 року.
- 7) Дайте характеристику Закону про кібербезпеку Естонії.
- 8) Дайте характеристику Стратегії кібербезпеки Литви 2011 року.
- 9) Дайте характеристику діяльності Аудіовізуальної вищої ради Бельгії у сфері захисту національного інформаційного простору.
- 10) Дайте характеристику Стратегії кібербезпеки Туреччини 2012 року.

Завдання:

1. Підготувати доповіді / презентації з наступних тем:

- 1) Захист національного інформаційного простору в Естонії.
- 2) Захист національного інформаційного простору в Литві.
- 3) Захист національного інформаційного простору в Бельгії.
- 4) Захист національного інформаційного простору в Туреччині.

2. Ознайомитися зі статтею Попової Т. «Захист національного інформаційного простору. Досвід США для України» <https://www.radiosvoboda.org/a/28830390.html> та бути готовими до дискусії та обґрунтування своєї точки зору щодо інформації, наведеної у статті.

3. Ознайомитися зі статтею Ткачук Т. «Ткачук Т. Інформаційна безпека держави в національному законодавстві європейських країн» http://vjhr.sk/archive/2018_1/part_2/24.pdf та бути готовими до дискусії та обґрунтування своєї точки зору щодо інформації, наведеної у статті.

3. ЗАВДАННЯ ДЛЯ ПІДСУМКОВОГО КОНТРОЛЮ ЗНАНЬ, УМІНЬ ТА НАВИЧОК СТУДЕНТІВ, ЗАЛІКОВИХ РОБІТ

Перелік питань до заліку

Заліковий білет містить 2 завдання, які полягають у розгорнутій відповіді на теоретичні питання.

Питання для підготовки:

1. Поняття та види інформації.
2. Право на інформацію.
3. Інформаційні відносини.
4. Окінавська хартія глобального інформаційного суспільства від 22.07.2000 року: мета, основні положення.
5. Основні принципи інформаційного суспільства.
6. Типи і моделі побудови інформаційного суспільства.

7. Завдання, цілі та напрями розвитку інформаційного суспільства в Україні.
8. Національна політика розвитку інформаційного суспільства в Україні.
9. Організаційно-правові основи розвитку інформаційного суспільства в Україні.
10. Стратегія розвитку інформаційного суспільства в Україні: мета, принципи, завдання.
11. Стратегія розвитку інформаційного суспільства в Україні: етапи та основні напрями реалізації.
12. Основні цілі Стратегії національної безпеки України.
13. Актуальні загрози національній безпеці України відповідно до Стратегії національної безпеки України.
14. Основні напрями державної політики національної безпеки України відповідно до Стратегії розвитку інформаційного суспільства в Україні.
15. Поняття та структура інформаційного простору.
16. Функції інформаційного простору.
17. Співвідношення понять «інформаційний простір» та «кіберпростір».
18. Поняття та основні характеристики національного інформаційного простору.
19. Мета формування і розвитку національного інформаційного простору України.
20. Інформаційний простір у мережі Інтернет: правове регулювання та контроль.
21. Поняття та зміст інформаційної безпеки держави.
22. Співвідношення понять «інформаційна безпека» та «кібернетична безпека (кібербезпека)».
23. Пріоритети забезпечення інформаційної безпеки відповідно до Закону України «Про Національну безпеку».
24. Суб'єкти та механізми забезпечення інформаційної безпеки України.
25. Мета та принципи Доктрини інформаційної безпеки України.
26. Національні інтереси України в інформаційній сфері відповідно до Доктрини інформаційної безпеки України.
27. Актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері відповідно до Доктрини інформаційної безпеки України.
28. Пріоритети державної політики в інформаційній сфері відповідно до Доктрини інформаційної безпеки України.
29. Механізм реалізації Доктрини інформаційної безпеки України.
30. Види загроз інформаційній безпеці України.
31. Інформаційна злочинність та інформаційний тероризм.
32. Поняття та форми інформаційного протиборства.
33. Ступені інформаційного протиборства (інформаційна експансія, інформаційна агресія, інформаційна війна).
34. Основні завдання, форми та засоби ведення інформаційної боротьби.
35. Інформаційна зброя та її особливості.

- 36.Завдання захисту національного інформаційного простору за досвідом ведення гібридної війни на сході України.
- 37.Захист національного інформаційного простору в США.
- 38.Принципи та особливості системи інформаційної безпеки Японії.
- 39.Захист національного інформаційного простору у Великій Британії.
- 40.Інформаційна безпека держави в національному законодавстві європейських країн.

Приклад залікового завдання

Харківський національний університет імені В. Н. Каразіна
Факультет міжнародних економічних відносин та туристичного бізнесу

Галузь знань: 29 «Міжнародні відносини»
Спеціальність: 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
Освітня програма: «Міжнародна інформаційна безпека»
Семестр: 3
Форма навчання: денна
Рівень вищої освіти: другий (магістерський)
Навчальна дисципліна: «Захист національного інформаційного простору»

ЗАЛІКОВЕ ЗАВДАННЯ № 1

1. Окінавська хартія глобального інформаційного суспільства від 22.07.2000 року: мета, основні положення (20 балів).
2. Актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері відповідно до Доктрини інформаційної безпеки України (20 балів).

Затверджено на засіданні кафедри міжнародних відносин,
міжнародної інформації та безпеки
протокол № 1 від “27” серпня 2019 р.

Завідувач кафедри _____ Л. В. Новікова

Екзаменатор _____ О. М. Доценко

РЕКОМЕНДОВАНА ЛІТЕРАТУРА:

Основна література

1. Бурячок В. Л. Основи формування державної системи кібернетичної безпеки: монографія / В. Л. Бурячок. К.: НАУ, 2013. 432 с.
2. Бусол О. Інформаційна безпека США: законодавче регулювання та перспективи співпраці для України. *Центр соціальних комунікацій НБУВ*. URL:
http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2988:info

[rmatsijna-bezpeka-ssha-zakonodavche-regulyuvannya-ta-perspektivi-spiivpratsi-dlya-ukrajini&catid=8&Itemid=350](#) (дата звернення: 20.08.2019).

3. Бусол О. Основні риси контролю за національним інформаційним простором Королівства Велика Британія. *Центр соціальних комунікацій НБУВ*. URL:

http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2962:osnovni-risi-kontrolyu-za-natsionalnim-informatsijnim-prostorom-korolivstva-velika-britaniya-2&catid=71&Itemid=382 (дата звернення: 20.08.2019).

4. Гуріна Ніна. Інформаційне протиборство – один з головних напрямків сучасних міжнародних відносин. *Всеукраїнська експертна мережа*. URL: http://www.experts.in.ua/baza/analytic/index.php?ELEMENT_ID=13657 (дата звернення: 20.08.2019).

5. Декларація принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті»: Міжнародний документ від 12 грудня 2003 року. URL: https://zakon.rada.gov.ua/laws/show/995_c57 (дата звернення: 20.08.2019).

6. Дубняк К. А. Інформаційний простір: структура та функціональні параметри. Держава та регіони. Серія: Соціальні комунікації. 2015. № 4 (24). С. 21–25.

7. Женевський план дій від 12 грудня 2003 року. Асоціація підприємств інформаційних технологій України. URL: <http://old.apitu.org.ua/wsis/pd> (дата звернення: 22.05.2019).

8. Косогов О. М., Сірик А. О. Завдання захисту національного інформаційного простору за досвідом ведення гібридної війни РФ на сході України. *Системи озброєння і військова техніка*. 2017. № 1 (49). С. 38–41.

9. Ліпкан В. А. Національна безпека України: навчальний посібник. Київ: КНТ, 2009. 576 с. URL: <http://politics.ellib.org.ua/pages-cat-154.html> (дата звернення: 20.08.2019).

10. Макаренко Є. Інформаційне протиборство у сучасних міжнародних відносинах. Міжнародні відносини. Серія «Політичні науки». 2017. № 17. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3316/2995 (дата звернення: 20.08.2019).

11. Малик Я. Інформаційна безпека України: стан та перспективи розвитку. Ефективність державного управління. 2015. Вип. 44. С. 13–20. URL: http://www.lvivacademy.com/vidavnitstvo_1/edu_44/fail/ch_1/3.pdf (дата звернення: 20.08.2019).

12. Мітін В. І. Інформаційний тероризм на сучасній міжнародній арені. *Международный научный журнал «Интернаука»*. 2011. № 2 (24). С. 65–68.

13. Окінавська хартія глобального інформаційного суспільства: Міжнародний документ від 22 липня 2000 року. URL: https://zakon.rada.gov.ua/laws/show/998_163 (дата звернення: 20.08.2019).

14. Політанський В. С. Світові моделі та фундаментальні принципи інформаційного суспільства. Науковий вісник Ужгородського національного університету. Серія Право. Випуск 43. Том 1. С. 34–39. URL:

http://www.visnyk-juris.uzhnu.uz.ua/file/No.43/part_1/10.pdf (дата звернення: 20.08.2019).

15. Попова Т. Захист національного інформаційного простору. Досвід США для України. *Радіо Свобода*. 02 листопада 2017. URL: <https://www.radiosvoboda.org/a/28830390.html> (дата звернення: 20.08.2019).

16. Про інформацію: Закон України від 02 жовтня 1992 № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#n18> (дата звернення: 20.08.2019).

17. Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19> (дата звернення: 20.08.2019).

18. Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки: Закон України від 09 січня 2007 року № 537-V. URL: <https://zakon.rada.gov.ua/laws/show/537-16> (дата звернення: 20.08.2019).

19. Про рішення Ради національної безпеки і оборони України від 06 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26 травня 2015 року № 287/2015. URL: <https://zakon.rada.gov.ua/laws/show/287/2015> (дата звернення: 20.08.2019).

20. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25 лютого 2017 року № 247/2017. URL: <https://zakon.rada.gov.ua/laws/show/47/2017> (дата звернення: 20.08.2019).

21. Про схвалення Стратегії розвитку інформаційного суспільства в Україні: Розпорядження Кабінету міністрів України від 15 травня 2013 року № 386-р. URL: <https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80/ed20130515#n21> (дата звернення: 20.08.2019).

22. Семенов А. Захист національного інформаційного простору Великої Британії. *Політична праксеологія: безпека, технології, комунікації*: Матеріали міжнародної конференції. За ред. В. Бебика. Київ: ВАПН, 2016. С. 91–93.

23. Солдатенко О. Інформаційний простір у мережі Інтернет: правове регулювання та контроль. *Адміністративне право і процес*. 2018. № 5. С. 134–140. URL: <http://pgp-journal.kiev.ua/archive/2018/5/27.pdf> (дата звернення: 20.08.2019).

24. Солодка О. М. Захист інформаційного простору України в умовах інформаційного суспільства. *Місце і роль бібліотек у формуванні національного інформаційного простору*: матеріали міжнародної наукової конференції, м. Київ, 21–23 жовтня 2014 року. URL: <http://conference.nbu.gov.ua/report/view/id/406> (дата звернення: 20.08.2019).

25. Ткачук Т. Інформаційна безпека держави в національному законодавстві європейських країн. *Visegrad Journal on Human Rights*. 2018. № 1 (Volume 2). С. 145–150. URL: http://vjhr.sk/archive/2018_1/part_2/24.pdf (дата звернення: 20.08.2019).

26. Ткачук Т. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. *Підприємництво, господарство і право*. 2017. № 10. С. 182–186. URL: <http://pgp-journal.kiev.ua/archive/2017/10/38.pdf> (дата звернення: 20.08.2019).

27. Туніська програма для інформаційного суспільства від 18 листопада 2005 року. *Інформаційне суспільство в Україні*. URL: https://informationsociety.wordpress.com/basics/BCIC_outcomes/tp/#C (дата звернення: 22.05.2019).
28. Туніське зобов'язання з питань інформаційного суспільства від 18 листопада 2005 року. *Асоціація підприємств інформаційних технологій України*. URL: <http://old.apitu.org.ua/BCIC/tz> (дата звернення: 22.05.2019).
29. Харченко І. М., Сапогов С. О., Шамраєва В. М., Новікова Л. В. Основні засоби інформаційного протиборства та інформаційної війни як явища сучасного міжнародного політичного процесу. Вісник Харківського національного університету імені В. Н. Казіна. Серія «Міжнародні відносини. Економіка. Країнознавство. Туризм». 2017. Випуск 6. С. 77–81. URL: <http://international-relations-tourism.karazin.ua/themes/irtb/resources/2c5d772b29c5a9e2139a9f6aa96834d0.pdf> (дата звернення: 20.08.2019).
30. Шевченко М. Поняття національного інформаційного простору та його характеристики. Теорія і практика сучасної журналістики. Український інформаційний простір. 2018. Випуск 1. С. 103–112.
31. Isazadeh A. Information Society: Concepts and Definitions. *WSEAS Transactions on Systems*. January 2004. URL: https://www.researchgate.net/publication/254476368_Information_Society_Concepts_and_Definitions (Last Accessed: 20.08.2019).
32. Molander R. C., Riddile A. S., Wilson P. A. Strategic Information Warfare: A New Face of War. *RAND Corporation*. URL: https://www.rand.org/pubs/monograph_reports/MR661/index2.html (Last Accessed: 20.08.2019).
33. Potts M. The State Information Security. *Network Security*. 2012. Volume 2012. Issue 7. P. 9–11. URL: <https://www.sciencedirect.com/science/article/pii/S1353485812700648> (Last Accessed: 20.08.2019).
34. Vozniuk E., Ukrainka L. Principles and Features of Japan's Information Security System. *Політичне життя*. 2017. № 4. С. 8–12.
35. What is the Difference between Cyber Security and Information Security? *Computer Science Degree Hub*. URL: <https://www.computersciencedegreehub.com/faq/what-is-the-difference-between-cyber-security-and-information-security/> (Last Accessed: 20.08.2019).

Допоміжна література

1. Антонюк В. В. Організаційно-правові засади формування та реалізації державної політики інформаційної безпеки України: 25.00.02 / Національна академія державного управління при Президентові України. Київ, 2017. 21 с.
2. Бондар Ю. В. Становлення та еволюція національного інформаційного простору України в процесі формування демократичної політичної культури українського суспільства: автореф. дис. ...канд. політ.

наук: 23.0.03/ Національний педагогічний університет імені М. П. Драгоманова. Київ, 2010. 20 с.

3. Буньківська О. В. Інформаційний простір: соціокультурна сутність, стан та проблеми функціонування в Україні: автореф. дис. ...канд. культурології: 26.00.01 / Київський національний університет культури і мистецтв. Київ, 2009. 23 с.

4. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / за ред. проф. В. Б. Толубка. Київ: ДУТ, 2015. 288 с.

5. Валюшко І. О. Інформаційна безпека України в контексті російсько-українського конфлікту: дис. ... канд. політ. наук: 23.00.04 / Дипломатична академія України при МЗС України; Чорноморський національний університет імені Петра Могили. Київ, 2018. 210 с.

6. Демченко м. А. Специфіка формування національного інформаційного простору в сучасній Україні в контексті зміни державної політики в інформаційній галузі. *Наукові праці МАУП*. 2016. Вип. 49 (2). С. 43–46.

7. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Lviv Polytechnic National University Institutional Repository*. 2016. Vol. 2. No. 1. P. 27–32. URL: http://ena.lp.edu.ua/bitstream/ntb/37314/1/7_31-36.pdf (дата звернення: 20.08.2019).

8. Корченко О. Г., Бурячок В. Л., С. О. Гнатюк. Кібернетична безпека держави: характерні ознаки та проблемні аспекти. *Безпека інформації*. 2013. Т. 19. № 1. С. 40–45.

9. Куцька О.М. Особливості інформаційно-психологічного впливу Російської Федерації напередодні та початковому етапі антитерористичної операції на сході України. *Інформаційна безпека людини, суспільства, держави*. 2017. № 1(21). С. 180–190.

10. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах Євроінтеграції: навчальний посібник. Серія: Національна і міжнародна безпека. Київ: КНТ, 2006. 280 с.

11. Мануйлов Є. М., Ю. Ю. Калиновський. Роль і місце інформаційної безпеки держави у розбудові сучасної української держави. Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». 2016. № 2 (29). С. 144–153.

12. Негодченко В. Основні напрями державної інформаційної політики в Україні. Підприємництво, господарство і право. 2016. № 4. С. 77–81. URL: <http://pgp-journal.kiev.ua/archive/2016/04/15.pdf> (дата звернення: 20.08.2019).

13. Об информационном портале по безопасности. *SecurityLab.ru be Positive Technologies*. URL: <https://www.securitylab.ru/about.php> (Last Accessed: 22.05.2019).

14. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 року № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 20.08.2019).

15. Семен Н. Ф. Російські Інтернет-ресурси як чинник інформаційної війни проти України (на прикладі сайтів «Правда.Ру» та «Российский диалог»): дис. ... канд. наук з соц. комун.: 27.00.01 / Міжнародний економіко-гуманітарний університет імені акад. С. Демянчука; Дніпровський національний університет імені Олеся Гончара. Рівне, 2018. 250 с.

16. Ткачук Т. Ю. Правове забезпечення інформаційної безпеки в умовах Євроінтеграції України: дис. ... докт. юрид. наук: 12.00.07 / ДВНЗ «Ужгородський національний університет. Ужгород, 2019. 487 с.

17. Хмелевський Р. М. Дослідження оцінки загроз інформаційній безпеці об'єктів інформаційної діяльності. *Сучасний захист інформації*. 2016. № 4. С. 65–70.

18. Широкова-Мурараш О. Г., Акчурін Ю. Р. Кіберзлочинність та кібертероризм як загроза міжнародній інформаційній безпеці: міжнародно-правовий аспект. *Інформація і право*. 2011. № 1. С. 76–81.

19. Collins A. Contemporary Security Studies. 3rd ed. United Kingdom: Oxford University Press, 2013. 478 p.

20. What is Information Security? URL: https://warwick.ac.uk/services/idc/informationsecurity/training/info_sec_quick_guide.pdf (Last Accessed: 20.08.2019).

Посилання на інформаційні ресурси в Інтернеті, відео-лекції, інше методичне забезпечення

1. Верховна Рада України - www.zakon1.rada.gov.ua.
2. Міністерство закордонних справ - <http://mfa.gov.ua/ua>
3. Міністерство юстиції - <https://minjust.gov.ua/ua>
4. Конституційний Суд України - <http://www.ccu.gov.ua/uk/index>
5. Організація Об'єднаних Націй - <http://www.un.org/>
6. Європейський суд з прав людини - <http://echr.coe.int/>
7. Європейський союз - <http://eeas.europa.eu/>
8. Організація з безпеки та співробітництва в Європі - <http://www.osce.org/>
9. Рада Європи - <http://www.coe.int/web/portal/home>
10. Управління Верховного комісара ООН з прав людини - <http://www.ohchr.org/>
11. Національна парламентська Бібліотека України - <http://www.nplu.org/>
12. Національна бібліотека України імені В. І. Вернадського - www.nbuv.gov.ua
13. Київська центральна міська публічна бібліотека ім. Лесі Українки - <http://lucl.lucl.kiev.ua>
14. Центральна наукова бібліотека Харківського національного університету ім. В. Н. Каразіна - <http://www.univer.kharkov.ua>
15. Харківська державна наукова бібліотека ім. В. Г. Короленка - <http://korolenko.kharkov.com>