СЕМКІВ ЮРІЙ МИРОСЛАВОВИЧ

РАДЧИК ГАЛИНА ІВАНІВНА

ПРАВОВІ ОСНОВИ РОЗВИТКУ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА ТА БЕЗПЕКА ЛЮДИНИ ПРИ ВИКОРИСТАННІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Навчальний посібник

ТЕРНОПІЛЬ 2007

ББК 32.81

С-30

УДК 621.363

Обговорено і рекомендовано до друку на засіданні циклової методичної комісії викладачів комп'ютерних предметів Технічного коледжу Тернопільського Держаного технічного університету ім. І. Пулюя

Обговорено і рекомендовано до друку на засіданні методичної комісії викладачів комп'ютерних технологій Тернопільського вищого професійного училища №4 ім М. Паращука. Протокол № 5 від 27.12.2006 р.

Семків Юрій Мирославович, Радчик Галина Іванівна.

С-30 ПРАВОВІ ОСНОВИ РОЗВИТКУ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА ТА БЕЗПЕКА ЛЮДИНИ ПРИ ВИКОРИСТАННІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ.
Навчальний посібник (конспект лекцій). - Тернопіль: Інфотехцентр, 2007. – 123 с.

В посібнику розглядаються правові основи інформаційного суспільства, захисту інформації, безпеки людини при використанні інформаційних технологій. Мета – доповнити існуючі навчальні видання.

Для викладачів, студентів вузів, коледжів, технікумів, учнів училищ, шкіл.

ЗМІСТ

ВСТУП

Такі терміни, як "інформаційні технології", "інформаційне суспільство" з'являються на сторінках наукових і науково-популярних видань. Це процес поступового усвідомлення суспільством значимості інформації як фундаментальної сутності і перетворення її в реальну силу - революцію і в свідомості людей і у виробництві. Перші освітні технології виникли тоді, коли людина навчилася записувати свої думки, що дало можливість транслювати знання одного покоління іншому- тоді і з'явився Вчитель. Сьогодні інформаційні технології і телекомунікації роблять будь - яке знання загальнодоступним. Однак легкість доступу до інформації ще не означає легкості одержання потрібної інформації. Відношення сигнал/шум заважає пошуку корисної інформації, здатне руйнувати психіку і змінювати соціальне поводження. Освітні технології повинні знешкоджувати негативні інформаційні потоки. В цих технологіях повинні бути включені критерії оцінки якості і безпеки інформації, техніка безпеки при роботі зі шкідливою інформацією, що стримують механізми породження небезпечної інформації наукою.

Розвиток і впровадження інформаційних технологій привів до виникнення електро – магнітного поля антропогенного походження. Всесвітня Організація Охорони Здоровя (ВООЗ) визначила дану проблему в число дуже важливих для людства з можливими поганими результатами для генофонду людини.

Відповідно до Женевської декларації 2003 року з питань інформатизації, дано таке визначення : "***Інформаційне суспільство – це таке суспільство, в якому кожний міг би створювати інформацію та знання, мати до них доступ, користуватися і обмінюватися ними для того, щоб дати окремим особам, громадянам, народам можливість повною мірою реалізувати свій потенціал…".***

1. Глобалізація інформації.

Вирішення глобальних проблем людства вимагає координованих зусиль всіх учасників міжнародного співтовариства, вимагає високого рівня взаємовідносин, що в сучасному розумінні називають обміном інформацією.

Міжнародна інформації послуговується двома термінами: **міжнародна інформація і міжнародна комунікація**.

Інформація – глобальна проблема людства.

Розглядаючи інформацію та комунікацію, треба підкреслити два таких моменти:

По-перше, інформація перетворилась на глобальну проблему, вона має світовий, міжнародний характер.

По-друге**,** значно зросла роль інформації у вирішенні інших глобальних міжнародних проблем, тобто вона стала складовою інших глобальних проблем, таких як боротьба зі стихійними лихами, проблема біжинців, проблема розподілу світових енергетичних ресурсів.

Інформація відтворює явища та закони зовнішнього світу і створює можливості передбачення і перетворення дійсності в інтересах міжнародного співтовариства. На відміну від інших ресурсів, які мають здатність вичерпуватись, інформаційні ресурси не тільки відтворюються, але й збільшуються протягом їх використання (тобто накопичення інформації у вигляді фундаментальних та спеціалізованих знань, у вигляді необхідної інформації зростає, і протягом останніх 10 років зросло майже в 30 разів). Інформаційний фактор здійснив у житті міжнародного співтовариства найбільш глибоку зміну за всю її історію. В реальному часі інформація об'єднала світ в єдину інформаційну систему і зараз обумовлює технічні, суспільні, політичні, соціальні та економічні системи. Існує вислів: **"Хто володіє інформацією, той володіє світом".**

Інформація є стратегічним ресурсом людства і у багатьох законах розвинених держав світу вона визначається як стратегічний ресурс держави, який охороняється системою національної безпеки.

За класифікацією дослідників глобальних проблем людства, віднесення до глобальних проблем відбувається за такими критеріями:

1) глобальні проблеми стосуються всього людства в цілому, кожної соціальної групи і кожної людини, тобто мають всецивілізаційний характер;

2) ці проблеми виступають як об'єктивний фактор, що певною мірою обумовлює розвиток усього світу;

3) глобальні проблеми вимагають для свого вирішення постійного міжнародного співробітництва усіх держав і максимальних об'єднаних зусиль усього людства. Невирішеність цих проблем створює загрозу для існування цивілізації та майбутнього планети.

За цими критеріями інформація набула статусу глобальної проблеми, оскільки сучасні засоби зв'язку глобалізували можливості передачі великих масивів інформації за неймовірно короткий час, мультимедійні системи здійснюють миттєву передачу інформації на будь-яку відстань, що впливає на суспільні процеси в світі.

Кожна держава розглядає глобальні проблеми через призму своїх національних інтересів. Наприклад, для країн Латинської Америки та Карибського регіону

проблема розвитку інфраструктури комунікацій є важливою і актуальною, в той же час в країнах Північної Америки, Західної та Північної Європи ця проблема є завершеною. Таким чином на міжнародних форумах, в міжнародних організаціях та інших міжнародних інституціях розробляються лише загальні принципи сприйняття глобальних проблем. Тобто держави узгоджують свої інтереси: одні надають можливості для розвитку цієї галузі, а інші просто розвивають цю галузь у себе. Таким чином забезпечується рівномірний розвиток комунікацій у всьому суспільстві, у всіх країнах.

4) Ще один аспект інформації як глобальної проблеми полягає у тому, що глобальні проблеми міжнародного співтовариства мають завжди як складову і проблему комунікацій. До таких глобальних проблем відносять на сьогодні врегулювання міжнародних конфліктів, підтримання миру і безпеки у світі, проблему голоду, проблема захисту навколишнього середовища, проблема біжинців, проблема стихійних лих та епідемій. І звичайно інформація є складовою таких глобальних проблем, як розподіл сировинних, продовольчих, енергетичних ресурсів та розподіл інформаційних ресурсів, проблеми демографії. Жодна з цих проблем не може бути вирішена без збору та аналізу інформації по цій проблемі, а це є прерогативою процесу комунікацій.

5) Інформація за останній час сприяла тому, що нагальні проблеми стають у центрі уваги міжнародного співтовариства у зв'язку з миттєвим обігом інформації. Таким чином з'являється можливість швидше мобілізувати ресурси усього міжнародного співтовариства і допомогти постраждалим.

6) Інформаційна криза виявляється у таких моментах:

а) існує протиріччя між обмеженими можливостями людини по переробці інформації і світовими інформаційними потоками;

б) виробництво значної кількості надлишкової інформації, що обмежує доступ до корисної інформації;

в) порушення цілісності інформаційної системи внаслідок приватних, відомчих і регіональних інтересів.

Інформаційна криза супроводжується інформаційним голодом, що став характерним для усієї світової спільноти. Інформаційна криза може розглядатися тільки у контексті міжнародних, соціальних і економічних відносин.

Серед нормативних документів, за якими здійснюються міжнародні інформаційні відносини можна визначити документи, які забороняють розповсюдження інформації (вони є обов'язковими до виконання усіма країнами-членами ООН і вони входять до національного законодавства кожної держави). До таких документів належать:

- Резолюція Генеральної Асамблеї ООН № 110 частина 2 від 3.11.1947 – засудження пропаганди агресивних війн;

- Міжнародний пакт про громадянські та політичні права 1966 року, ст.20 – заборона законом пропаганди агресії та насильства;

- Міжнародна конвенція про ліквідацію всіх форм расової дискримінації 1972 року – заборона пропаганди расової вищості;

- Загальна декларація прав людини (1948 р.),

- Конвенція про авторське право (Україна приєдналася до неї у 1995 році).

Але міжнародні документи ООН можуть носити як зобов'язуючий, так і рекомендаційний характер. Якщо порушується зобов'язуючий документ, то на державу накладаються штрафні санкції, в основному політичні і економічні. У випадку порушення рекомендаційного документу, держава може відчути на собі моральний або політичний тиск інших держав. Тобто рекомендаційні документи створюються для того, щоб держава створила певні положення в національному законодавстві.

2 Теорія інформаційної цивілізації. Загальні положення.

Глобальна роль інформації привела до появи в суспільстві концепції інформаційної цивілізації. У зв'язку з цим третє тисячоліття називають тисячоліттям становлення інформаційної цивілізації і визначають характеристики інформаційного суспільства.

Автори, що розглядали інформаційне суспільство: Збігнев Бжезинський, Махлюен, Понятовський, Тофлер, Масуда, Белл.

Існують різні визначення інформаційного суспільства (ІС). Вони розглядали ІС як новий рівень в історії людства і основні цілі нової концепції визначали дуже чітко:

1) **створення єдиної комп'ютеризованої нації;**
2) **глобалізм інформаційного простору;**
3) **розвиток комунікаційних мереж;**
4) **вільний потік інформації незважаючи на кордони держав**.

Існує багато концепцій, автори яких намагаються пояснити, чому в історії відбувається все так, а не інакше. Основними з них вважаються ***цивілізаційна*** (зв'язана насамперед з ім'ям А.Тойнби) і ***формаційна,*** зв'язана з ім'ям Карла Маркса. Перша розглядає як першопричину історії феномен цивілізації, як цілісності економічних, культурних і природних факторів, друга суспільно-економічні структури (спосіб виробництва). Тоффлер, Белл і деякі інші американські соціологи - автори постіндустріальної теорії - виходять із третьої концепції, заснованої на представленні про ***технології,*** як про основний компонент суспільних відносин, як про головний системний фактор.

На думку Тоффлера, технологічний розвиток людства проходить хвилеподібно і можна виділити три основні хвилі технологічних змін.

Перша хвиля - почалась багато тисяч років тому і давно завершилася- це аграрна революція, що призвела до переходу людства на нові суспільні відносини, сформувало перші цивілізації.

Друга хвиля - почалась приблизно 300 років тому – це індустріальна революція, заснована на фабричному виробництві, що ознаменувалося становленням відомих нам форм суспільного ладу. Саме з нею зв'язана поява тоталітарних режимів. Вони були породжені індустріальним суспільством, з його бюрократизмом, гігантоманією, стандартизацією. Гігантські фабрики сприяли росту бюрократизму в суспільстві, вимагали посилення регулюючої ролі держави, що повинна була тепер все більш ретельно стежити за слухняністю багатомільйонних мас робітників, зайнятих вимотуючим монотонною працею. Особливо підсилилася

ця тенденція з переходом до фордизму - конвеєрному виробництву, уперше введеному на заводах Форда. Ця форма організації фабричної праці характеризується високим рівнем спеціалізації, розбиттям процесу праці на безліч дрібних операцій, твердою субординацією, абсолютним підпорядкуванням нижчестоящих виробничих інстанцій вищестоящим, системою заохочувально-каральних мір з метою оптимізації процесу праці. Така система організації праці могла привести й у деяких випадках, (СРСР, нацистська Німеччина), до появи відповідних їй форм диктаторської державної влади, заснованої на тотальній регламентації всього громадського життя.

Третя постіндустріальна революція розвертається на наших очах. Саме з нею пов'язані кризові явища сучасної епохи тому, що радикальні суспільні перетворення завжди хворобливі і не всі можуть їх осмислити і до них пристосуватися. Але високі технології несуть людству волю. Саме з ними зв'язана і катастрофа тоталітарних режимів. Занадто могутні і розгалужені бюрократичні піраміди стали неефективні в умовах поширення постіндустріальних і інформаційних технологій. Бюрократія виявилася в скрутному положенні в умовах безупинної науково-технічної революції, і змушена була (по всьому світі) терміново перебудовувати і реформувати свої ряди. Саме такі задачі ставив М.С.Горбачов на початковому етапі його правління в ході так званого прискорення. Однак, ті бюрократичні чи держави корпорації, що не зуміли оперативно здійснити зміни, програли конкурентам і розвалилися під власною вагою. Радянська державно-індустріальна централізована модель позволяла успішно здійснювати деякі сучасні виробничі проекти, (насамперед у військовій області), за рахунок гігантської концентрації зусиль всієї економіки країни. Але при цьому бюрократична машина держави була вкрай неповоротка. Змушена контролювати все і вся у величезній країні, вона не могла забезпечити гнучке динамічне реагування на зміни, що відбуваються у світі високих технологій. В умовах глобальної технологічної революції, радянське відставання стало фатальним, в тому числі й у такій важливій для будь-якої великої держави сфері, як військова техніка. Тому СРСР програв технологічне і військове змагання Заходу.

Що таке постіндустріальні технології і чи можна з їхньою допомогою здійснити звільнення особистості?

Мова йде насамперед про такі речі як аерокосмічна промисловість, виробництво роботів, виробництво могутніх компактних комп'ютерів з їхнім наступним використанням у промисловості і повсякденному житті, мова йде про нові джерела енергії, про генну інженерію, про нові області медицини, про нові способи передачі і збереження інформації і т.д. Відмітна риса нових технологій - це, на думку Тоффлера і Белла штучний інтелект, мініатюрність, компактність, здатність зберігати ресурси. У цих умовах виникає необхідність якісно нового підходу до праці, що буде тепер ґрунтуватися не на вимотуючій рутині повторюваних порівняно простих механічних операцій, а на гнучкому творчому відношенні до виробничого процесу і на суверенному розпорядженні робочим часом. Тепер немає потреби в конвеєрах, однак різко зросла потреба у творчо мислячих фахівцях, здатних працювати зі складним обладнанням і самостійно приймати рішення. На

зміну класичній фабриці, що робить на гігантських конвеєрах стандартизовану продукцію, прийдуть невеликі екологічно чисті виробництва, де будуть працювати, головним чином, висококваліфіковані фахівці, що розвили в собі здатність до творчої праці. Відповідно, замість старих величезних енергетичних установок, що руйнують природу, прийдуть принципово нові компактні джерела енергії, засновані на використанні вітру, припливів, морських течій, сонця і т.д. Але це тільки початок. А потім... Нація, держава, велика корпорація, промислова монополія чи олігополія, єдина служба теленовин, релігійна конгрегація, що включає в себе сотні мільйонів людей, усі ці структури - породження минулого, їхнє існування є результат дії ***індустріальних технологій***. Їхні величезні розміри, централізм, бюрократичний пристрій, тоталітарні методи керування, були адекватні задачам індустріального виробництва, з його гігантоманією, необхідністю жостского ієрархічно регулювання, стандартизації, спеціалізації і т.д. Все це поступово іде в минуле. На підході нові суспільні відносини, засновані на териториальних автономіях, невеликих виробничих об'єднаннях, порівняно малих по розмірах релігійних, культурних, сімейних і інших асоціаціях. Це будуть об'єднання людей, близьких один до одног по поглядах, інтересам, професії і т.п. Сучасні технології допоможуть їм самостійно налагодити своє життя, зв'язуючи з іншими групами лише в міру необхідності. Об'єднання будуть виникати і розпадатися, зв'язуватися між собою в мережні структури, сучасні засоби виробництва і комунікації дозволять розвивати такі мережі в планетарному масштабі. Тому така структура стане глобальною.

Ринок і комерційне виробництво поступове поступляться місцем індивідуалізованому виробництву по замовленнях, здійснюваним безпосередньо зацікавленими індивідами, або групами індивідів тому, що високі технології - дають можливість без особливого росту витрат змінювати параметри продукції. А комп'ютерні мережі і нові засоби комунікації дозволять миттєво встановлювати зв'язок між виробником і споживачем, тобто виявляти потреби населення методами прямої демократії. В такий спосіб буде ліквідований характерний для індустріалізму розрив між інтересами виробництва і споживання. На зміну настирливій рекламі прийде стирання границь між виробництвом і споживанням - тепер сам замовник зможе визначати характеристики і навіть безпосередньо брати участь у моделюванні потрібної йому продукції.

На зміну величезним фінансовим, промисловим і торговим корпораціям, прийдуть корпорації нового типу, засновані на децентралізованому мережному виробництві, на безлічі невеликих регіональних центрів концентрації фінансового капіталу (банків), індивідуалізованій торгівлі і т.д. Навіть політична представницька демократія поступово розчиниться в новій демократії, заснованої на виявленні побажань і політичних інтересів конкретних індивідів і їхніх асоціацій за допомогою комп'ютерних і інших комунікаційних мереж. Таким чином, багато проблем, зв'язані з придушенням особистості величезними бюрократичними індустріальними структурами підуть у минуле, тому що підуть у минуле самі ці структури, а ті виробничі й інші суспільні структури, що неминуче прийдуть їм на зміну, будуть набагато більш демократичні.

Правий чи не правий Елвин Тофлер і його послідовники? Однозначно відповісти на це питання, очевидно, не можна. Але варто відзначити, що Тофлер, схоже, не бере до уваги два фундаментальні протиріччя нинішньої цивілізації. ***Перше - розрив між ростом технологічних можливостей людства і його низьким рівнем культурного й етичного розвитку***. Що може бути гірше варвара, озброєного комп'ютерами і генною інженерією? Тим часом, деякі старі суспільні проблеми і протиріччя не зникають зовсім з появою нових технологій, а лише змінюють вигляд.

Друге протиріччя - між багатомірною натурою людини, між принциповою спонтанністю, глибиною, невичерпністю його і, з іншого боку, сутністю техніки, що, в зростаючій степені втягує нас в орбіту свого існування, змушує нас сприймати цільний світ, де все розглядається з фатальною неминучістю, як наявний ресурс, що підлягає плануванню. Очевидно, техніка необхідна людині, лихо починається тоді, коли люди перестають розуміти, що таке сутність техніки і яке місце техніки, перестають розуміти, що це одна з багатьох речей, а зовсім не деяка універсальність!

З моменту виходу у світ книг Тофлера пройшло біля двадцяти років і тепер можна підвести деякі підсумки. Вірно, що впровадження виробничої автоматизації в 60- х 70 -х, комп'ютерна та інтернетівська революція 90- х, змінили вигляд світу. Вірно і те, що потенційно деякі нові технології мають в собі ті можливості, про які писав Тоффлер і інші теоретики постіндустріалізму. Наприклад, у світі в сотні разів зросла кількість людей, зайнятих самостійною виробничою діяльністю - суверенних індивідуальних працівників, що тепер мають можливість розпоряджатися результатами своєї праці. Збільшилося значення невеликих, автономних виробничих підрозділів, де були введені елементи трудового самоврядування. Широке розповсюдження інтернету дозволило людям з різних країн і регіонів спілкуватися, прямо і вільно обмінюватися думками.

Але не менш істотно й інше. З'ясувалося, що на зміну національних держав з їхньою бюрократією приходять континентальні супердержави із супербюрократією (наприклад, знаменита "єврократія" - централізована бюрократія об'єднаної Європи уже встигла прославити себе величезною кількістю регламентуючих заборон і "цінних вказівок"). Навряд чи могло бути інакше, адже глобалізорована планетарна ринкова економіка вимагає наявності певних форм централізованого регулювання.

З'ясувалося і те, що широке впровадження капіталомістких виробничих новацій під силу насамперед великим корпораціям, саме вони мають у своєму розпорядженні необхідними для цього ресурсами капіталу, реальністю стали невеликі розміри окремих виробництв, побудованих по мережному принципі (тобто на основі автономних і напівавтономних від центра підрозділів), але, в той же час, в 80-і та 90-і роки мала місце небачена в історії хвиля гігантських корпоративних злиттів. На сьогоднішній день 2\3 світові виробництва зосереджене в руках приблизно 500 Транснаціональних корпорацій (ТНК), що, звичайно, сприяє концентрації в їхніх руках економічної і політичної влади. При цьому тисячі автономних груп працівників і мільйони "нових самостійних індивідуалів" змушені тепер конкурувати між собою за одержання замовлень від центрів концентрації капіталу, внаслідок чого, в цьому новому світі цінність людини продовжує

визначатися, відповідно до домінуючих установок ринку, в старих категоріях вартості, корисності і "економічної ефективності".
Виявилося, що комп'ютеризований маркетинг веде не тільки до росту впливу споживача, але і до усе більш витонченої системи маніпулювання його смаками, коли замість декількох стандартизованих варіантів того самого товару, фірми-виробники обрушують на нього сотні всіляких модифікацій того ж самого товару. В хід йде все, починаючи від реальних потреб в певному предметі і завершуючи спробами впливати на емоції, амбіції, комплекси, затаєні страхи споживача. Таким чином, комп'ютерна епоха не привела до заміни ринку якимись іншими формами обміну, (як припускав Тофлер), і не зумла ліквідувати характерне для сучасної економіки панування виробництва над споживанням. Підсилюються тенденції, опис яких дається в кожнім підручниках маркетингу, і які можна звести до відомої формули : ***корпорації не задовольняють попит, а створюють його***.

Розвиток телекомунікацій привів не стільки до формування "невеликих локальних телемереж", як пророкував Тоффлер, скільки до формування незліченних віртуальних світів глобалізованих засобів масової інформації (підконтрольних все тим же ТНК), що безупинно обрушують на людей потоки комерційної і політичної реклами.

Виявилося, що комп'ютери можна використовувати не тільки для ефективного виявлення суспільних потреб, але і для ще більш ефективного контролю держави і великого бізнесу над цим самим суспільством, із усіма його потребами. Людина в сучасному світі поступово стає все більш прозорою: наявність комп'ютерних сховищ інформації дозволяє в миттєво одержати величезні масиви інформації, починаючи з картки психотерапевта і завершуючи особистим переписуванням. Правда, є закони, що регулють застосування комп'ютерного контролю. Але закони, часом, значать дуже мало.

Постіндустріалізм не зміг вирішити екологічні проблеми. Триваючий сьогодні ріст масового споживання примушує використовувати колишні гігантські енергетичні установки, тому що нові джерела енергії не в змозі забезпечити сучасну промисловість. Тому зберігається і загроза теплового, радіаційного і т.п. забруднення.

Постіндустріальна дійсність містить у собі не тільки можливості, про які так докладно і з таким ентузіазмом пише Тофлер, але і тенденції, на які вказує російський письменник Зинов'єв, у своїй антиутопії "Глобальний Человейник". Нові технології неймовірно розширили сферу можливостей людства... і ***залишили людини віч-на-віч з загрозою нового рабства, заснованого на комп'ютерному контролі, манипулятивном маркетингу і віртуальній реальності ЗМІ.***

Розглянемо приклади використання суперкомп'ютерів для моделювання ***людського мозку, держави, Всесвіту.***

В однаковій мірі незвична й обрана методика - комп'ютерна симуляція. Вченим приходиться виходити з ньютонівської максими - "гіпотез не вигадую", щоб обмеживши мінімумом припущень, надати систему самій собі.
Такий підхід давно і упевнено використовується для опису "окремих випадків", коли поводження простих об'єктів погано вкладається в рамки відомих формул. Але до систем, складність яких перевершує всі очікування, його застосовують вперше.

Мозок. Федеральна політехнічна школа Лозанни (EFPL) придбала в IBM суперкомп'ютер Blue Gene, восьмий у світі по швидкодії. Машина, зарекомедовавши себе детальним розрахунком структури білків, протягом двох років зображувала фрагмент кори головного мозку. Точніше - нейронну мережу в неокортексі: цю область вважають головною серед відповідальних за " людське" в свідомості: мову, пам'ять, творче мислення. Кожний з 4096 процесорів стане "нервовою клітиною", здатної обмінюватися сигналами із сусідами. Всередині неокортекса вони згруповані в стовпчики, і саме такий стовпчик буде відтворювати весь суперкомп'ютер.
Ніяких додаткових закономірностей, крім біо- і електрохімічних реакцій, у програму не закладали. . Нейрофізіологи вирішили відштовхуватися від "ясних і очевидних" принципів, зокрема для перевірки більш складних гіпотез, але навряд чи обмежаться цим. Глава Інституту мозку EFPL заявив, що на наступних стадіях планується відтворити весь мозок. Коли це відбудеться, невідомо, але "вступна частина" - моделювання неокортекса - повинне зайняти не більш двох років.

Творці суперкомп'ютера, представники EFPL свідомо не формулюють питання винесенного Тьюрингом у заголовок знаменитої статті 1950 року –
" Чи може машина мислити". В їхньому розпорядженні - 22,8 терафлопа і фізичні закони. Теоретик штучного інтелекту намагався зрозуміти, як за допомогою математичних алгоритмів імітувати операції, що здійснює людське мислення. Тепер саме слово "імітація" виглядає навмисним спрощенням - механізм збираються скопіювати, а зовсім не "перевинайти".
Змусити комп'ютер "думати" - одна із самих популярних проблем кібернетики. Тьюринг не застав результатів, що перетворила його висловлення з "заклинань технократа" у програму дій: функціональні мови програмування з'явилися незабаром після його смерті, нейронні мережі і "нечітка логіка" - пізніше. Всі ці засоби, знайшовши собі несподіване застосування, почали жити самостійним життям.

Модель держави. Лабораторія в Лос-Аламосе - головний оборонний дослідницький центр США, всесвітньо відомий завдяки Манхеттенському проекту. Могутній суперкомп'ютер уже давно містить всередині себе "віртуальну Америку" - з людьми та інфраструктурою, це- черговий захід для боротьби з тероризмом. Зміст

моделі - передбачити наслідки можливих терактів, не втягуючи в "навчання" реальних людей і техніку, ("навчальна тривога" не здатна нікого змусити поводитись так само, як під час дійсної катастрофи).
Автори експерименту, посилаючись на таємність, обмежилися окремими репліками про те, як влаштоване “віртуальна держава”. Відомо, що в ньому можна простежити за переміщеннями кожного окремого громадянина, змусивши його реагувати на "зовнішні подразники" - сигнал тривоги, поширення новин, безпосередню небезпеку. Поводження терористів продумане вдрібних деталях - їхні дії визначає не програма, а самі розроблювачі. Вже випробувані такі сценарії, як поширення хвороботворних бактерій і припинення роботи електростанцій.
Цікаво, що в Лос-Аламосі були здійснені перші роботи з комп'ютерного моделювання взагалі - саме в контексті Манхеттенського проекту. Тоді потрібно було чисельно розрахувати механізм детонації ядерного заряду, а в якості "побічного продукту" з'явилися математична теорія ігор і представлення про архітектуру сучасних комп'ютерів (і те і інше - завдяки Джонові фон Нейману).
Більш пізні і більш близькі аналоги "віртуальної Америки" варто шукати в математичній біології: експерименти по чисельному відтворенню колонії бактерій широко відомі, а перша програма, що демонструє їхня можливість - гра "Життя" - є найпростішим і самим наочним прикладом комп'ютерної симуляції. Причому, якщо останньої досить для виконання практично будь-якого мікропроцесора, то потужності суперкомп'ютера вистачає, щоб куди більш складні віртуальні істоти "поводилися" правдоподібно.

...обчислює кількість зірок; всіх їх називає їх іменами
Книга Псалмів Давидових, 146:4

Модель Всесвіту. Експеримент за назвою Millenium Run, здійснений на суперкомп'ютері в Інституті Макса Планка, самий масштабніший з усіх. У віртуальний куб зі стороною 2 мільярди світлового років вклали 10 мільярдів частинок і простежили їхню історію від моменту Великого Вибуху до сучасності. Кожна частинка - з більшої, ніж у середнього зоряного скупчення, "віртуальною масою" - позначала деякий обсяг протозоряної речовини - "темної матерії". Частки розмістили в далекому минулому - і протягом місяця чекали від 4-терафлопового комп'ютера рішення, що відповідає структурі квазі-всесвіту в задані моменти часу. За масштаби довелося розплачуватися істотними спрощеннями. Експериментатори розглядали тільки гравітаційні взаємодії між близькими точками, і скористалися співвідношенням між "звичайною" і "темною" речовиною, на яке вказують сучасні космологічні теорії.

Відповідно до задуму, результат повинний був підтвердити вже існуючі погляди. Це і відбулося, коли на початку червня журнал Nature опублікував підсумкову статтю учасників експерименту. Дивна "робоча гіпотеза" теоретиків стала визнаним фактом. Космос дійсно на 70 відсотків складається з "темної енергії", що змушує

його розширюватися, на чверть - з "темної речовини", і тільки на п'ять відсотків - зі звичних нам атомів.

Комп'ютерна модель також перевела з розряду екзотики в категорію фактів надважкі чорні діри, що служать "зародками" галактик або знаходяться в центрі яскравих квазарів на периферії видимого простору. Ще астрофізики з'ясували, що "випадкові відхилення" на ранніх стадіях росту Всесвіту не згладжуються при її наступному розвитку, як це відбувається в звичайних молекулярних системах.
Організатори запевняють, що опублікована тільки мала частина висновків - масив даних занадто великий, і в ньому можна буде шукати закономірності і після появи нових гіпотез. Виходить, що у вчених з'явився "Всесвіт у кишені", що дозволяє звернутися до себе в будь-який момент, коли знадобиться довідатися що-небудь про прототип. В незакінченому - стані є два інших експерименти по "моделюванню всього". Але і ту частину, що зроблена, не всі оцінюють однаково. Одночасно з тими, хто справедливо думає, що це - прорив, у суперкомп'ютерних симуляцій є багато противників. Найчастіше вказують на очевидний недолік - моделі грубі, а дійсність набагато складніше. Але більш серйозним здається інший контраргумент - наявність сильної техніки позбавляє чисельні експерименти колишньої елегантності. А можлива перевага "буквально відтвореного" людського мозку над математично вибудованим штучним інтелектом чомусь нагадує перемогу комп'ютера над живим шахістом - безумовну, але марну.

З точки зору розвитку суспільства, в даній характеристиці існують положення, які зараз здаються неможливими **(наприклад створення єдиної комп'ютеризованої нації вважається утопічним).** Справа в тому, що створення інформаційної цивілізації залежить не лише від дослідників, а і від самого суспільства. Зараз кожен із індивідуумів визначає для себе рівень насичення інформацією: чи побутовий, чи спеціалізований. І звичайно не можна заставити всіх користуватися інформацією на спеціалізованому рівні.

Однак вже зараз певні положення цієї концепції починають реалізовуватись. Так японський дослідник Масуда розробив "План інформаційного суспільства – національна мета Японії до 2000 року". На цей план було асигновано десятки млрд. доларів, і Японія реалізувала його майже повністю (крім створення регіональної системи життєдіяльності людини). Компонентами цього плану є:
1) створення баз даних для управління від найвищого до місцевого рівня;
2) комп'ютеризація усіх соціальних сфер суспільства;
3) створення системи інформаційного контролю за виконанням рішень на всіх рівнях;
4) створення комп'ютерної системи охорони навколишнього середовища і регіональної системи життєдіяльності людини.

3.Основні поняття міжнародної інформації.

До основних понять МІ відносять такі складові, як міжнародна інформація, міжнародний інформаційний простір, інформаційні ресурси, інформаційний потенціал, національний інформаційний продукт і джерела інформації.

МІ є складовою глобальної комунікації, мета якої – з'ясування закономірностей взаємодії суспільства та інформації і формування інформаційного суспільства. МІ орієнтована на інформаційне забезпечення зовнішньої та внутрішньої політики, економічного курсу країн, національної безпеки, на розвиток міжнародних зв'язків і входження держави у міжнародні організації та інституції. В кожній країні є концепція державної інформаційної політики, в якій визначаються різні аспекти інформаційного забезпечення міжнародних відносин. Так, наприклад федеральна інформаційна політика США спрямована на забезпечення доступу до інформації для кожного індивіда, детальних зв'язків у своєму суспільстві і міжнародному співтоваристві. Інформаційна політика України спрямована на захист власного інформаційного простору, збереження інформаційного суверенітету і забезпечення інформаційної безпеки держави.

Функції МІ полягають в узагальненій та професійній оцінці інформації, прогнозуванні міжнародно-правових та економічних наслідків прийнятих рішень, у створенні обгрунтованих пропозицій та рекомендацій щодо їх реалізації.

Інформація належить до глобальних проблем світу, тому одним із понять МІ є поняття *міжнародний інформаційний простір* (МІП). Міжнародна інформація функціонує в МІП, який характеризується такими показниками:

- територія розповсюдження інформації за допомогою компонентів міжнародних та національних систем зв'язку;
- інфраструктура, тобто технологічні засоби і можливості зберігання, обробки і розповсюдження інформації по вертикалі і горизонталі;
- наявність міждержавної і національної комунікаційної політики, як комплексу принципів і норм, що регулюють функціонування та використання міжнародної інформації світовим співтовариством;
- наявність міжнародних і регіональних угод у галузі комунікацій, що базуються на розумінні міжнародної ролі інформаційних процесів (ці міжнародні угоди складають окрему галузь міжнародного права – інформаційного права, яка зараз проходить фазу становлення і кодифікації норм, становлення інститутів, що контролюють виконання цих норм. З питань міжнародного інформаційного права можна подивитися книгу Колосова "Міжнародне право", особлива частина);
- можливості доступу до інформації для громадськості та участь міжнародного співтовариства у загальній системі зв'язку.

Кожна країна своїм законодавством визначає кордони своєї території і звичайно, кордони своєї інформаційної території. Звичайно термін "інформаційна територія держави" – це дещо умовний термін, тому що держава не в силах припинити прийом інформації, що передається через численні канали штучних супутників Землі її громадянами. Вона може лише контролювати транслювання цих каналів на своїй території. Але за прийнятою конвенцією "Про використання сигналів, що передаються через штучні супутники Землі", країна має заплатити за право транслювання таких каналів, при порушенні цієї умови на країну накладаються штрафні санкції до кількох млрд. доларів.

Декотрі країни в основі своєї інформаційної політики мають певні ідеологічні засади, які забороняють населенню використовувати певну інформацію. Зовсім недавно, коли в Ірані до влади прийшли релігійні партії, вони заборонили прийом світської інформації на телеприймачі своєї країни, таким

чином обмеживши участь країни у світових інформаційних потоках. Були навіть факти погрому приймаючої супутникової апаратури, що могла приймати інформацію, що суперечить релігійній ідеології країни.

Інформаційний простір має кілька визначень:

МІП визначається конституційними нормами окремих держав, міжнародними угодами та технічним забезпеченням процесу інформації. Він складається із державних (національних) інформаційних просторів, регіональних просторів а також просторів окремих територій.

З 1992 році в Україні широко обговорюється проблема формування інформаційного простору, захист від інформаційної експансії і створення інформаційного суверенітету держави. В Європі послуговуються іншими принципами. Там створюють єдиний інформаційний простір, який би включав в себе інформаційні простори всіх країн і був би захищений від американської експансії.

На сьогодні окремі регіони і країни визначають квоти на присутність у своєму інформаційному просторі транснаціональних монополій, інших держав та приватних осіб. Наприклад, Європейське співтовариство визначило таке співвідношення: 14% відводиться для вищезгаданих суб'єктів неєвропейського походження, 86% – для європейських суб'єктів. Окремі країни, наприклад Франція (яка проводить політику збереження франкофонії), виробляють спеціальне законодавство на присутність в своєму інформаційному просторі іншомовних (в даному випадку англомовних) представників.

Велике значення для формування і збереження національного інформаційного простору має законодавство про рекламу. Європейська конвенція про транскордонне телебачення від 1989 року має спеціальний додаток і протокол про розповсюдження реклами у Європейському інформаційному просторі, особливо якщо виробниками і розповсюдниками є неєвропейські суб'єкти. Він встановлює максимум, що дорівнює 17%, тобто 83% прибутку від реклами має залишатися в Європі.

Визначення інформаційних ресурсів є як в Конституції держави, так і в загальних законам про інформацію і доступі до інформації.

"До інформаційних ресурсів України входить вся належна їй інформація, незалежно від змісту, форм, часу і місця створення". **(Закон України "Про інформацію)**

- **Інформаційний потенціал** – це сукупність інформаційних засобів країни, що включають комп'ютерні мережі, національну систему інформації (національну інфраструктуру), сукупність самої інформації а також різновиди інформації. Сюди входять також інформаційно-аналітичні служби, видавництва, кіно, засоби масової комунікації і електронні видання.
- **Національний інформаційний продукт** – матеріальний або нематеріальний результат інформаційної діяльності, що створюється за допомогою поєднання інтелектуальної діяльності людини та синтезованих засобів зв'язку.

Національний інформаційний потік включає в себе технічні можливості інформації, компонентами яких є первісні засоби зв'язку (радіо, телефон, телеграф, телебачення, аудіо-, відеокасети).

Інфраструктура національного інформаційного потоку на базі сучасних комунікаційних технологій має такий вигляд: телеграф, телефон, факс, персональний комп'ютер, сканер, супутник, оптичні волокна зв'язку, кабелі, аудіо-відеоматеріали, бази даних. На сьогодні на території України в інформаційному просторі працює 300 ретрансляторів, які передають міжнародну і національну інформацію безпосередньо у пам'ять комп'ютерів, а потім – у локальні системи.

- **Конвергенція засобів зв'язку** – це поєднання різних засобів зв'язку у світових інформаційних мережах.

Джерела інформації – це передбачені, або встановлені законом, носії інформації, до яких входять документи, інші носії, що зберігають інформацію, повідомлення засобів масової комунікації, фундаментальну інформацію або публічні виступи.

Серед характеристик джерел інформації найважливішими є такі: статус джерела, надійність, кваліфікація, довіра до джерела, цінність і вага інформації. Всі джерела інформації поділяються на три типа: **відкриті, закриті і конфіденційні**. Є також поділ на особистісні джерела і опосередковані джерела. До **особистісних джерел** відносять безпосередньо осіб: дипломати, офіційні представники уряду, співробітники дипломатичних представництв а також інші офіційні особи, які висловлюють офіційну точку зору.

Міжособистісні – це джерела, до яких належать особисті контакти із широким типом предстаництва: суспільні, політичні, ділові, культурні, військові, соціальні економічні. Вони найчастіше використовуються у дипломатичній практиці, у діяльності міжнародних організацій, у посередництві між країнами, у врегулюванні міжнародних конфліктів та для передачі особистісної інформації. Тобто це зустрічі президентів 1 на 1, зутрічі дипломатів. До цих дхерел також можна віднести контакти, які відбуваються на рівні міністрів відповідних відомств для вирішення поточних, конфліктих та кризових проблем. Міжособистісні джерела, часто використовуються також у стратегічних напрямках діяльності, тобто розвідкою, а особливо промисловою розвідкою.

Опосередковані – це джерела, які виступають посередниками між конкретним джерелом інформації і суспільством (громадською думкою). До них відносять: засоби массової комунікації (газети, радіо, телебачення, реклама), інформаційно аналітичні установи, електронні засоби комунікації, архіви і бібліотеки та ін. джерела зберігання інформації. Тобто фактично опосередковні джерела інформації – джерела із 2-х або третіх рук.

Опосередковані джерела поділяються на:

Офіційні – органи держ. викон. влади, спеціалізовані нуково-дослідні інституції та установи, відомчі установи, силові структури та ін. держ. органи, які виступають з офіцйною точкою зору. Крім того органи статистики, інформаційно-аналітична

економічна інформація, (тобто аналіз економіки по всіх галузях), інформацію, яка подається установами соціальної політики і праці, інститутом демографії (да інші установи, що вивчають демографію), інформацію статистики промисловості (доходи, валовий збір, кредити та ін.), інформацію силових структур. Є офіційна точка зору, якоїсь установи (заява, нота) і є особиста точка зору представника цієї організації - це дві великі різниці.

Неофіційні – це джерела, які використовують суб'єктивні оціночні прогнози та аналізи соціально-економічної та політичної ситуації, політичні партії і рухи, громадські організації та структури (політична партія, якщо вона не є домінуючою в державі не може виступати від імені держави з офіційної точки зору), соціологічні дослідження, аналітичні прогнози, повідомлення засобів массової комунікації, якщо вони не є офіційними представниками виконавчої влади (зараз в Україні офіційна точка зору виконавчої влади висловлюється через газету «Урядовий кур'єр»), незалежні соціологізні дослідження, джерела які стосуються певних релігійних концессій та національних меншин. Крім того офіційні та неофіційні д жерела поділяються на:

Відкриті – інформація, яка публікуєтсья в офіційних дослідженнях, відомостях (ВР, Кабмін), повідомлення про наукові розробки, діяльність помисловості, банківської системи.

Інформація загального характеру: політична, економічна, військова для оцінки економічного та політичного потенціалу держави Така інформація використовуються для складання прогнозів на довготривалий період а також для прийняття рішеннь політичними, економічними та військовими органами. Ця інформація потрібна для політичної економічної стратегії, для дипломатії під час переговорів і для планування політичних кроків у майбутньому.

Спеціальна інформація, яка стосується конкретної галузі. Вона може мати відношення до економіки, науки, сировинних ресурсів, віійськової справи. Ця інформація – частина загального стратегічного платування а також призначена для аналізу і прогнозування вузьким колом спеціалістів.

Закриті: до них належать: розвідувальні, дипломатичні, стратегічні, статистичні джерела (наприклад статистика про продукцією військового комплексу, інформація про кількість народжених і померлих), інформація про новітні технології, які становлять держ. таємницю, а також всю інформація, яка вважається таємною. До закритої інформації (джерела) відносять: інформацію, що міститься у директивах і вказівках посадовим особам, які представляють державу на переговорах, консультаціях та нарадах з політичних питаннь; інформацію про стратегію і планування зовнішньої політики; відомості про номенклатуру, обсяги фінансування операцій експорту та імпорту озброєння. Кожна країна має закон «про держ. таємницю і національну безпеку», і додаток «звіт відомостей, що становлять державну таємницю». Цей додаток встановлюється і змінюється відповідно змінам приоритетів держави.

Кофіденційні – джерела, які захищаються законом і які володіють інформацією спеціального призначення з точки зору зацікавлених країн. Під конфіденційнми джерелами розуміють документи, публікації, технічні носії інформації, технічні засоби обробки інформації, інформаційні продукти промислової, інтелектуальної

політичної сфери, а також інформація, яку відносять до розвідувальної інформації. *До них відносять джерела розвідки, закриті джерела міністерств і відомств* (є 3 ступіні секретності 5, 10, 15 років, після закіняення цього стоку інформацію можуть розсекретити – оприлюднити). Конфіденційні джерела інформації, на які посилаються при вирішенні тих чи інших питаннь (оприлюднені) завжди не називаються. Конфіденційне джерело розкривається тільки у випадку проведення судового слідства із санкцій прокурора, або коли інформація має характер, що стосується життєдіяльності всієї цівілізації, життєдіяльності і існування людства (наприклад, розробка бактеоріологічної зброї в Іраку, аварія на ЧАЕС).

Джерела дезінформації.

Ними можуть виступати: спеціалізовані відомства; опосередковані джерела, які видають неперевірену інформацію. Ці джерела найчастіше використовуються для перевірки на політичні економічні та військові кроки держави, на вивчення думки громадськості, що до прийняття рішеннь, для свідомого перекручування інформації з метою досягнення ласних інтересів.

Витік інформації (пробні шари). Це метод дезінформації для вивчення думки громадскості. «Веер» – методика, коли інформація спочатку розповсюджується в ін. країнах, а потім звідти просочується в нашу з посилкою на зарубіжні джерела.

Методи дезінформації дуже поширені, їх використовували (і будуть) на макрорівні для певних цілей.

Джерела інформації по фірмах.

Для вивчення фірм використовуються різні джерела інформації, за якими:

- визначають ***фірми-конкуренти***, їх стратегію і тактику,
- визначають фірми-нейтрали,
- розробляють оптимальну стратегію бізнесу,
- ведуть відбір ***оптимальних (можливих) контрагентів*** і відбір найбільш конкурентноспроможного товару або послуги.

Вимоги до таких джерел інформації:

- достовірність,
- повнота,
- актуальність змісту,
- точність даних.

Джерела інформації про фірми класифікують наступним чином:

1) інформація про фірми, яка надається ***міжнародними організаціями та установами ООН***;
2) інформація про фірми, яка надається ***спеціалізованими організаціями***;
3) інформація, яка надається ***спеціалізованими банками даних***;
4) інформація, яка надається ***спеціалізованими засобами масової комунікації*** (діловими виданнями);
5) інформація, яка надається ***самою фірмою*** (фірмова інформація);
6) неформалізована ***особиста інформація***.

1. Такими джерелами інформації є міжнародні економічні організації системи ООН, які складають досьє на фірми на основі інформаційних технологій. Такі досьє називаються ***"ростерами",*** вони включають в себе інформацію про промисловий розвиток регіонів, економічну та науково-технічну допомогу країнам, що

розвиваються. Сюди відносяться *UNIDO* (United Nations Industrial Development Organization – організація ООН по промисловому розвитку), *ПРООН* (Програма розвитку ООН), *ГАТТ* (General Agreement on Trade and Tariffs – Генеральна угода про тарифи і торгівлю), *WTO* (World Trade Organization – Всесвітня торгова організація).

Одним із найдостовірніших джерел є **UNIDO**, вона має досьє на 800 тис. фірм різного профілю. Структура і склад досьє UNIDO розроблена англійськими спеціалістами в галузі маркетингу. Банк даних UNIDO про фірми і організації формується на основі анкет-запитань, які UNIDO направляє фірмам, що становлять міжнародний інтерес.

В досьє UNIDO входять такі питання:

- базові дані (адреса фірми, імена відповідальних співробітників, юридичний статус фірми);
- фінансове становище;
- банк, з яким працює фірма;
- напрями діяльності;
- кількість зайнятих у фірмі службовців;
- наявність дочірніх компаній у країні і за кордоном;
- залежність фірми від інших фірм у фінансовому становищі;
- членство в міжнародних спеціалізованих асоціаціях і організаціях.

Додатково в досьє включається інформація про професійний рівень персоналу фірми в будь-яких відділеннях (основних та дочірніх), про основну спеціалізацію фірми, дані про виробничо-технічний досвід, консультаційні послуги фірми, обсяг і характер проектів, здійснених фірмою, місця, де ці проекти були здійснені, характеристика маркетингу фірми та технології "паблік рілейшенз". Досьє UNIDO постійно коректуються у залежності від становища фірм, їх прогресу на світовому ринку, можливої стратегії їхнього розвитку. Крім UNIDO, повну інформацію про фірми можна отримати у публікаціях центру ООН по ТНК, а також у довідниках Європейської економічної комісії ООН.

2. До ***спеціалізованих джерел інформації*** про фірми належать: державні організації, торгово-промислові палати, спілки підприємців, консультаційні фірми, банки і кредитно-довідкові бюро. Найбільш дорогою і конфіденційною є інформація про фірми, яка надається спеціалізованими інформаційними агентствами і кредитно-довідковими бюро.

У довідках на фірми, які видаються кредитними бюро, включаються неопубліковані дані про фінансове становище фірми, фінансовий оборот, акціонерний капітал, історію створення фірми, характер і основні напрямки діяльності, перелік виробництв і дочірніх фірм, склад і біографічні дані керівників, фінансові показники діяльності фірми за останній рік, скорочений баланс, показники прибутку і витрат фірми. Найбільша кредитно-довідкова фірма у світі - американська компанія **Dun&Bradstreet Corporation**. Заснована в 19 столітті, має найбільшу приватну базу даних. У 70-х роках фірма придбала німецьку інформаційну компанію з усіма дочірніми філіалами у Західній Європі, Кредитне бюро Італії, англійське кредитне бюро, інформаційні фірми скандинавських країн.

Збір інформації відбувається через мережу філіалів і дочірніх компаній, способи передачі інформації різноманітні, використовується широкий перелік видів каналів зв'язку: кур'єрська доставка, телефонні розмови, факси, комп'ютерні мережі, інші канали зв'язку, магнітні плівки, CD-диски, вирізки з друкованих ЗМІ.

Ця фірма щорічно публікує понад 60 видів міжнародних і національних довідників по фірмах, вона є монополістом у сфері програмного забезпечення.

Фірма надає фінансову інформацію по галузях високих технологій, аналіз стану ринків, інформацію про страхування фірм. Міжнародна база даних цієї організації включає 14 млн. досьє. Окремо фірма має базу даних по США (понад 10 млн. довідок). Зараз представництво цієї фірми є в СНД (штаб-квартира знаходиться в Москві).

У анкеті-запиті компанія збирає такі дані: назва, рік створення фірми; номер і дата реєстраційного свідоцтва; назва банку, де відкритий валютний рахунок; основні напрямки діяльності; зарубіжні партнери; дочірні фірми як у країні, так і за кордоном; статутний фонд на момент створення і на поточний момент; засновники фірми; фінансова інформація про річний балансовий звіт. Інша всесвітньо відома кредитно-довідкова організація – австрійська фірма **Kreditschutzverband**. На ці дві фірми приходиться 85% світового ринку інформації про фірми.

3. ***Спеціалізовані банки даних.*** СБД створюються консультативними видавничими фірмами, комп'ютерними фірмами, які спеціалізуються на виробництві і збуті програмних продуктів. Такі фірми обслуговують кілька банків даних і відповідають за достовірність і своєчасність її оновлення.

Існує 2 групи Баз Даних:

1) традиційні, лідером серед яких є система Діалог (має 400 баз даних);
2) бази даних електронної пошти. Найбільша – база даних електронної пошти належить корпорації AOL (America On-line) і працює в режимі постійних електронних конференцій.

Найбільша база даних належить корпорації Dun&BradStreet Corp. Спеціалізується на зборі, обробці та наданні інформації у галузі економіки, бізнесу, маркетингу. Інформація в цих базах даних має виключно конфіденційний характер, її збір і обробка відбувається за участю урядових структур країни.

4. ***Спеціалізовані засоби масової комунікації*** – це газети, журнали, радіо-, телепродукція, електронні засоби масової комунікації, які надають інформацію про поточну діяльність фірм.

Найбільше інформації про поточну діяльність фірм має Dow Jones. Вони публікують дані про випуск окремих видів продукції, капіталовкладень, стан замовлень, структуру фірми, призначення і переміщення співробітників, вартість акцій, рівень ділової активності і т.і.

5. ***Фірмова інформація*** – це річні звіти про діяльність фірм, представницька інформація, фірмові каталоги.

6. ***Особиста (неформалізована) інформація*** є конфіденційною, найбільш достовірною. Вона поділяється на 2 види:

1) ***інформація, отримана під час ділових контактів, переговорів, зустрічей***. Ця інформація систематизується у формі довідки на фірму.

2) ***інформація на фірму, яка отримується з інших джерел*** (від представників влади, конкурентні фірми, Торгово-промислової палати, маркетингових дослідників фірми, аналітиків, представників оптової та роздрібної торгівлі).

4. Інформаційна безпека в сучасному світі.

Інформаційна безпека має кілька напрямків:

1. ***Один із таких напрямків*** – це система заходів, спрямованих на недопущення несанкціонованого доступу до інформації, несанкціонованої її модифікації або порушення цілісності. Цей напрямок часто називають Informational Security.

2. ***Другий напрямок інформаційної безпеки*** – це захист політичних, державних і громадських інтересів країни, захист загальних моральних цінностей, недопущення закликів до порушення територіальної цілісності, заборона інформації, яка включає ідеї війни, насилля, дискримінації і посягання на права людини.

3. Попередження розповсюдження відомостей, що становлять державну таємницю, а також відомостей з обмеженим доступом і інформації закритого типу, що переміщається через державний кордон.

Інформаційне забезпечення урядів, різноманітних державних органів, недержавних організацій та фірм визначається відповідно до їх потреб, у кожному конкретному випадку.

- **Інформаційна безпека – це стан захищеності суспільства, держави, особистості, стан захищеності інформаційних ресурсів, які забезпечують прогресивний розвиток життєво важливих сфер суспільства**.

Інформаційна безпека в різних сферах суспільства має свою специфіку:

У політиці інформаційна безпека стосується інформаційно-аналітичної діяльності дипломатичних представництв і зовнішньо-економічних відомств.

В економіці інформаційна безпека стосується захисту інформації у банківських системах та мережах зв'язку, захисту конфіденційної економічної інформації від несанкціонованого доступу.

Поняття інформаційної безпеки тісно пов'язане із поняттям інформаційної загрози.

Об'єктами захисту інформації виступають:

- документи,
- програми ЕОМ,
- ноу-хау,
- бази даних,
- тексти, на яких зафіксована інформація,
- інші матеріальні носії інформації, захист яких передбачений державними нормативними актами, внутрівідомчими постановами та розпорядженнями, іншими спеціальними документами.

Найбільш важливі види інформації, яких стосується проблема інформаційної безпеки є:

- стратегічна інформація;
- політична інформація;
- соціально-економічна інформація;
- воєнна інформація;

наукова інформація

4.1 Аутентифікація користувачів та забезпечення цілісності повідомлень .

З широким розповсюдженням в сучасному світі електронних форм документів і засобів їх обробки, актуальною стала проблема встановлення оригіналів та авторства електронної документації . Для часткового вирішення цієї проблеми застосовуються засоби аутентифікації . Засоби аутентифікації, які використовуються в комплексі з криптографічними алгоритмами забезпечують високий рівень захисту інформації.

В наш час існує три задачі аутентифікації :

1. **аутентифікація користувачів** - полягає в періодичній перевірці достовірності ідентифікації користувача;
2. **аутентифікація даних** – перевірка того, що масив даних не був змінений на протязі неконтрольованого проміжку часу;
3. **аутентифікація повідомлень** – встановлення авторства повідомлень, які один абонент посилає іншому по відкритому каналу зв'язку .

Аутентифікація користувачів може здійснюватися як апаратними, так і програмними методами. При апаратній реалізації користувач може бути аутентифікований за певними фізичними ознаками, іншими словами по біометричному принципу. Можуть використовуватися додаткові особисті речі: наручні браслети, ключі. Даний вид аутентифікації характеризується вищим рівнем надійності, проте є складнішим та дорожчим у використанні, тому використовується на підприємствах, яким необхідно забезпечити високий рівень захисту інформації. Дешевший варіант аутентифікації користувачів полягає у створенні програмних засобів. Програма аутентифікації є резидентною програмою. Вона періодично з певним кроком часу задає випадковим чином запитання із заздалегідь створеного файлу. КС порівнює відповіді користувача з наперед зареєстрованими або обчисленими відповідями, і на основі цього надає або забороняє користувачу подальшу роботу в КС. У випадку неправильної відповіді - користувач втрачає можливість роботи і повинен заново ввійти в комп'ютерну систему.

Основні способи аутентифікації користувачів:

1) наперед визначена інформація, якою може користуватися користувач: пароль, персональний ідентифікаційний номер, спеціальні фрази;
2) елементи апаратного забезпечення:ключі, магнітні карточки, мікросхеми;
3) характерні особисті ознаки користувача: відбитки пальців, рисунок сітківки очей,тембр голосу;
4) характерні навики та риси поведінки користувача в режимі реального часу: стиль роботи на клавіатурі, прийоми роботи з маніпулятором миші (швидкість відповідної реакції на запити, швидкість читання текстів);

5) навики та знання користувачів, обумовлені освітою, культурою, навчанням, вихованням, звичками**.**

Процедура аутентифікації користувачів може бути реалізовано як з постійним періодом повтору, так і з змінним періодом. При досить великому періоді повтору збільшиться ймовірність несанкціонованого доступу, а при досить малому зменшується ефективність роботи користувача, оскільки користувач постійно відволікається від виконання основної роботи.

Крім того, після встановлення достовірності ідентифікації користувача реєструються всі дії користувача в операційному журналі системи. В такому журналі крім записів санкціонованого використання тих чи інших ресурсів системи, можуть накопичуватися дані про спроби несанкціонованого доступу користувачів з автоматичною сигналізацією адміністратору системи для прийняття організаційних заходів. Програма аутентифікації повинна заборонити усі види переривань.

Біометрія – ідентифікація людини по унікальним, властивим тільки їй біологічним ознакам. Системи доступу і захисту інформації, засновані на таких технологіях, є не тільки самими надійними, але самими зручними для користувачів на сьогоднішній день.

Основні переваги цієї технології:

1. висока надійність (підробити папілярний візерунок пальця людини або райдужну оболонку практично неможливо);
2. простота ідентифікації для користувача (сканування відбитка пальця простіша операція ніж введення паролю, тому проводити цю процедуру можна не тільки перед початком роботи, але і під час її виконання, що, природно, підвищує надійність захисту. Особливо актуально в цьому випадку використання сканерів, сполучених з комп'ютерними пристроями. Так, наприклад, є миші, при використанні яких великий палець користувача завжди лежить на сканері. Тому система може постійно проводити ідентифікацію, причому людина не тільки не буде припиняти роботу, але і взагалі нічого не помітить);
3. неможливість передачі користувачам своїх ідентифікаційних даних третім особам. У сучасному світі, на жаль, продається практично все, у тому числі і доступ до конфіденційної інформації. Тим більше що людина, що передала ідентифікаційні дані зловмисникові, практично нічим не ризикує. Про пароль можна сказати, що його підібрали, а про апаратний ключ або смарт-картку, що їх витягли з кишені. У випадку ж використання біометричного захисту подібний "фокус" уже не пройде.

Недоліки:

1. Найбільший недолік біометричних систем захисту інформації - ціна. І це незважаючи на те, що вартість різних сканерів істотно знизилася за останні два роки. Правда, конкурентна боротьба на ринку біометричних пристроїв здобуває усе більш тверді форми. А тому варто очікувати подальшого зниження ціни.

2. Ще один недолік біометрії - дуже великі розміри деяких сканерів. Природно, це не відноситься до ідентифікації людини по відбитку пальця і деяких інших параметрів. Мало того, у деяких випадках узагалі не потрібні спеціальні пристрої. Цілком достатньо обладнати комп'ютер мікрофоном або веб-камерою.

Біологічні ознаки розбиті на дві великі групи: **статичні та динамічні ознаки**. До **статичних** ознак відносяться відбитки пальців, райдужна оболонка і сітківка ока, форма особи, форма долоні, розташування вен на кисті руки (термограма) і т.д. Тобто тут перераховане те, що практично не міняється згодом, починаючи з народження людини. **Динамічні ознаки** - це голос, почерк, клавіатурний почерк, особистий підпис і т.п. Загалом, до цієї групи відносяться так звані поведінкові характеристики, тобто ті, котрі побудовані на особливостях, характерних для підсвідомих рухів у процесі відтворення якої-небудь дії. Динамічні ознаки можуть змінюватися з часом, але не різко, стрибком, а поступово.

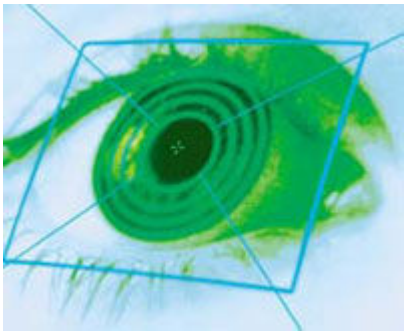
Ідентифікація людини по статичних ознаках більш надійна. Не можна знайти двох людей з однаковими відбитками пальців або райдужною оболонкою ока. Але, на жаль, усі ці методи вимагають спеціальних пристроїв, тобто додаткових витрат. Ідентифікація по динамічних ознаках менш надійна. Крім того, при використанні цих способів досить велика імовірність виникнення "помилок першого роду" – імовірність помилкового доступу. Наприклад, під час застуди в людини може змінитися голос. А клавіатурний почерк може змінитися під час стресу, випробовуваного користувачем. Але зате для використання цих ознак не потрібно додаткове устаткування. Для побудови найпростішої біометричної системи захисту інформації потрібні клавіатура, мікрофон або веб-камера, підключена до комп'ютера, і спеціальне програмне забезпечення.

Основні принципи роботи біометричних систем захисту.

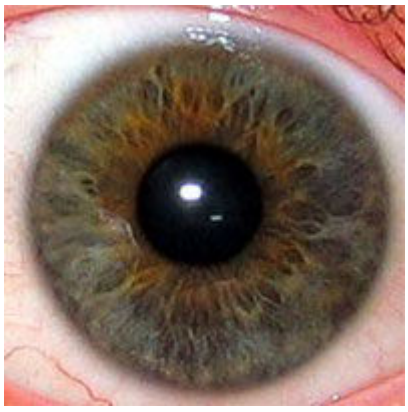
В пам'яті комп'ютера зберігається не зразок відбитка пальця, голосу людини або картинка райдужної оболонки її ока. У спеціальній базі даних зберігається цифровий код довжиною до 1000 біт, що асоціюється з конкретною людиною, що має право доступу. Сканер або будь-який інший пристрій, використовуваний у системі, зчитує визначений біологічний параметр людини. Далі він обробляє отримане зображення або звук, перетворюючи їх у цифровий код. Саме цей ключ і порівнюється з вмістом спеціальної бази даних для ідентифікації особистості. Переваги ідентифікації по цифровому коду згенерованому на основі отриманого

сканером образу очевидні. По-перше, малюнок відбитка з гарною якістю займає досить багато місця. Обсяг бази даних, у якій зберігаються дані про тисячі користувачів є дуже великим. Повне порівняння двох образів-картинок - процедура досить тривала. Але ж для того, щоб підібрати підходящий, потрібно перебрати безліч відбитків. Ну і, по-третє, будь-який невеликий поріз або подряпина на подушечці пальця користувача приведуть до відмовлення в доступі. У той час як при ідентифікації по цифровому коді допускається похибка до 30% площі малюнка без збитку для роботи системи.

Ідентифікація по райдужній оболонці ока.



На сьогоднішній день існує багато різних біометричних технологій. І усі вони використовують різні ознаки людини, унікальні для кожної особистості. Найбільше поширення серед біометричних технологій одержала ідентифікація по відпечаткам пальців. Правда, останнім часом усе велику і велику популярність здобуває використання як робочу ознаку райдужної оболонки ока. І, якщо задуматися, у цьому немає абсолютно нічого дивного. Справа в тім, що райдужна оболонка - елемент досить унікальний. По-перше, вона має дуже складний малюнок, у ній багато різних елементів. Тому навіть не дуже якісний її знімок дозволяє точно визначити особистість людини. По-друге, райдужна оболонка є об'єктом досить простої форми (майже плоске коло). Так що під час ідентифікації дуже просто врахувати всі можливі перекручування зображення, що виникають через різні умови зйомки. Ну і, нарешті, по-третє, райдужна оболонка ока людини не міняється протягом усього його життя із самого народження. Точніше, незмінної залишається її форма (виключення складають травми і деякі серйозні захворювання очей), колір же згодом може змінитися. Це додає ідентифікації по райдужній оболонці ока додатковий плюс у порівнянні з багатьма біометричними технологіями, що використовують відносно недовговічні параметри, наприклад геометрію особи або руки.



До речі, в ідентифікації особистості по райдужній оболонці ока є ще одна серйозна перевага. Справа в тім, що деякі біометричні технології страждають одним недоліком. При установці в настроюваннях системи ідентифікації високого ступеня захисту від помилок першого роду (імовірність помилкового допуску) імовірність появи помилок другого роду (помилковий недопуск у систему) зростає до недозволено високих величин декількох десятків відсотків. Отож, ідентифікація по райдужній оболонці ока цілком урятована від цього недоліку. У ній співвідношення помилок першого і другого родів є одним із кращих на сьогоднішній день. Для приклада можна привести кілька цифр. Дослідження

показали, що при імовірності виникнення помилки першого роду в 0,001% (відмінний рівень надійності) імовірність появи помилок другого роду складає усього лише 1%.

На жаль, є в розглянутої технології і недоліки. І першим з них є відносно висока вартість устаткування. І дійсно, для проведення дослідження потрібна як мінімум камера, що буде одержувати початкове зображення. А коштує цей пристрій набагато дорожче, ніж, наприклад, сенсор відбитків пальців. Крім того, вона вимагає досить багато місця для розміщення. Усе це обмежує область використання ідентифікації особистості по райдужній оболонці ока. На сьогоднішній день вона застосовується в основному в системах допуску на різні об'єкти як цивільного, так і військового призначення.

Ну а тепер, коли ми розглянули основні переваги і недоліки ідентифікації особистості по райдужній оболонці ока, давайте розберемося, як вона здійснюється. Першим етапом, природно, є одержання досліджуваного зображення. Робиться це за допомогою різних камер. Причому варто відзначити, що більшість сучасних систем припускає використання для ідентифікації не одного знімка, а декількох. Вони необхідні для одержання більш повного зображення радужки, а також можуть використовуватися при деяких способах захисту від муляжів (докладніше про це ми будемо говорити пізніше).

Другий етап - виділення зображення райдужної оболонки ока. Узагалі ж, особою складності він не представляє. Ми вже говорили, що радужка - це досить темна (щодо білка ока) майже плоска фігура, більш-менш схожа на коло. Крім того, усередині неї повинна знаходитися ще одна окружність, що дає сильні відблиски (зіниця). Сьогодні розроблена безліч способів точного одержання границі райдужної оболонки по описаних ознаках. Єдиною проблемою є області, закриті повіками. Втім, вона вирішується за допомогою створення протягом одного сеансу декількох знімків. Адже століттям властиві мимовільні рухи, тремтіння. Таким чином то, що приховано на одному знімку, може виявитися видно на іншому. Крім того, на райдужній оболонці ока настільки багато різноманітних елементів, що, по деяким даним, для надійної ідентифікації досить усього лише 30-40 відсотків з них. Так що багато систем взагалі ігнорують закриті області без помітного збитку для надійності.

Наступний етап ідентифікації - це приведення розміру зображення радужки до еталонного. Це потрібно по двох причинах. По-перше, у залежності від умов зйомки (освітленість, відстань для об'єкта) розмір зображення може змінюватися. Відповідно й елементи радужки теж будуть виходити різними. Утім, з цим особливих проблем не виникає, тому що задача вирішується шляхом масштабування. А от із другою причиною справи йдуть не так добре. Справа в тім, що під впливом деяких факторів може мінятися розмір самої радужки. При цьому розташування її елементів відносно один одного стає трохи іншим. Для рішення цієї

задачі використовуються спеціально розроблені алгоритми. Вони створюють модель райдужної оболонки ока і по визначених законах відтворюють можливе переміщення її елементів.

Наступною дією є перетворення отриманого зображення райдужної оболонки ока в полярну систему координат. Це істотно полегшує всі майбутні розрахунки. Адже радужка - це майже коло, а всі основні її елементи розташовуються по окружностях і перпендикулярним їм прямим відрізкам. До речі, у деяких системах ідентифікації цей етап неявний: він сполучений з наступним.

П'ятим кроком у процесі ідентифікації особистості є вибірка елементів райдужної оболонки ока, що можуть використовуватися в біометрії. Це самий складний етап. Проблема полягає в тім, що на райдужній оболонці немає якихось характерних деталей. А тому не можна використовувати ставшими звичними в інших біометричних технологіях визначення типу якоїсь крапки, її розміру, відстані до інших елементів і т.д. У даному випадку використовуються складні математичні перетворення, що здійснюються на основі наявного зображення радужки.

Ну і, нарешті, останнім етапом ідентифікації людини по райдужній оболонці ока є порівняння отриманих параметрів з еталонами. І в цієї дії є одна відмінність від багатьох інших подібних задач. Справа в тім, що при виділенні унікальних характеристик необхідно враховувати закриті області. Крім того, частина зображення може бути перекручена століттями або відблисками від зіниці. Таким чином, деякі параметри можуть істотно відрізнятися від еталонного. Утім, ця проблема досить легко вирішується завдяки надлишковому змістові на райдужній оболонці ока унікальних для кожної людини елементів. Як ми вже говорили, збігу 40% з них досить для надійної ідентифікації особистості. Інші ж можуть вважатися "зіпсованими" і просто-напросто ігноруватися.

Ну а тепер прийшла настав час підвести підсумки. Незважаючи на деякі недоліки, технологія ідентифікації особистості по райдужній оболонці ока є досить перспективною. Особливо гарна вона завдяки своїй надійності і гарному співвідношенню помилок першого і другого роду для систем доступу до різних цивільних і військових об'єктів. Ну а якщо врахувати ще і незмінність радужки протягом усього людини життя, то стає зрозуміло, що ця технологія цілком може бути використана для створення біометричних паспортів, про які останнім часом ведеться безліч споровши в багатьох країнах світу.

Сама, мабуть, велика складність, з яким довелося зштовхнутися розроблювачам технології, - це забезпечення нормальних умов зйомки райдужної оболонки. Справа в тім, що поверхня ока звичайно відбиває сторонні джерела світла, створюючи на зображенні сильні відблиски. Природно, це дуже сильно погіршує точність ідентифікації. Для того щоб "перебороти" відблиски, необхідно використовувати власне підсвічування, причому її яскравість повинна бути як мінімум у кілька разів більше яскравості сторонніх джерел світла. У перших системах ідентифікації для цього використовувався спалах на зразок тих, котрі застосовуються у фотоапаратах. Правда, таке рішення не подобалося кінцевим користувачам. І дійсно, мало приємного в яскравому світлі, спрямованому прямо в око. Утім, сучасні системи позбавлені цього недоліку. У них застосовується інфрачервоне підсвічування, що не доставляє користувачам ніяких незручностей.

Іншою проблемою, зв'язаної зі зйомками райдужної оболонки, є позиціонування ока. Справа в тім, що для одержання повного, якісного зображення необхідно, щоб райдужна оболонка знаходилася на визначеному (фокусному) відстані від камери в строго обмеженій зоні. Але адже в просторі не прочертиш лінії. А як по-іншому можна обмежити необхідну зону? Пошуком рішення цієї задачі займалося кілька компаній. У результаті з'явився цілий ряд різних розробок. Але найбільше поширення одержали тільки чотири з них.

Одним з найпростіших рішень задачі установки ока користувача в потрібне положення є використання так званих фіксаторів погляду. Звичайно ними є невеликі лампочки або спрямовані світлодіоди. Вони встановлюються на сканер таким чином, щоб світло було видно тільки при визначеному положенні ока (потрібному для одержання якісного зображення). Таким чином, користувач сам повинний буде знайти поглядом фіксатор і ненадовго завмерти в цьому положенні.

Іншим варіантом є використання прозорих з однієї сторони маленьких дзеркал. Для проведення процесу ідентифікації користувач повинний підійти до сканера і встати так, щоб побачити відображення власного ока. З іншої сторони дзеркала встановлена камера. Таким чином, користувач сам може установити своє око в потрібне для ідентифікації положення.

Третій варіант уже більш складний. У сканер крім камери вбудовуються кілька додаткових сенсорів і підсистема розпізнавання особи. Далі процес ідентифікації відбувається в такий спосіб. Спочатку користувач підходить до сканерові. Потім пристрій розпізнає особа й обчислює його місце розташування. А далі за допомогою голосу або спеціальних покажчиків людині подаються команди про переміщення (уліво, вправо, ближче, далі і т.д.) доти, поки його око не потрапить у потрібну зону. Правда, варто відзначити, що додаткове устаткування, встановлене в сканері, збільшує його кінцеву вартість.

Ну і, нарешті, є ще четвертий варіант рішення задачі позиціонування ока, самий складний у реалізації. Справа в тім, що крім перерахованого в попередньому абзаці устаткування сканер оснащується камерою на поворотній підставці. Це дуже зручно. Система визначає особу людини, що підійшла, і сама наводить камеру і встановлює неї в оптимальне для зйомки положення. Тобто від користувача для проведення ідентифікації не потрібно починати ніяких дій. На жаль, незважаючи на

свою виняткову зручність, це рішення не одержало великого поширення. Справа в тім, що сканери з поворотною камерою складні у виготовленні, а тому коштують досить дорого.

Іншою проблемою, з яким зштовхнулися розроблювачі систем ідентифікації особистості по райдужній оболонці ока, є можливість застосування підробки. Найпростішим випадком є пред'явлення камері фотографії ока. Крім того, сучасні технології дозволяють створювати досить точні муляжі цього органа. Для цього необхідні тільки цифрова фотографія.

Традиційні парольні системи мали великий недолік в тому, що аутентифікація проходила в односторонньому порядку, тобто користувач доказував системі свої права на роботу в КС , не сумнівався в праві системи отримувати від нього парольні відомості. Така ситуація в сучасних криптосистемах не приймається, із-за небезпеки втручання зловмисника в процес обміну.

Для ліквідації цього недоліку використовуються так звані протоколи рукостискання. В них одна сторона доказує іншій , що знає , спільну секретну інформацію без її розголошення в явному вигляді. Найбільш перспективними є протоколи аутентифікації з нульовим розголошенням даних.

Прикладом такого протоколу є система **Гіллоу-Куіскуотера.**
В якості відкритих параметрів використовується просте число N та ціле число V< (N-1).

Параметри N і V є статистично відкритими ключами і не змінюються від сеансу до сенсу. Їх розмір від 512 до 4096 двійкових розрядів.

1. Таємний ключ **x**. Вибирають число **y** , яке задовольняє умову : ($y*x^v$)mod N=1;
2. сторона ***A*** вибирає ціле число r<(N-1), обчислює значення: T=(r^vmod N) і передає стороні ***B*** числа **y** і **T**;
3. сторона ***B*** вибирає ціле число d<(N-1) і посилає стороні ***A***;
4. сторона ***A*** обчислює значення: D=r*x^d mod N і відправляє його ***B***;
5. сторона ***B*** самостійно обчислює функцію: $T' = (D^v y^d \bmod N)$ і порівнює результати з отриманим значенням ***T*** . Якщо $T = T'$, то сторона ***A*** дійсно знає секретне число ***x*** і їй можна довіряти.

4.2 Проблема аутентифікації даних та електронний цифровий підпис.

Уявіть собі ситуацію: вам відправили по електронній пошті документ з конфіденційною інформацією по фінансуванню на майбутній рік. Вам необхідна абсолютна впевненість в тому, що отриманий файл абсолютно ідентичний оригіналу і цифри, що містяться в ньому, не були змінені "в дорозі". Декілька скоректованих значень можуть коштувати вашій фірмі круглої суми. Підозра, що документ "в дорозі" був підроблений з'являється якщо деякі цифри не сходяться, а

електронна передача велася через зовнішню поштову систему. Як переконається в тому, що одержаний вами документ - абсолютна копія відправленого вам оригіналу?

В кінці звичайного листа або документа виконавець або відповідальна особа звичайно ставить свій підпис. Це дає можливість по-перше, переконатися одержувачу в оригінальності листа, порівнявши підпис із зразком, який у нього зберігається. По-друге, особистий підпис є юридичною гарантією авторства документа. Останній аспект особливо важливий при підписанні різного роду торгових домовленостей, складенні довіреностей.

Якщо підробити підпис людини на папері досить не просто, а встановити авторство підпису сучасними криміналістичними методами – технічна деталь, то з електронним підписом справа стоїть зовсім інакше. Підробити послідовність бітів зможе любий користувач ЕОМ.

Під поняттям "цілісність повідомлення" розуміють всю величину і точність повідомлення переданого по мережі. Безпека повинна забезпечувати конфіденційність даних, яка полягає в тому, що повідомлення отримає адресат і ніхто більше.

Найпростіший спосіб перевірки цілісності даних, переданих в цифровому представленні, - це **метод контрольних сум**. Під контрольною сумою (**digital fingerprint**) розуміють суму всіх чисел, яка складається з вхідних даних. Метод контрольних сум - це найпростіша форма цифрової аутентифікації, тобто величина, отримана в результаті підрахунку вмісту деяких інших даних, змінюється при корекції даних, на основі яких він отриманий.

Недолік методу контрольних сум полягає в тому, що хоча неспівпадання значень цих сум служить точним доказом, що даний документ піддався змінні, рівність порівнюваних значень ще не дає гарантії, що інформація залишилась незмінною. Можна довільним чином змінити порядок проходження чисел в документі, а контрольна сума при цьому збереже колишнє значення. Можна змінити окремі числа в документі і підігнати інші так, щоб забезпечити колишнє значення контрольної суми.

Електронним цифровим підписом називають приєднане до тексту його криптографічне перетворення, яке дає змогу в разі одержання тексту іншим користувачам перевірити авторство і достовірність повідомлення.

Технологія електронного підпису передбачає, що кожен абонент володіє двома ключами – відкритим і закритим. Закритий ключ абонента А використовується тільки для формування цифрового підпису, а відкритий ключ може бути використаний іншими абонентами для перевірки оригіналу отриманого від А повідомлення. Найбільш простим і поширеним інструментом електронного підпису є відомий нам алгоритм RSA, інший метод електронного підпису – це метод DSS (Digital Signature Algorithm).

Система аутинтифікації повідомлень використовується для захисту системи від таких порушень:

1) Відмова. Користувач А заявляє, що він не посилав повідомлення користувачу В, хоча насправді все таки послав. Для виключення такого порушення використовується електронний підпис.
2) Модифікація. Користувач В змінює повідомлення і запевняє, що таке повідомлення він отримав від користувача А.

3) Підробка. Користувач В формує повідомлення і запевняє, що таке повідомлення послав йому користувач А.
4) Активне перехоплення. Порушник перехоплює повідомлення між користувачами А і В для його модифікації.
5) Маскування. Порушник посилає користувачу В повідомлення від імені користувапча А.
6) Повтор. Порушник передає повідомлення, яке користувач А раніше передав користувачу В. На цей метод припадало в минулому багато випадків незаконного знищеня грошей в системах електронних платежів.

В алгоритмах цифрового підпису використовуються різні математичні принципи, але найчастіше використовуються однонаправлені функції. В 1991р. Національний інститут стандартів і технологій США розробив алгоритм цифрового підпису DSA.

DSA використовує параметри:

1) $p=2^{\alpha}$, де α приймає значення від 512 до 1014 біти і кратне 64.
2) q,h довільні
3) g=h(p-1)/q, h-довільне число < p-1, $\frac{h(p-1)}{q} \bmod p < 1$
4) x<q
5) $y=g^x \bmod p$

Крім цього алгоритм використовує **хеш-функції H(x).** Перші параметри p,q і g загальнодоступні і можуть поширюватися в мережі. Індивідуальний особистий ключ−x, загальнодоступний−y. Нехай користувач хоче підписати повідомлення m. Він вибирає випадковий номер r<q.

Обчислює $r=(g^{r \bmod p}) \bmod q$

$S=(H(m)+xr) \bmod q$.

Параметри r і S це електронний підпис. Їх можна послати разом із повідомленням або записати окремо.

Щоб перевірити оригінальність підпису сторона В обчислює

$W= y^{-1 \bmod q}$

$u_1=(H/m)\cdot w) \bmod q$

$u_2=(r\cdot w) \bmod q$

$V=((g^{u1}\cdot y^{u2}) \bmod p) \bmod q$, якщо V=r, то підпис А- дійсний

Хеш-функцією в криптографії називають такий алгоритм перетворення інформації, який перетворює стрічку бітів довільної довжини в стрічку бітів фіксованої довжини.

Хеш-функції використовуються для :

1) створення стиснутого повідомлення, яке застосовується в механізмах цифрового підпису;
2) для захисту паролів;
3) для побудови кода аутентифікації повідомлень.

До хеш-функції висуваються такі основні вимоги:

1. по відомому значенню функції H(m) неможливо або дуже складно знайти аргумент m.

2. для даного аргумента m неможливо знайти інший аргумент m′ такий що H(m)=H(m`).

Часто виникає ситуація, коли одержувач повинен доказати оригінальність повідомлення третій особі. Щоб мати таку можливість, до повідомлення повинна бути дописана цифрова сигнатура – стрічка символів, яка залежать від ідентифікаторів відправника, так і від змісту повідомлення.

4.3 Стандарт шифрування даних. Алгоритм DES.

Стандарт шифрування даних (Data Encryption Standart – DES) розроблений у 70-х роках фахівцями фірми IBM, у 1976 році прийнятий у якості федерального стандарту США для захисту комерційної та урядової інформації. Як і шифр одноразового блокноту DES оперує з інформацією поданою у двійковій формі.

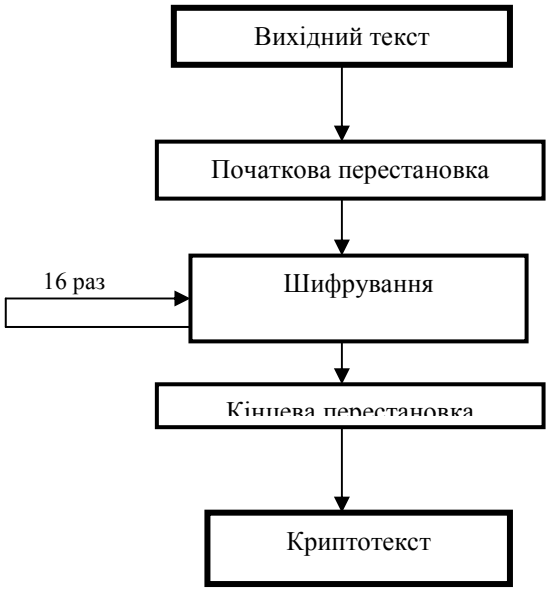
До теперішнього часу DES є найбільш поширеним алгоритмом, що використовується в системах захисту комерційної інформації.

Основні переваги DES:

1. Використовується ключ з фіксованою довжиною 64 біти. Істотне значення мають тільки 56 біт, решта 8 бітів – використовуються для контролю на парність;
2. Зашифрувавши повідомлення за допомогою одного пакету програм, для дешифрування можна використовувати будь-який інший пакет програм, що відповідає стандарту DES;
3. Відносна простота алгоритму забезпечує високу швидкість обробки;
4. Алгоритм має високу стійкість.

Алгоритм DES використовує комбінацію перестановок і підстановок. Всі перестановки підібрані розробниками таким чином, щоб максимально ускладнити процес дешифрування шляхом підбору ключа.

Всього двійкових ключів розміром 64 біти є 2^{64}. Елементарні обчислення показують, що процесор з тактовою частотою 100 МГц перебиратиме їх 10^8 тобто більше 5800 років. Повний перебір може бути в найгіршому разі. У середньому потрібний ключ буде знайдено аж за 2900 років, тобто за такий час коли таємниця втратить свою актуальність.



Узагальнена схема шифрування в алгоритмі DES.

Початкова перестановка та кінцева здійснюються відповідно до матриць IP та PI, які є матрицями (8*8).

Робота алгоритму DES:

Двійкове повідомлення яке розбивають на блоки по 64 біти кожен і шифрується кожен блок окремо, використовуючи один і той же ключ **К**, тобто повідомлення $\mathbf{M=M_1*M_2*M_3*\ldots*M_n}$ перетворюється у криптотекст $\mathbf{C=C_1*C_2*C_3*\ldots*C_n}$.

Нехай з файлу вихідного тексту прочитаний черговий блок $\mathbf{M_n=T}$. Цей блок перетворюється за допомогою матриці IP, яка має вигляд:

$$\begin{pmatrix} 58 & 50 & 42 & 34 & 26 & 18 & 10 & 2 \\ 60 & 52 & 44 & 36 & 28 & 20 & 12 & 4 \\ 62 & 54 & 46 & 38 & 30 & 22 & 14 & 6 \\ 64 & 56 & 48 & 40 & 32 & 24 & 16 & 8 \\ 57 & 49 & 41 & 33 & 25 & 17 & 9 & 1 \\ 59 & 51 & 43 & 35 & 27 & 19 & 11 & 3 \\ 61 & 53 & 45 & 37 & 29 & 21 & 13 & 5 \\ 63 & 55 & 47 & 39 & 31 & 23 & 15 & 7 \end{pmatrix}$$

Це перетворення запишемо $T_0=IP(T)$. Отримана послідовність бітів T_0 розбивається на дві послідовні частини:

старші біти **молодші біти**

L_0 – ліву, R_0 – праву, кожна з яких містить 32 біти.

Потім виконується ітерактивний процес шифрування, що складається з 16 циклів. Якщо $\mathbf{T_i}$ – результат і-тої ітерації, який представлений у вигляді:

$$T_i=L_i*R_i, \quad i=1\ldots16, \text{ то}$$
$$L_i=R_{i-1}$$
$$R_i=L_{i-1} \oplus f(R_{i-1},K_i).$$

Функція **f** називається функцією шифрування. Її аргументами є послідовність $\mathbf{R_{i-1}}$ і 48 бітовий ключ **К**1, який є результатом перетворення 64 бітного ключа **К**.

По закінченні шифрування здійснюється відновлення позиції за допомогою матриці PI тобто $\mathbf{C_n=PI(T_{16})}$.

Процес дешифрування даних є обернений по відношенню до процесу шифрування. Всі дії повинні бути виконані в оберненому порядку. Інтерактивний процес дешифрування може бути описаний наступними формулами:

$$R_{j-1}=L_j \qquad j=1\ldots16$$
$$L_{j-1}=R_j \oplus f(L_j,R_j)$$

$F(R_{i-1},K_i)$, K_i – 48 бітів.

Для обчислення значення функції **f** використовуються:

- функція **E** (розширення 32 біт до 48);
- функція **S**1…**S**8 (перетворення 6 бітового числа в 4 бітове);
- функція **P** (перестановка бітів в 32 бітній послідовності).

Нехай до 32 бітового блоку застосовують функцію **E** результат **$E(R_{i-1})$ – 48** бітовий блок. Додається за модвулем + (XOR) до 48-бітового ключа.

$E(R_{i-1})$ + $K_i=B_1…B_8$ B_i=6 бітів.

Функція **S** перетворює 6 бітове число в 4 бітне

4*8=32 отримаємо 32 біти.

Функція **P** ще раз переставляє блоки в 32 бітній послідовності

$F(R_{i-1},K_i)=P(S_1(B_1), . . . , S_8(B_8))$.

R_{i-1}(32 біти)

Для обчислення значення функції f використовуються :

- функція E (розширення 32 біт до 48);
- функція P (перестановка бітів в 32-х бітній послідовності).

Не кожній ітерації використовується нове значення ключа $\mathbf{K_j}$ (довжиною 48 біт). Нове значення ключа $\mathbf{K_i}$ обчислюється з початкового ключа **К** за допомогою функції **G.** Функція **G** в ключі **К** викидає контрольні біти, які знаходяться в позиціях: 8, 16, 24, 32, 40, 48, 56, 64, іпо спеціальній таблиці зсуває біти ключа вліво.

Для застосцвання алгоритму DES для рішення різноманітних криптографічних задач розроблено п’ять робочих режимів:

- електрона кодова книжка ECB
- зчеплення блоків шифру CBC
- обернений зв’язок по виходу OFB
- режим багатократного шифрування.

Режим “Електроної кодової книжки”. Довгий файл розбивають на 64-бітові відрізки по 8 байт. Можна представити у вигляді схеми:

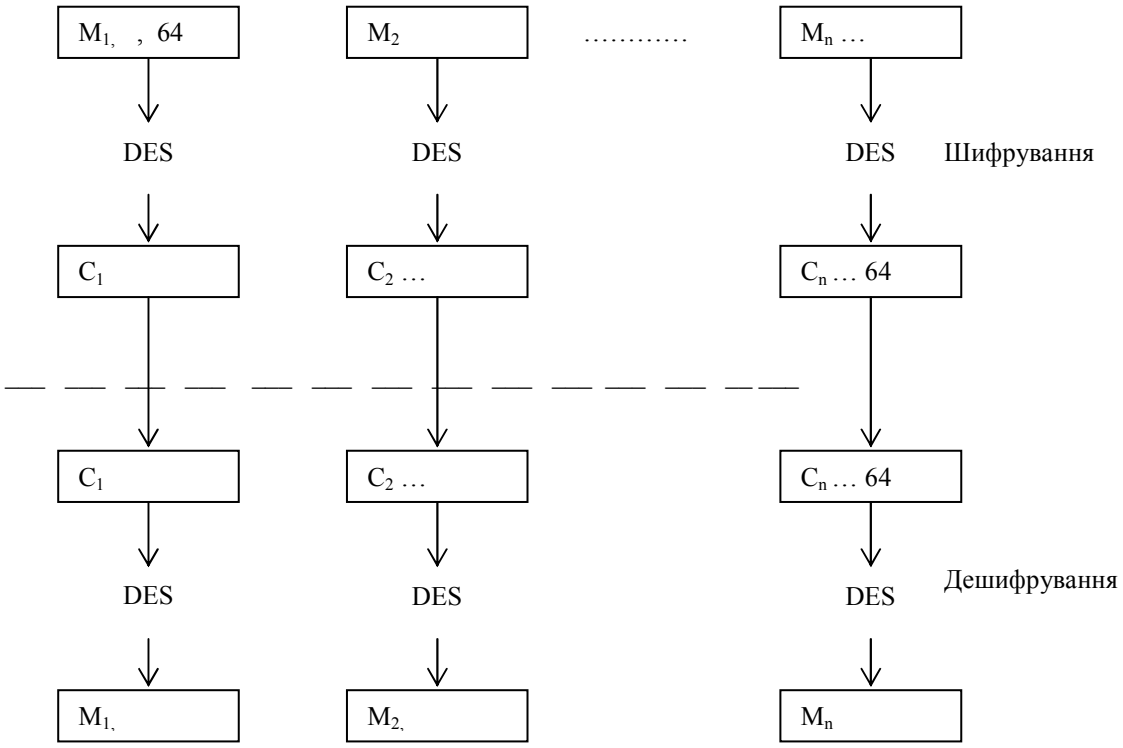


Схема алгоритму DES в режимі електроної кодової книжки.

Основна перевага – простота реалізації. Недолік відносно слабка стійкість проти кваліфікованих криптоаналітиків.

Режим зчеплення блоків шифру.

У цьому режимі початковий файл розбивають на блоки $\mathbf{M=M_1*M_2*\ldots*M_n}$. Перший блок $\mathbf{M_1}$ складається по модулю 2 з 64-бітовим початковим вектором, який міняється щодня і тримається в секреті. Отримана сума потім шифрується з використанням ключа DES, який відомий відправнику і одержувачу інформації. Отриманий 64-бітовий шифр $\mathbf{C_1}$ складається по модулю 2 з другим блоком тексту, результат шифрується.

4.4 Криптосистеми з відкритим ключем. Алгоритм RSA.

Якою б надійною та складною не була криптографічна система, її недоліком в практичній реалізації є розподілення ключів. Для того щоб була можливість обміну конфіденційною інформацією між двома суб'єктами АС, ключ повинен бути згенерований одним із них, а потім в конфіденційному порядку переданий іншому. Таким чином для передачі ключа необхідно використовувати криптосистеми або захищені канали зв'язку.

Для вирішення цієї проблеми, на основі результатів отриманих сучасною алгеброю, були запропоновані системи з відкритим ключем.

Суть їх полягає в тому, що кожним адресатом АС генерується два ключі, які математично пов'язані між собою. Один ключ використовується для шифрування вихідного тексту і називається **відкритим** ключем, другий для дешифрування називається **закритим** ключем. Знаючи зашифрований текст і ключ шифрування неможливо відновити вихідне повідомлення. Прочитати його можна тільки за допомогою другого ключа – ключа дешифрування. Відкритий ключ публікується в доступному місці, і доступний кожному, кому потрібно послати повідомлення адресату. Закритий ключ зберігається в таємниці. Криптосистеми з відкритим ключем називаються ще **асиметричними**.

Система переписування при використанні асиметричного шифрування виглядає в такий спосіб. Для кожного з N абонентів, що ведуть переписування , обрана своя пара ключів "відкритий E*i* " та "закритий D*i*", де *I* - номер абонента. Усі відкриті ключі відомі всім користувачам мережі, кожен закритий, навпаки, зберігається тільки в того абонента, якому він належить. Якщо абонент, скажемо під номером 7, збирається передати інформацію абоненту під номером 9 він шифрує дані ключем шифрування E9 та відправляє її абоненту 9. Незважаючи на те, що всі користувачі мережі знають ключ і можливо, мають доступ до каналу по якому йде зашифроване повідомлення, вони не можуть прочитати вихідний текст, тому що процедура дешифрування незворотня по відкритому ключу. І тільки абонент під номером 9, одержавши повідомлення, робить над ним перетворення за допомогою відомого тільки йому ключа D9 і відновлює текст повідомлення. Потрібно відмітити, що

якщо повідомлення потрібно відправити в протилежному напрямку (від абонента 9 до абонента 7), то потрібно буде використовувати іншу пару ключів (E7, D7).

Криптографічні системи з відкритим ключем використовують односторонні функції, для яких характерна слідуюча властивість:

При заданому значенні x відносно просто обчислити значення f(x) , але якщо відоме значення функції f(x) то достатньо важко або практично неможливо знайти значення аргумента x.

Щоб гарантувати надійний захист інформації системи з відкритим ключем повинні задовільняти такі вимоги:

1. перетворення відкритого тексту повинно бути незворотнім процесом і виключати можливість його відновлення на основі відкритого ключа;
2. знаючи відкритий ключ неможливо обчислити закритий.

Алгоритми шифрування з відкритим ключем отримали широке застосування в АС.

Асиметричні криптосистеми використовуються:

1. як самостійні засоби захисту даних, які передаються і зберігаються;
2. як засіб для розподілення ключів;
3. як засіб аутентифікації користувачів.

Алгоритм RSA.

На сьогоднішній час існує велика кількість систем з відкритим ключем, але найбільш практичне значення отримала система RSA назва якої походить від перших літер прізвищ її авторів (Rivest, Shamir, Adleman).

Вони скористалися тим фактом, що знаходження добутку двох великих простих чисел є достатньо простою задачею, але розклад добутку на множники є досить трудомістким процесом. Тому для будь-якої довжини ключа можна дати нижню оцінку числа операцій для розкриття шифру, з врахуванням продуктивності сучасних комп' ютерів оцінити необхідний на це час.

Можливість гарантовано оцінити захищеність алгоритму RSA стала однією із причин популярності цієї системи на фоні десятків інших систем.

Генерування ключів .

1. Майбутній отримувач шифрованого тексту вибирає два прості числа p,q.
2. Обчислює значення n=p*q.
3. Обчислює значення функції Ойлера φ(n)=(p-1)(q-1).
4. Вибирає довільне число d, яке є взаємно-простим із числом φ(n) і d< φ(n).
5. Знаходить число e мультиплікативно-обернене до числа d, тобто яке задовільняє рівність (d*e)mod φ(n)=1.

Таким чином *:*

Відкритий ключ***: параметри e,n.***

Таємний ключ*:* ***параметр: d****.*

Шифрування відбувається блоками . Для цього повідомлення записують у цифровій формі і розбивають на блоки так, що кожен блок позначає число, яке не перевищує n. Якщо блок записаний у вигляді двійкового слова довжини m , то повинна конуватись нерівність $2^m < n$.

Блок M розглядається як елемент кільця Z_n і як такий, що може підноситися до степеня e за модулем n:

$$E(M) = M^e \bmod n$$

В результаті отримаємо блок криптотексту C=E(M).

Дешифрування блоку крипотексту C полягає у піднесенні C до степеня d, тобто Відправник повідомлення зашифровує своє послання використовуючи загальнодоступні відкриті параметри e, n і відправляє по відкритих каналах зв'язку

Отримувач розшифровує отримане повідомлення на основі відомого тільки йому ключа d. Зловмисник, який перехопить всі повідомлення у відкритому каналі не зможе по цих даних знайти вихідний текст. Задача розшифровування еквівалентна задачі розкладу великого числа на прості співмножники, тобто задачі факторизації. На межі сучасних можливостей є факторизація чисел із 150 десятковими цифрами. Розклад на множники чисел, які мають 200 десяткових цифр, на думку експертів залишається справою майбутнього.

Розглянемо приклад. Для простоти використаємо маленькі числа (на практиці використовуються набагато більші).

1. Нехай майбутній отримувач шифрованого тексту вибере два прості числа p=7, q=11.
2. Визначимо n=7*11.
3. ***Обчислимо φ(n)=(p-1)(q-1)=6*10=60.***
4. ***Виберемо довільне взаємно-просте із φ(n) = 60 число d, наприклад d=13.***
5. ***Знаходимо таке число e, яке задовільняє умову e*13 mod 60=1 ітеративним способом***

1)1*60+1=61
2)2*60+1=121
3) 3*60+1=181
.....
8) 8*60+1=481 481/13=37

Отже *e=37.*

Майбутній отримувач інформації публікує в загальнодоступному місці тільки відкриті параметри обміну : e=37, n=77. Використовуючи отриману пару ключів зашифруємо повідомлення "так". Числовий вигляд повідомлення 22 00 14.

$$E(22) = 22^{37} \bmod 77$$

При реалізації методу RSA на ЕОМ виникає єдина проблема, яка полягає в тому, що при піднесенні числа до великого степеня не можна використовувати стандартні функції мов програмування, а потрібно написати власну підпрограму .

Надійність RSA на пряму залежить від складності розкладу великих чисел на множники. Другим важливим параметром криптосистеми є швидкість шифрування.

Таблиця генерації 512 – бітних ключів.

Таблиця 1.

Процесор	Швидкість генерації відкритих ключів	Швидкість генерації закритих ключів
20 MHz 80386	065	55
166 MHz Pentium	30	25
500 MHz Pntium II	250	220

Довжина ключа.

Розмір ключа в алгоритмі RSA пов'язаний з розміром модуля n. Два числа p і q, добутком яких є модуль, повинні мати приблизно однакову довжину, оскільки в цьому випадку знайти співмножники складніше, ніж у випадку коли довжина чисел значно розрізняється. Наприклад, якщо передбачається використовувати 768 – бітовий модуль, то кожне число повинне мати довжину приблизно 384 біти.

Оптимальний розмір модуля визначається вимогами безпеки: модуль більшого розміру забезпечує високий рівень безпеки, але зменшує швидкість роботи алгоритму RSA. Довжина модуля вибирається в першу чергу на основі важливості даних і на основі можливих загроз.

В початковій версії RSA довжина ключа становила 500 бітів.

В кінці1995 року лише один раз практично вдалося реалізувати розкриття шифру RSA для 500 – значного ключа. Для цього з допомогою Internet було задіяно 1600 комп'ютерів добровольців на протязі п'яти місяців нерерервної роботи.

В 1999 році 512 бітовий ключ був розкритий за сім місяців і це означає, що 512 – бітові ключі вже не забезпечують достатню безпеку за винятком дуже короткострокових задач безпеки.

В даний час лабораторія RSA рекомендує для звичайних задач ключі розміром 1024 біти, а для особливо важливих задач – 2048 бітів. Менш цінна інформація може бути надійно зашифрована ключем 768 – бітової довжини, оскільки такий ключ все ще недосяжний для всіх відомих алгоритмів злому. Для оцінки рівнів безпеки різних розмірів ключів можна використовувати модель пропоновну Lenstra I Verheul.

Звичайно ключ індивідуального користувача має певний термін існування, який закінчується через деякий час, наприклад , через рік. Це дає можливість регулярно змінювати ключі і забезпечувати необхідний рівень безпеки. Після закінчення терміну життя ключа, користувач повинен створити новий ключ, заздалегідь упевнившись, що параметри криптосистеми залишилися колишніми, зокрема що система використовує ключі тієї ж довжини. Звичайно, заміна ключа не захищає від нападу на повідомлення, зашифровані колишнім ключем, але для цього розмір ключа повинен підбератися згідно актуальності даних. Можливість заміни ключів дозволяє підтримувати криптографічну систему у відповідності з поточними рекомендаціями про розміри ключів, які регулярно публікує Лабораторія RSA.

Розміри ключів в криптосистемі RSA (а також і в інших криптосистемах з відкритим ключем) набагато більші розмірів ключів системи блокового шифрування

типу DES, але надійність ключа RSA незрівнянна з надійністю ключа аналогічної довжини іншої системи шифрування.

Практичне використання алгоритму RSA .

На практиці криптосистема RSA часто використовується разом з криптографічною системою секретного ключа типу DES для зашифровування повідомлення ключем RSA за допомогою цифрового конверта. Припустимо, що відправник посилає зашифроване повідомлення. Спочатку це повідомлення шифрується по алгоритму DES, використовуючи випадково вибраний ключ DES і потім шифрує ключ DES відкритим ключем RSA. Зашифроване повідомлення і ключ DES разом формують цифровий коверт RSA і відсилають. Отримавши цифровий конверт, сторона В розшифровує ключ DES за допомогоюсвого закритого ключа , а потім використовує ключ DES, щоб розшифрувати саме повідомлення.

Криптосистема RSA використовується в самих різних продуктах, на різних платформах і в багатьох галузях. В даний час криптосистема вбудовується в багато комерційних продуктів, число яких постійно збільшується. Алгоритм RSA використовується в банківських комп'ютерних системах для роботи з віддаленими клієнтами по обслуговуванню кредитних карточок. Також його використовують операційні системи фірм Microsoft, Apple, Novel. В апаратному виконанні RSA алгоритм застосовується в захищених телефонах, на мережній платі Ethernet, на смарт-картах, широко використовується в криптографічному устаткуванні THALES (Racal). Алгоритм RSA входить до складу всіх основних протоколів для захищених комунікацій Internet, у тому числі S/MIME, SSL і S/WAN, а також використовується в багатьох установах, в більшості корпорацій, в державних ршлшлабораторіях і університетах. Більшість інших стандартів, що розробляються включають або сам алгоритм, або його підтримку і рекомендують криптосистему RSA для забезпечення секретності, встановлення аутентифікації(автентичності). На осінь 2003 року технології із застосуванням алгоритму RSA ліцензіювали більше ніж 900 компаній.

Для апаратної реалізації операції шифрування і дешифрування RSA розроблені спеціальні процесори. Ці процесори, реалізовані на надвелих інтегральних схемах, дозволяють виконувати операції RSA, пов'язані із зведенням великих чисел у колосально великий степінь за модулем N, за відносно короткий час.

Технологію шифрування RSA BSAFE використовують близько 500 мільйонів користувачів всього світу. Оскільки в більшості випадків при цьому використовується алгоритм RSA, то його можна вважати найпоширенішою криптосистемою загального ключа в світі і ця кількість має явну тенденцію до збільшення у міру зростання Internet.

Криптосистема RSA часто називається стандартом де факто. Незалежно від офіційних стандартів, існування такого стандарту надзвичайно важливе для розвитку електронної комерції і взагалі економіки. Це єдина система відкритого ключа, яка допускає обмін документами з електронно-цифровими підписами між користувачами різних держав, що використовують різне програмне забезпечення на різних платформах, така можливість насущно необхіна для розвитку електронної комерції і взагалі економіки.

Технологія RSA використовується для створення електронно цифрового підпису, який є засобом аутентифікації електронних повідомлень. Це дає можливість усі найважливіші документо-потоки (овіційні листи, юридичні документи, чеки, контракти) перевести в електронно-цифровий вигляд.

Системи шифрування

Таблиця 2.

Вид шифрування	**Переваги**	**Недоліки**
Симетричні криптосистеми	Велика швидкість. Легко реалізуються апаратно.	Один ключ для шифрування та дешифрування . Важко розповсюджувати ключі. Не підтримують цифрові підписи
Асиметричні криптосистеми	Використовуються два різні ключі. Відносно легко розповсюджувати ключі. Забезпезпечує цілісність і неможливість відмови від авторства (через цифровий підпис)	Працює повільно. Потребує великих обчислювальних потужностей.

Програмна реалізація RSA приблизно в 100 разів повільніша за програмну реалізацію DES. З розвитком технології ці оцінки можуть трохи змінюватися. Мала швидкодія RSA не перекреслює цінність цього алгоритму.

Порівняльна характеристика витрат часу і коштів для “зламу ” ключів

Таблиця 3.

Вартість, у.од.	**Довжина ключа, бітах**				
	40	56	64	80	128
100 тис.	2 секунди	35 годин	1рік	700років	1019 років
1 млн.	0,2 с	3,5 години	37 днів	600 років	1018 років
1000 млн.	2 мілісек	2 хвилини	9 годин	70 років	1017 років

Використання асиметричних криптосистем не забезпечує ”абсолютного” захисту інформації. Однак вони :

- Гарантує мінімально необхідний час для “зламу ” ключів, від декількох місяців до декількох років, за цей час інформація , що передається стає неактуальною.
- Гарантують, що вартість зламу у кілька разів перевищує вартість самої інформації.

Таблиця простих чисел

Перша тисяча простих чисел.

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199 211 223 227 229 233 239 241 251 257 263 269 271 277 281 283 293 307 311 313 317 331 337 347 349 353 359 367 373 379 383 389 397 401 409 419 421 431 433 439 443 449 457 461 463 467 479 487 491 499 503 509 521 523 541 547 557 563 569 571 577 587 593 599 601 607 613 617 619 631 641 643 647 653 659 661 673 677 683 691 701 709 719 727 733 739 743 751 757 761 769 773 787 797 809 811 821 823 827 829 839 853 857 859 863 877 881 883 887 907 911 919 929 937 941 947 953 967 971 977 983 991 997 1009 1013 1019 1021 1031 1033 1039 1049 1051 1061 1063 1069 1087 1091 1093 1097 1103 1109 1117 1123 1129 1151 1153 1163 1171 1181 1187 1193 1201 1213 1217 1223 1229 1231 1237 1249 1259 1277 1279 1283 1289 1291 1297 1301 1303 1307 1319 1321 1327 1361 1367 1373 1381 1399 1409 1423 1427 1429 1433 1439 1447 1451 1453 1459 1471 1481 1483 1487 1489 1493 1499 1511 1523 1531 1543 1549 1553 1559 1567 1571 1579 1583 1597 1601 1607 1609 1613 1619 1621 1627 1637 1657 1663 1667 1669 1693 1697 1699 1709 1721 1723 1733 1741 1747 1753 1759 1777 1783 1787 1789 1801 1811 1823 1831 1847 1861 1867 1871 1873 1877 1879 1889 1901 1907 1913 1931 1933 1949 1951 1973 1979 1987 1993 1997 1999 2003 2011 2017 2027 2029 2039 2053 2063 2069 2081 2083 2087 2089 2099 2111 2113 2129 2131 2137 2141 2143 2153 2161 2179 2203 2207 2213 2221 2237 2239 2243 2251 2267 2269 2273 2281 2287 2293 2297 2309 2311 2333 2339 2341 2347 2351 2357 2371 2377 2381 2383 2389 2393 2399 2411 2417 2423 2437 2441 2447 2459 2467 2473 2477 2503 2521 2531 2539 2543 2549 2551 2557 2579 2591 2593 2609 2617 2621 2633 2647 2657 2659 2663 2671 2677 2683 2687 2689 2693 2699 2707 2711 2713 2719 2729 2731 2741 2749 2753 2767 2777 2789 2791 2797 2801 2803 2819 2833 2837 2843 2851 2857 2861 2879 2887 2897 2903 2909 2917 2927 2939 2953 2957 2963 2969 2971 2999 3001 3011 3019 3023 3037 3041 3049 3061 3067 3079 3083 3089 3109 3119 3121 3137 3163 3167 3169 3181 3187 3191 3203 3209 3217 3221 3229 3251 3253 3257 3259 3271 3299 3301 3307 3313 3319 3323 3329 3331 3343 3347 3359 3361 3371 3373 3389 3391 3407 3413 3433 3449 3457 3461 3463 3467 3469 3491 3499 3511 3517 3527 3529 3533 3539 3541 3547 3557 3559 3571 3581 3583 3593 3607 3613 3617 3623 3631 3637 3643 3659 3671 3673 3677 3691 3697 3701 3709 3719 3727 3733 3739 3761 3767 3769 3779 3793 3797 3803 3821 3823 3833 3847 3851 3853 3863 3877 3881 3889 3907 3911 3917 3919 3923 3929 3931 3943 3947 3967 3989 4001 4003 4007 4013 4019 4021 4027 4049 4051 4057 4073 4079 4091 4093 4099 4111 4127 4129 4133 4139 4153 4157 4159 4177 4201 4211 4217 4219 4229 4231 4241 4243 4253 4259 4261 4271 4273 4283 4289 4297 4327 4337 4339 4349 4357 4363 4373 4391 4397 4409 4421 4423 4441 4447 4451 4457 4463 4481 4483 4493 4507 4513 4517 4519 4523 4547 4549 4561 4567 4583 4591 4597 4603 4621 4637 4639 4643 4649 4651 4657 4663 4673 4679 4691 4703 4721 4723 4729 4733 4751 4759 4783 4787 4789 4793 4799 4801 4813 4817 4831 4861 4871 4877 4889 4903 4909 4919 4931 4933 4937 4943 4951 4957 4967 4969 4973 4987 4993 4999 5003 5009 5011 5021 5023 5039 5051 5059 5077 5081 5087 5099 5101 5107 5113 5119 5147 5153 5167 5171 5179 5189 5197 5209 5227 5231 5233 5237 5261 5273 5279 5281 5297 5303 5309 5323 5333 5347 5351 5381 5387 5393 5399 5407 5413 5417 5419 5431 5437 5441 5443 5449 5471 5477 5479 5483 5501 5503 5507 5519 5521 5527 5531 5557 5563 5569 5573 5581 5591 5623 5639 5641 5647 5651 5653 5657 5659 5669 5683 5689 5693 5701 5711 5717 5737 5741 5743 5749 5779 5783 5791 5801 5807 5813 5821

5827 5839 5843 5849 5851 5857 5861 5867 5869 5879 5881 5897 5903 5923 5927 5939 5953 5981 5987 6007
6011 6029 6037 6043 6047 6053 6067 6073 6079 6089 6091 6101 6113 6121 6131 6133 6143 6151 6163 6173
6197 6199 6203 6211 6217 6221 6229 6247 6257 6263 6269 6271 6277 6287 6299 6301 6311 6317 6323 6329
6337 6343 6353 6359 6361 6367 6373 6379 6389 6397 6421 6427 6449 6451 6469 6473 6481 6491 6521 6529
6547 6551 6553 6563 6569 6571 6577 6581 6599 6607 6619 6637 6653 6659 6661 6673 6679 6689 6691 6701
6703 6709 6719 6733 6737 6761 6763 6779 6781 6791 6793 6803 6823 6827 6829 6833 6841 6857 6863 6869
6871 6883 6899 6907 6911 6917 6947 6949 6959 6961 6967 6971 6977 6983 6991 6997 7001 7013 7019 7027
7039 7043 7057 7069 7079 7103 7109 7121 7127 7129 7151 7159 7177 7187 7193 7207 7211 7213 7219 7229
7237 7243 7247 7253 7283 7297 7307 7309 7321 7331 7333 7349 7351 7369 7393 7411 7417 7433 7451 7457
7459 7477 7481 7487 7489 7499 7507 7517 7523 7529 7537 7541 7547 7549 7559 7561 7573 7577 7583 7589
7591 7603 7607 7621 7639 7643 7649 7669 7673 7681 7687 7691 7699 7703 7717 7723 7727 7741 7753 7757
7759 7789 7793 7817 7823 7829 7841 7853 7867 7873 7877 7879 7883 7901 7907 7919

Прості числа - особливі представники числового простору, що поділяються без залишку лише на себе самих і одиничку. По числовій осі вони розподілені нерівномірно і закон, якому підкоряється цей розподіл - якщо, звичайно, він взагалі існує - дотепер математикам невідомий. Перевірка на простоту начебто б нескладна, але вона збільшується з ростом величини самого числа, що перевіряється, і для уже відомих математикам простих чисел давно вийшла за межі фізичних можливостей людини: виконати перевірку простоти числа довжиною в тисячі і мільйони цифр можна лише за допомогою комп'ютерів, та й їм вимагаються на це місяці і роки завзятої роботи. Ця складність з успіхом використовується, зокрема, у **комерційній криптографії**.

Незважаючи на те, що установити загальну залежність розподілу простих чисел наука поки не змогла, є кілька приватних випадків, приблизно (з великою часткою імовірності) їх визначальних. Саме такою часткою случаємо і є залежність Мерсенна. Саму ідею дві тисячі років тому підказав Евклід, а багато пізніше, у 17-м столітті, чітко сформулював французький чернець Марен Мерсенн. Суть її зводиться до припущення, що число, описуване формулою 2^P-1, де **P** – просте число, також буде простим. Правило це виконується не завжди, але все-таки дозволяє заощадити час на пошуки гігантських простих чисел (саме пошуку чисел Мерсенна присвячений проект GIMPS). Усього до дійсного моменту чисел Мерсенна було відоме тільки 39. І легко зрозуміти той захват, з яким було зустрінуте повідомлення керівників GIMPS про відкриття чергового представника цієї послідовності. Число, простоту якого підтвердив комп'ютер, стало 40-м по рахунку з відомих чисел Мерсенна і може бути записане в такий спосіб: $\mathbf{2^{20996011}-1}$.

Звичайно, незважаючи на порівняльну "простоту", пошук чисел Мерсенна вимагає фантастичних обчислювальних витрат. Проект GIMPS - самий великий приклад організації робіт такого роду: у ньому беруть участь понад 60 тисяч чоловік, а програма-клієнт, що перебирає варіанти, працює на 210 тисячах машин по усьому світі. Інтенсивність обчислень настільки висока, що починають виявлятися дрібні дефекти комп'ютерної техніки і, відповідно до офіційної статистики проекту, близько 2% його первинних результатів виявляються помилковими.. Попереднє число Мерсенна було знайдено два роки тому також учасником GIMPS.

4.5 Закони про захист інформації.

Вперше проблема інформаційної безпеки внесена США в 1947 році при прийнятті Закону "Про національну безпеку" США. На сьогодні у США в усі підрозділи військ введені спеціалісти по інформації та комунікаціям, тобто спеціалісти по інформаційним війнам та технологіям.

Інформаційна безпека розглядається як глобальна проблема захисту інформації, захисту інформаційного простору та інформаційного суверенітету, а також як проблема інформаційного забезпечення прийняття урядових рішень. Практичне вирішення проблем інформаційної безпеки, притягнення до відповідальності за порушення або загрозу інформаційній безпеці у кожній державі здійснюється у порядку, передбаченому нормами міжнародного права, відповідними міждержавними договорами а також внутрішнім законодавством. Інформаційна безпека регулюється визначеними нормами міжнародного права, які зафіксовані у документах ООН і ЮНЕСКО, у документах європейських міжнародних організацій, а також у нормативних актах окремих держав.

Так існує міжнародна норма стосовно перекручення інформації, інформації, що включає заклики до повалення державного ладу в іншій країні. В міжнародних документах зафіксований захист інтелектуальної та комерційної інформації.

Кожна більш-менш розвинена країна має закони про захист інформації в різних галузях. Так:

1. Франція має закон "Про інформації, інформаційні файли та права людини" (1978 рік),
2. Німеччина – Закон "Про захист інформації" (1990 рік),
3. Австрія, Бельгія, Данія, Ірландія – Закон "Про захист інформації",
4. Фінляндія, Ісландія – Закон "Про захист інформації про особу"
5. Люксембург – Закон "Про використання інформації в процесі роботи з комп'ютером".

4.6 Інформаційні загрози.

☒ **Інформаційна загроза - це сукупність факторів, які створюють небезпеку для конституційних прав і свобод особистості, державної таємниці, зберігання цінної для суспільства інформації, від несанкціонованого доступу і розповсюдження.**

З точки зору інформаційної безпеки загрози поділяються на зовнішні і внутрішні. До зовнішніх відносять такі заходи і засоби здійснення інформаційних операцій, наслідком яких є політичний, економічний вплив на інші держави, що здійснюється на основі новітніх інформаційних технологій.

Інформаційна безпека в різних сферах має свою **специфику:**

політична – стосується інформаційно-аналітичної діяльності дипломатичних представників і зовнішньо-економічних відомств;

економічна – захист інформації у банківських системах та мережах зв‘язку, конфіденційної інформації від несанкціонованого доступу.

Об‘єктами захисту інформації є документи, програми ЕОМ, ноу-хау, бази данних, тексти та інші матеріальні носії інформації, захист яких передбачений

державними нормативними актами, внутрішньовідомчими постановами, розпорядженнями та спеціальними документами.
Найбільш важливі види інформації, яких стосується ІБ є ***стратегічна*** інформація, ***соціально-економічна*** інформація, ***воєнна, наукова.*** Надання інформації на державному рівні повинно включати проблему ІБ. Кожна країна включає питання ро ІБ в компетенцію Національної безпеки.

Інформаційні загрози та їх різновиди.

Розглядаються ***зовнішні*** і ***внутрішні*** загрози ІБ, а також заходи і засоби протистояння і боротьба проти несанкціонованого доступу до інформації.

Зовнішні загрози:
- інформаційному простору;
- інформаційному суверенітету;
- внутрішній стабільності;
- діяльності державного або недержавного органів і фірм.

Внутрішні загрози:
- національній безпеці;
- для впливу на свідомість суспільства;
- доступу до інформаційних ресурсів країни.

Типи міжнародних інформаційних операцій і основні засоби їх здійснення.

На сьогодні у світі розроблені спеціальні міжнародні інформаційні операції, які називаються ***інформаційними війнами*****,** які здійснюються за допомогою спеціальних установ, дипломатичних представників у країнах перебування; спеціальних технологій, що включають в себе новітні досягнення у галузі інформації і комунікацій.

Приклади (інформаційних операцій)**:**
“Буря в пустелі”, “Грім в пустелі” в районі Перської затоки;
“Відродження надії “у Сомалі;
“Спільні зусилля” у Боснії та Герцоговині;
“Автономія Албанії”;
“Шторм на Гаваях”;

☒ **Інформаційна операція –** це інформаційна підготовка суспільства до проведення певних дій: військового, економічного чи політичного втручання.

Ідея “***інформаційної парасольки”*** зараз замінює ідею ядерної парасольки і вважається одним із стратегічних напрямків впливу США на нейтральні держави, а також на держави певного блоку.

До **інформаційної експансії** можна віднести поширення сфери впливу ТНК у певному регіоні з метою конкуренції, завоювання інформаційного ринку і одержання прибутків від видів інформаційної діяльності.

Інформаційна війна.

Інформаційні війни здійснюються для забезпечення політичних, економічних інтересів політичних партій, урядів, політичних рухів для реалізації влади і реалізації національних інтересів на території іншої держави або в окремих регіонах. Інформаційна війна має також іншу назву – "інформаційна операція" і застосовується з метою пропаганди ідей масового впливу на громадську думку, а

також для вивчення реакції міжнародного співтовариства на ті чи інші прогнозовані рішення.

Інформаційна війна має два аспекти (два види забезпечення):

- технологічний аспект;
- ідеологічний аспект.

З точки зору технічного забезпечення мова йде про те, що у визначений час приводяться в дію програмні віруси, логічні бомби, закладені у пам'яті інформаційних комп'ютерних мереж. Вони здатні зруйнувати і знищити програми управління, бази даних, а також зруйнувати і знищити рахунки у зарубіжних банках, заглушити теле- і радіомовлення у певному регіоні, припинити діяльність армійських пунктів зв'язку і управління.

До ідеологічного аспекту відносять ідеологічну обробку населення, яка призводить до нестабільності політичної ситуації у країні, до дезорієнтації населення і спричинення паніки. Спеціалісти свідчать, що навіть незначне проникнення інформації з метою забезпечення операції веде до значних матеріальних наслідків і до забезпечення інтересів більш розвинутої країни. Крім того, масований вплив інформації на громадську думку приводить до спокійного ставлення до агресивних кроків і навіть воєнних дій.

Через засоби комунікації при здійснення інформаційних операцій впливають на міжрегіональні протиріччя, розпалюють міжетнічну і міжнаціональну підозрілість, створюють комплекс меншовартості.

Усі міжнародні інформаційні операції поєднують в собі кілька різних засобів їх здійснення: психотехнології, інформаційна інфраструктура, комп'ютерне забезпечення, вплив на міжнародну думку. До важливих компонентів інформаційної війни належить інформаційне забезпечення держави у міжнародних інформаційних потоках.

Інформаційна інтервенція – це тенденційна інформація, коли розповсюджується через системи зв'язку суб'єктивні факти та суб'єктивна інформації, які впливають на суспільну думку і прийняття рішень в іншій державі. В рамках інформаційної інтервенції здійснюють маніпулювання інформацією для досягнення мети.

Інформаційний тиск – один із видів інформаційних загроз, який застосовується для розв'язання міжнародних проблем, для попередження міжнародних конфліктів або для того, аби змусити державу, що порушує міжнародні правила, увійти в міжнародне правове поле.

Інформаційний тиск застосовується як прийом превентивної дипломатії. Інформаційно-аналітичне забезпечення зовнішньої політики є складовою зовнішньополітичних комунікацій, які є одним з елементів сучасного міжнародного співробітництва. Інформаційно-аналітичне забезпечення відображає реагування міжнародного співтовариства на політичні процеси у системі, на зміну економічної ситуації, забезпечує адекватний вплив на небажані зміни. Від інформаційного забезпечення залежить якість урядових рішень, передбачення і випередження подій, прийняття спільних рішень із глобальних проблем міжнародного товариства. Недостовірність інформації, неточність, можуть породжувати серйозні проблеми в міжнародних відносинах.

Слід зазначити, що система інформаційної безпеки будь-якої країни є невід'ємною частиною загальної національної системи безпеки. Іншими словами, в системі національної безпеки інформаційна безпека виступає як її підсистема. Інформаційну безпеку слід розуміти як сукупність засобів забезпечення інформаційного суверенітету України, захист інформаційної сфери від зовнішніх і внутрішніх інформаційних загроз. Ця безпека має включати і ефективну протидію сукупності інформаційних загроз, які небезпечні не лише для суто інформаційної сфери.

Потреба забезпечення інформаційної безпеки обумовлюється:

- необхідністю забезпечення національної безпеки України в цілому;
- існуванням таких загроз інформаційній сфері країни, які можуть завдавати значної шкоди загальним національним інтересам;
- врахуванням того, що за допомогою інформації можна впливати на зміну свідомості і поведінки великих мас людей.

Завдання інформаційної безпеки — це створення системи протидії інформаційним загрозам, та захист власного інформаційного простору, інформаційної інфраструктури, інформаціиних ресурсів держави. Також до інформаційної безпеки відносять і забезпечення права юридичних та фізичних осіб, всього населення своєчасно отримувати повну інформацію. Важлива роль тут належить ЗМІ України.

До інформаційної безпеки варто віднести й реалізацію конституційного права громадян на свободу думки і слова, на вільне вираження своїх поглядів і переконань (стаття 34 Конституції України), Концепції національної безпеки України (Схвалена Верховною Радою України 16 січня 1997 року)

Концепція національної безпеки України має забезпечити:

- єдність принципів формування і проведення державної політики національної безпеки;
- поєднання підходів до формування відповідної законодавчої бази, підготовки доктрин, стратегій, концепцій, державних і відомчих програм у різних сферах національної безпеки.

Національна безпека України, як стан захищеності життєво важливих інтересів особи, суспільства та держави від внутрішніх і зовнішніх нагроз є необхідною умовою збереження та примноження духовних і матеріальних цінностей.

Головними об'єктами національної безпеки є:

громадянин — його права і свободи;
суспільство — його духовні та матеріальні цінності;
держава — її конституційний лад, суверенітет, територіальна цілісність і недоторканність кордонів.

Основними принципами забезпечення національної беазпеки є:

- пріоритет прав людини; верховенство права; пріоритет, договірних (мирних) засобів у вирішенні конфліктів;
- адекватність заходів захисту національних інтересів реальним та потенційним загрозам;
- демократичний цивільний контроль за воєнною сферою, а також іншими структурами в системі забезпечення національної безпеки;

- додержання балансу інтересів особи, суспільства та держави, їхня взаємна відповідальність;
- чітке розмежування повноважень органів державної влади.

Національна безпека України досягається шляхом проведення виваженої державної політики відповідно до прийнятих доктрин, стратегії, концепцій і програм у таких сферах, як політична, економічна, соціальна, воєнна, екологічна, науково-технологічна, інформаційна тощо. Конкретні засоби і шляхи забезпечення національної безпеки України обумовлюються пріоритетністю національних інтересів, необхідністю своєчасного вжиття заходів, адекватних характеру і масштабам загроз цим інтересам, і грунтуються на засадах правової демократичної держави.

Загрози національній безпеці України.

Основні можливі загрози національній безпеці України в найбільш важливих сферах життєдіяльності:
- у політичній сфері,
- в економічній сфері:
- неефективність системи державного регулювання економічних відносин;
- наявність структурних диспропорцій, монополізму виробників, перешкод становленню ринкових відносин;
- невирішеність проблеми ресурсної, фінансової та технологічної залежності національної -економіки від інших країн;
- економічна ізоляція України від світової економічної системи;
- неконтрольовапий підплив за межі України інтелектуальних, матеріальних і фінансових ресурсів;
- криміналізація суспільства, діяльність "тіньових" сгруктур,
- у соціальній сфері,
- у воєнній сфері,
- у науково-технологічній сфері.

Основні напрямки державної політики національної безпеки України.

Державна політика національної безпеки визначається виходячи з пріоритетності національних інтересів та загроз національній безпеці України і здійснюється шляхом реалізації відповідних доктрин, стратегій, концепцій і програм у різних сферах національної безпеки відповідно до чинного законодавства.

В економічній сфері:
- недопущення незаконного використання бюджетних коштів і державних ресурсів, їхнього перетікання у “тіньову” економіку;
- контроль за експортно-імпортною діяльністю, спрямованою на підтримку важливих для Украйни пріорітетів та захист вітчизняного виробника;
- боротьба з протиправною економічною діяльністю, протидія неконтрольованому відпливу національних, матеріальних, фінансових, інтелектуальних та інших ресурсів.

Для формування збалансованої державної політики та ефективного проведення комплексу узгоджених заходів щодо захисту національних інтересів по всіх сферах створюється система забезпечення національної безпеки України.

Основні функції системи забезпечення національної безпеки в усіх сферах її діяльності такі:
- створення і підтримка в готовності сил та засобів забезпечення національної безпеки;
- управління діяльністю системи забезпечення національної безпеки;
- здійснення планової та оперативної діяльності щодо забезпечення національної безпеки;
- участь у міжнародних системах безпеки;

5 Інформаціна політика ООН.

Міжнародна інформація і обмін інформацією відтворюють зовнішньополітичні інтереси окремих держав, блоків держав та цілих систем, тобто відтворюють реальні відносини між державами. В той же час у сфері міжнародної інформації відбувається гостра конкуренція держав.

Усі світові інформаційні потоки контролюють усього 5 ТНК. Це такі, як Associated Press, Reuters, France Press, RCA, Ashet, RTL. Вони отримують 90% прибутків від розповсюдження інформації в міжнародних каналах. Монополія ТНК привела до незбалансованого обігу інформації з одного боку і з іншого – до надмірних прибутків самих корпорацій. Якщо подивитися на акціонерів цих ТНК, то видно, що 65% акцій RCA належать підприємствам Америки, що замаються виробництвом лазерної зброї; 55% акцій Ashet належать французьким корпораціям, що займаються виробництвом приладів нічного бачення. Аналогічна ситуація і в інших компаніях, тобто понад 50% прибутків цих корпорацій відходить до військово-промислового комплексу. Отже фактично, міжнародну інформаційну систему контролює ВПК.

В 1970 році країни соцтабору, країни неприєднання (139 країн) та країни Азії, Африки та Латинської Америки виступили проти нерівномірного розподілу інформації у світі і зажадали збалансованого представлення в світових інформаційних потоках і рівномірного розподілу прибутків (прибутки всіх корпорацій здійснюються в основному за рахунок розміщення реклами товарів та послуг та інших пропозицій у світових інформаційних мережах. Так, наприклад, по 70 каналам RTL (якщо взяти їх сукупність) реклама передається по всьому світу цілодобово).

В 1980 році ЮНЕСКО прийняла декларацію про міжнародний обмін інформацією, яка називалася "Новий міжнародний інформаційний порядок". Вона забезпечувала рівність держав у міжнародних інформаційних потоках і розподіл прибутків від рівноправно представленої інформації держав. В 1981 році США і Великобританія відмовились підписувати цю декларацію і на знак протесту вийшли з ЮНЕСКО. Треба сказати, що США і досі не є членом ЮНЕСКО. Великобританія з приходом до влади в минулому році нового уряду поновила своє членство, але до сих пір не виконує в повному обсязі своїх фінансових зобов'язань. Таким чином США, держава, яка має найбільші внески в ООН і отримує найбільша прибутки від діяльності інформаційних ТНК не підтримала цю програму і її реалізація була зірвана (були реалізовані лише окремі пункти).

Два роки тому Федеріко Майор (директор ЮНЕСКО) знову повернувся до так званої "теорії рівного потоку інформації" і надав право ТНК здійснювати свою

діяльність незалежно від рівноправної участі країн у світових інформаційних потоках. Діяльність департаменту економічної і соціальної інфрмації ООН у сучасній системі міжнародних відносин посідає місце лідера із накопичення та розповсюдження інформації. За 50 років свого існування (від 1945 року) ООН створила цілий ряд міжнародних документів, які регламентують інформаційну діяльність міжнародного співтовариства і сприяють розповсюдженні інформації в усіх країнах-членах ООН і серед світової громадськості.

Основні напрямки інформаційної стратегії ООН включають:

1. ***Накопичення інформації про усі види діяльності міжнародного співтовариства.***

Інформаційна база ООН складає понад 1000 інформаційних баз даних, не враховуючи серійних публікацій (близько 2000 на рік) а також серійних публікацій із спеціальних із спеціальних галузей міжнародного співробітництва. Інформація ООН складається із баз даних в інформаційних мережах, із друкованих видань, радіо- і телепродукції, аудіо-, відеоматеріалів та ілюстрацій.

2. ***Висвітлення різними засобами діяльності міжнародної організації, просування принципів ООН, зафіксованих у статуті цієї організації, ведення інформаційних кампаній через інформаційні представництва і місії в усіх регіонах світу***.

На сьогодні ООН має 106 інформаційних місій, які займаються розповсюдженням інформації по країнах-членах ООН, а також у країнах, що не входять до неї.

Інформаційні служби ООН висвітлюють проблеми, які зафіксовані у Статті 1 статуту ООН про діяльність міжнародного співтовариства. До таких проблем відносять:

- вплив інформації на міжнародне співтовариство;
- використання новітніх комунікаційних технологій для прогресу цивілізації;
- збереження культурної ідентичності і самобутності в умовах інформаційної експансії;
- забезпечення прав людини у галузі інформації і сприяння гуманітарному розвитку людства.

3. ***Пропаганда ідеалів цієї організації серед народів світу.*** Це завдання покладено на Департамент публічної інформації, а також на комітет з інформації ООН та спеціалізовані установи ООН: UNESCO, UNIDO, UNICEF і ПРООН.

4. ***Регулювання міжнародних інформаційних потоків з метою усунення диспропорцій в інформаційному обміні.***

Цей напрямок був проголошений декларацією "Новий міжнародний інформаційний порядок", однак, отримавши серйозну протидію з боку США та Великобританії, був призупинений на світовому рівні, однак продовжується на регіональному (через регіональні представництва та інформаційні місії, Департамент економічної та соціальної інформації та політичного аналізу, Економічну та Соціальну Раду – ЕКОСОС).

5. ***Сприяння "вільному потоку інформації" та усуненню перешкод вільній конкуренції на світовому ринку інформаційних послуг***.

Даний напрямок був проголошений на заміну Новому інформаційному порядку на вимогу США та Великобританії. Він передбачає зняття обмежень діяльності ТНК

на міжнародному рівні (це однак не передбачає відміну таких обмежень на національному та регіональному ринку, що зараз широко використовується в Європі), забезпечення вільної конкуренції на ринку інформації.

Діяльність Департаменту економічної і соціальної інформації та політичного аналізу (ДЕСІПА).

Цей департамент було засновано 1993 року з метою розповсюдження економічної та соціальної інформації як в самій організації, так і в її представництвах, які сприяють гуманітарному розвитку країн третього світу (Азії, Африки, Латинської Америки).

ДЕСІПА пропонує інформацію, що стосується вирішення глобальних економічних проблем та конкретних економічних програм для підтримки країн, що потребують економічного розвитку.

Приблизний бюджет цього підрозділу: 50 млн. доларів від ООН і 35 млн. доларів позабюджетних надходжень.

Департамент публічної інформації.

Це спеціалізована установа ООН, яка безпосередньо займається розповсюдженням інформації про діяльність організації. Цей департамент має мандат ООН на забезпечення інформацією міжнародного співтовариства для розуміння цілей і принципів діяльності організації. Департамент публічної інформації має три функціональних підрозділи, такі як:

1) ***підрозділ мас-медіа*** – вироблення та розповсюдження інформації для країн-членів ООН про програмну діяльність організації а також розповсюдження інформації у міжнародних інформаційних потоках за допомогою мас-медіа.

2) ***бібліографічний підрозділ*** – контролює видавничі програми ООН, здійснює інформаційну підтримку представництв і місій ООН у різних регіонах світу і видає періодичні щорічники, такі як "Хроніка ООН", "Щорічник ООН" і "Бізнес, що розвивається". Ці видання фінансуються Всесвітнім банком та рядом регіональних банків

3) ***підрозділ забезпечення інформаційних послуг (інформаційний центр)*** – впроваджує інформаційну стратегію ООН по тематичним напрямках. Цей підрозділ видає два регулярних щорічники: "Розвиток Африки" та "Розвиток світу сьогодні".

6. Інформаційні технології та інформаційне суспільство в Україні.

Інформаційне суспільство.

Протягом останнього двадцятиріччя в світі йде процес формування інформаційного суспільства, а тому все більше розвиваються обчислювальні та інформаційні мережі – унікальний симбіоз комп’ютерів і комунікацій. З кожним днем активніше розвиваються сучасні інформаційні технології і в Україні. Людська цивілізація на межі тисячоліть вступила в еру інформації. Світовою системою комп’ютерних комунікацій щодня користуються сотні мільйонів людей. Інформація

стає вирішальним чинником у багатьох галузях народного господарства. Саме вона є продуктом наукової та дослідницької діяльності, необхідним компонентом у ході наукових досліджень. Зростає потреба у засобах структурування, накопичення, зберігання, пошуку та передачі інформації – задоволення саме цих потреб і є метою створення та розвитку інформаційних мереж. У прагненні до сумісного використання ресурсів обчислювальних та інформаційних центрів (бібліотек, програм, криміналістичних обліків) виникає необхідність її включення до світових інформаційних мереж. В цих умовах стає все важче, а інколи просто неможливо, отримувати необхідну інформацію, якщо не володієш потужними можливостями, що надаються інформаційними мережами світу. Щоб прямувати в ногу з часом, необхідно включатись у глобальні комп'ютерні мережі та уміло користуватися всіма їх привілеями. Особливо органам державної влади та управління, громадським організаціям і неурядовим установам, кожній людині нашої держави, жителям планети Земля.

Саме з цих причин 4 лютого 1998 р. Верховна Рада України прийняла низку законів стосовно інформатизації всіх сфер суспільної діяльності в Україні. Так, зокрема, в **Концепції Національної програми інформатизації** у розділі VI цього закону визначаються основні напрями інформатизації. Серед них пріоритетним є інформатизація правоохоронної діяльності.

В Указі Президента України «Про заходи щодо розвитку національної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» від 31 липня 2000 року (№ 9282/000) зазначається, що з метою розвитку національної складової глобальної інформаційної мережі Інтернет, забезпечення широкого доступу громадян до цієї мережі, ефективного використання її можливостей для розвитку вітчизняної науки, освіти, культури, підприємницької діяльності, зміцнення міжнародних зв'язків, належного інформаційного забезпечення здійснення органами державної влади та органами місцевого самоврядування своїх повноважень, повнішого задоволення потреб міжнародного співтовариства в об'єктивній, комплексній інформації щодо різних сфер суспільного життя в Україні, а також вирішення інших завдань, визначених в Посланні Президента України до Верховної Ради України **«Україна: поступ у XXI сторіччя. Стратегія економічного та соціального розвитку на 2000–2004 роки»**

Ці документи визначають пріоритетні напрямки стратегії і тактики побудови інформаційного суспільства в Україні, а також розвиток інтернет-технологій і створення надійного фундаменту інформаційної безпеки людини, суспільства і держави. Таким чином, інформація сьогодні стає основним об'єктом і продуктом нашого суспільства, а інформація і комп'ютеризація відповідно основними інструментами її опрацьовування. При цьому, під інформацією слід розуміти сукупність (позначених термінами) взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, що спрямовані на створення умов для задоволення інформаційних потреб громадян та суспільства на основі створення, розвитку і використання інформаційних систем, мереж, ресурсів інформаційних технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки. Для України широкомасштабний вступ до глобальної інформаційної цивілізації наклався з

проголошенням 24 серпня 1991 року державної незалежності. Після визначення державного суверенітету, поряд з іншими галузями законодавства в Україні створюється національна публічно-правова інституція: законодавство та підзаконні нормативні акти в сфері політики щодо державного регулювання суспільних інформаційних відносин, в тому числі таких, що пов'язані з інформатизацією, комп'ютеризацією і автоматизацією.

Сьогодні національне (державне і публічне) право має значний масив нормативних актів (законів та підзаконних правових документів – наказів, інструкцій, положень, статутів), які прямо чи опосередковано регулюють суспільні інформаційні відносини в Україні. Проведені узагальнення і підрахунки кількісного складу нормативних актів, які підготовлені органами державної влади, є чинними і регулюють інформаційні відносини та характеризуються наступними показниками: в Україні сьогодні діє **259** Законів України, **290** Постанов Верховної Ради (нормативного змісту), **370** Указів Президента України, **89** Розпоряджень Президента України, **1159** Постанов Кабінету Міністрів України, **206** Розпоряджень Кабінету Міністрів України, більш ніж 1**100** нормативних актів міністерств, комітетів і окремих відомств.

Інформаційне право.

Першочергове питання, яке постало сьогодні перед українським суспільством та його складовою – правознавством, – це визначення статусу суспільних інформаційних відносин та шляхів їх публічно-правового регулювання з метою уникнення, зменшення, запобігання та подолання юридичними методами негативних проявів інформаційного суспільства та стимулювання бажаних для людини, держави та суспільства правил поведінки його суб'єктів – учасників інформаційних відносин. Будь-яка правова інституція, щоб претендувати на автономність існування, вимагає формулювання її поняття, визначення змісту, розробки теоретичних і методологічних основ. В **об'єктивному змісті** інформаційне право – це регулювання сукупності суспільних відносин щодо інформації, які знаходять вираз у нормах врегульованих на публічно-правовому та приватно-правовому рівні. В **суб'єктивному змісті** інформаційне право – це законодавчо врегульована множина прав і обов'язків конкретних учасників суспільних відносин щодо інформації, як об'єкта суспільних відносин.

Основною юридичною формою виразу норм інформаційних відносин є законодавство, яке регулює ці відносини в інформаційній сфері. Під категорією «інформаційне законодавство України», було б доцільно розуміти множинну сукупність нормативно-правових актів, прийнятих Верховною Радою України у формі законів та постанов нормативного змісту, які регулюють суспільні відносини щодо інформації. Входження України в інформаційне суспільство потребує розробки науково-теоретичних засад концепції формування і розвитку інформаційного законодавства. Використання положень теорії гіперсистем з метою дослідження і систематизації українського права, дозволяє зробити висновок, що сучасне українське інформаційне законодавство існує сьогодні як міжгалузевий, міждисциплінарний комплексний інститут в загальній системі національного законодавства. У теоретиків права, які дотримуються традиційної доктрини поділу права на галузі (за принципом: норми права – інститути права – галузь права чи

норми права – інститути права – підгалузі права – галузь права) виникає запитання: що являє собою категорія «**гіперсистема**», яке їй місце може бути надано в системі теорії і методології права згідно з загальною теорією права? Доцільно тут зазначити, що категорія «**гіперсистема права**» відносно нове поняття в юридичній науці. Традиційна для нашої країни теорія права її раніше не знала. Вона зародилася на основі здобутків і досліджень у галузі кібернетики та інформатики і використання їх результатів для вивчення права, як соціальної системи. У відповідності з **теорією гіперсистем**, існування сучасного права аналізується і розглядається з позиції великих, складних, ієрархічних багатопорядкових системи підсистем, що формуються з галузевих інститутів права. Ця категорія н вводиться в теорію права України юридичної концепції існування і формування правових субінституцій – автономних міжгалузевих комплексних інститутів права, щодо яких галузеві інститути виступають у ролі агрегуючих підсистем.

Законодавча практика Верховної Ради України свідчить, що сьогодні приймаються закони, які є системоутворюючими публічно-правового регулювання комплексного змісту в окремих суспільних відносинах на основі доктрини поділу права на провідну галузь – конституційне право і окремі галузі – адміністративне, цивільне, трудове, кримінальне. Вперше ця концепція була апробована при розробці і формуванні теорії інформаційного права України. Проведений аналіз правового регулювання інформаційних відносин в Україні та узагальнений досвід міжнародної практики дозволяє визначити низку доктринальних, основоположних, методологічних, принципових положень у площині інформаційного права:

- основний об’єкт правового регулювання – суспільні інформаційні відносини;
- основний предмет суспільних відносин інформація (відомості, дані, знання, таємниця тощо);
- метод правового регулювання – це системне комплексне застосування методів конституційного, цивільного, адміністративного, трудового та кримінального права (що визначає міжгалузевий характер публічно-правового регулювання) та застосування методів приватно-правового регулювання (на рівні правочинів, угод, звичаїв, традицій, норм суспільної моралі, професійної, ділової етики тощо).

Отже, за правовою природою походження інформаційне право слід розглядати, як міжгалузевий комплексний інститут національного права України, яке має приватно-правову і публічно-правову природу, тобто норми права розробляються і формуються як на публічному (державному), так і приватному рівнях суспільних відносин. Через предмет регульованих суспільних відносин (інформацію) інформаційне право має зв`язок з іншими міжгалузевими інститутами права: банківським, страховим, конкурентним, екологічним, місцевого самоврядування, авторським, інтелектуальної власності, винахідницьким, рекламним правом тощо. Інформаційне право утворює у поєднанні з ними велику, складну, агреговану гіперсистему права третього порядку. Тобто у відповідності з положеннями теорії гіперсистем права інформаційне право базується на засадах правових систем другого порядку, якими є п’ять галузей права: провідна галузь – конституційне, окремі галузі – адміністративне, цивільне, трудове, кримінальне. У своїй єдності вони утворюють єдину систему першого порядку – право України (українське право). Домінуючою методологією розробки і формування інформаційного права України повинні стати доктринальні положення сучасного вітчизняного конституційного права (основа –

Конституція України) та узагальнені дані найкращих здобутків міжнародного права щодо визнання пріоритету верховенства прав людини у сфері суспільних інформаційних відносин. При такому підході доктринальною визнається також багатооб'єктність юридичних норм щодо застосування законодавства з метою правової кваліфікації суспільних інформаційних відносин, природної єдності всіх умовно визначених галузей права.

Визначення поняття і статусу інформаційного права, як міжгалузевого комплексного інституту права, породжує питання щодо визначення статусу і співвідношення його з іншими інститутами права, предметом яких є суспільні відносини щодо інформації (твір, винахід, корисна модель, масова інформація, архіви, бібліотеки тощо). Концептуально пропонується також визначитися, які інші інститути права агрегуються з інформаційним правом. Окремі з них на певних умовах мають статус міжгалузевих субінститутів. До таких можна віднести: банківське, бюджетне, страхове, податкове, інвестиційне право складають систему фінансового права; авторське, винахідницьке, раціоналізаторське право та інші, що складають систему права інтелектуальної власності; право щодо засобів масової інформації: преса, радіо, телебачення, Інтернет тощо. Важливим аспектом розробки теорії інформаційного права є проблематика його підсистем – субінститутів на наш погляд. Серед основних субінститутів сфер правового регулювання інформаційних правовідносин можна зазначити такі:

- визначення та правове закріплення провідних напрямів і методів державної політики у сфері вибору мов спілкування, формування провідної технології, комунікації в державі тощо;
- правове регулювання суспільних відносин у сфері засобів масової інформації, визначення їх подібностей та відмінностей, систематизація їх через агрегацію (преса, видавнича справа, радіо, телебачення, комп'ютерні мас-медіа інтернет-технології тощо);
- забезпечення умов для розвитку механізму правового захисту всіх форм власності на інформацію та інформаційні ресурси (право власності на інформацію);
- організація та управління створенням і розвитком державних інформаційних систем і мереж, забезпечення їх сумісності та взаємодії їх з іншими в єдиному інформаційному просторі України;
- правове регулювання щодо створення реальних умов для якісного та ефективного забезпечення необхідною інформацією громадян, органів державної влади, органів місцевого самоврядування, державних і приватних організацій, громадських об'єднань на основі використання державних інформаційних ресурсів, сучасних інформаційних технологій;
- забезпечення співвідношення інтересів суб'єктів суспільних інформаційних відносин у сфері національної безпеки, склаІнформатизація і комп'ютеризація викликали необхідність перегляду сутності категорії «документ». У практиці вже давно існує поняття «електронний документ», «електронні довідки», «електронні звіти», «електронні гроші» тощо. У зв'язку з цим перевірка достовірності документа, встановлення юридичного факту та його документального фіксування, повинно покладатися (бути функцією) на окремі органи, які уповноважені видавати відповідні документи чи перевіряти їх достовірність. Важливою складовою проблематики інформаційного права є формування в ньому юридичної деліктології

(вчення про правопорушення) у сфері інформаційних відносин на принципі гармонізації норм з галузевими деліктологіями: конституційного, адміністративного, цивільного, трудового та кримінального права.

Ентропія (невизначеність) законодавця в цьому напрямку знайшла відображення у Законах України «Про інформацію», «Про захист інформації в автоматизованих системах» новому чинному Кримінальному Кодексі України (2001 р.) – ст. 361–363 та деяких інших, де визначено диспозиції правопорушень, але чітко не визначено, а в деяких зовсім відсутня відповідальність за них в адміністративно-правовому, цивільно-правовому та кримінально-правовому аспектах. У проблематиці інформаційного права особлива увага повинна звертатися на виявлення та дослідження недоліків, як вітчизняних, так і зарубіжних правовідносин, їх регулювання для уникнення помилок у правотворчій та правозастосовній діяльності в Україні. Мета досліджень – запобігання негативним для суспільства наслідків інформатизації і комп'ютеризації, попередження поширенню правопорушень, проступків, правопорушення, злочині, що вчиняються з використанням сучасних інформаційних технологій. Особливе місце в інформаційній деліктології повинно відводитися дослідженню кримінологічних, адміністративно-правових, цивільно-правових, трудових, кримінально-правових та криміналістичних аспектів такого негативного для суспільства явища, як комп'ютерна злочинність. Проблемою також є визначення економічних та моральних збитків від порушення інформаційних правовідносин.

Один з важливих аспектів інформаційного права є проблематика державного правотворення. Правотворча діяльність найкраще повинна здійснюватися на таких основоположних принципах наукового забезпечення:

- формування концепції інформаційного законодавства України;
- системний та комплексний підходи у вирішенні проблем правотворчості;
- ґрунтовне фундаментальне та прикладне теоретичне обґрунтування новацій (понять, категорій тощо);
- узагальнення і використання досвіду зарубіжних країн;
- залучення широкого кола вітчизняних фахівців до розробки проектів законодавчих та підзаконних актів в галузі інформаційного права України.

Формування системи інформаційного законодавства висунуло проблему гармонізації його на міждержавному рівні, з урахуванням засад міжнародного права (його провідних складових: публічного і приватного). Сьогодні можна констатувати, що у міжнародному праві активно формується його інституція – міжнародне інформаційне право світової інформаційної цивілізації. За оцінками експертів на міжнародному рівні існує близько **50 міждержавних угод** (глобальних, універсальних, регіональних та субрегіональних), у яких визначені правові основи регулювання міжнародних інформаційних відносин.

Глобальна комп'ютеризація через Інтернет породила необхідність пошуку засобів і методів гармонізації національних правових систем у сфері міжнародних інформаційних відносин, співвідношення цих систем на рівні колізійного та матеріального міжнародного права. У багатьох регіонах світу (Європі, Америці, Азії) формуються міжнародні стандарти правових норм на рівні типових законів, багатосторонніх конвенцій, угод тощо.

Ряд теоретиків та практиків у сфері правового регулювання суспільних інформаційних відносин пропонують механічно імплементувати (ввести) ці норми в національне інформаційне законодавство України без глибокого вивчення і порівняльного аналізу чинного законодавства. Звісно, що при розробці і формуванні національного законодавства недопустиме необґрунтоване копіювання зарубіжного досвіду. Гармонізацію можна проводити також шляхом внесення нового змісту в існуючі форми правових норм. До речі, саме така практика існує у цивілізованих країнах, які раніше від нас стали на шлях формування правового інформаційного суспільства, у складі глобальної інформаційної цивілізації.

Міжнародний досвід свідчить, що у сфері суспільно інформаційних відносин, при їх законодавчій легалізації в першу чергу враховуються такі загальнолюдські принципи, як повага та гуманне ставлення до людини, її честі, гідності, репутації; презумпція невинності громадянина, приватної особи на засадах співвідношення потреб та інтересів окремих людей, їх корпорацій (об'єднань), націй, держав та світового співтовариства.

Якісно новий підхід щодо правового регулювання в сфері суспільних інформаційних відносин, у тому числі на міжнародному рівні запропонований вітчизняною наукою. В її складі сьогодні набирають сили нові наукові дисципліни – ***правова кібернетика*** та ***правова інформатика***, ***правова нейробіоніка*** і ***правова нейрокібернетика***, ***адміністративна інформатика та цивільна інформатика, трудова інформатика і криміналістична інформатика*** застосування принципів, підходів і методів кібернетики та інформатики до вирішення проблем права, зокрема і правотворення, правозастосування.

Виходячи з положень **правової інформатики** слід зазначити, що правотворення повинно базуватися на основі методології системного і комплексного підходів, зокрема теорії формування комплексних гіперсистем права, агрегації і інтеграції галузевих інститутів права.

Звичайно, що національне інформаційне законодавство повинно стати на шлях систематизації через кодифікацію – створення системоутворюючого його Кодексу. Цей Кодекс повинен буде розвивати визначені в Конституції України положення інформаційних відносин, в тому числі щодо інформаційної безпеки людини, суспільства, нації, держави. Він повинен об'єднати, гармонізувати і розвивати норми і принципи суспільних відносин, що визначені в законодавстві України; враховувати ратифіковані Україною нормативні акти (угоди, конвенції) міжнародного права; легалізувати позитивні звичаї в сфері інформаційних відносин та норми суспільної моралі, загальнолюдські цінності, визначені Організацією Об'єднаних Націй в її Статуті, Декларації прав людини та інших загальноприйнятих міждержавних нормативних актах, які сьогодні виступають в ролі стандартів, за якими визначається цивілізованість не тільки окремої країни, але й світового співтовариства в цілому.

Майбутній Кодекс України про інформацію має на меті об'єднати в одному законодавчому акті регулювання провідних суспільних відносин, об'єктом яких є інформація, незалежно від форми, способу, засобу чи технології її прояву у суспільних відносинах. Це дозволяє, у разі виникнення необхідності публічно

правового урегулювання нових суспільних відносин щодо інформації агрегувати юридичні формулювання їх у Кодекс через внесення в нього на рівні законів змін і доповнень без породження нових системоутворюючих законодавчих актів.

Методологічною базою правотворення такого Кодексу повинна стати юридична доктрина щодо умовного поділу права України на галузі за наступною принциповою моделлю: основа конституційне право; його положення знаходять паралельний розвиток (у відповідності з методами правового регулювання і захисту прав) в адміністративному, цивільному, трудовому, кримінальному праві та інших підсистемах національного права України, в яких інформація виступає як опосередкований, (додатковий, факультативний) предмет регулювання суспільних відносин.
Розробка проекту Кодексу повинна проводитися методом агрегації: удосконалення окремих правових норм, чи створення нових міжгалузевих правових інститутів не повинно порушувати цілісність та призначення національного законодавства, а покращувати, удосконалювати його дієвість в цілому, створювати нову системну якість, яка не притаманна окремим його складовим.

Мета Кодексу визначається у відповідності з теорією системи цілей, правове регулювання суспільних відносин між їх суб'єктами щодо інформації у різних формах її об'єктивного вираження (творах, результатах інтелектуальної діяльності) незалежно від сфери (чи галузі) суспільних відносин, матеріальних носіїв інформації (паперових, електронних тощо) та технології фіксації (літери, знаки, образи, цифри тощо).
Провідними функціями Кодексу повинні бути:
- **регулятивна** – визначення прав, обов'язків та зобов'язань суб'єктів;
- **нормативна** – визначення норм, правил поведінки суб'єктів інформаційних відносин;
- **охоронна** – визначення гарантій та меж правомірної поведінки, за якими діяння утворюють правопорушення (делікти) та відповідальність за них у відповідності з нормами цивільного, адміністративного, трудового, кримінального права;
- **інтегративна** – системне поєднання комплексу визначених юридичних норм, які регулюють інформаційні відносини в Україні, тобто Кодекс повинен стати поєднуючою ланкою між провідними традиційними галузями права щодо застосування їх методів в сфері інформаційних відносин;
- **комунікативна** – зазначення в окремих статтях посилань на законодавчі акти, які є, або необхідність в яких може виникнути, системоутворюючими різних міжгалузевих інститутів права.
Серед провідних завдань Кодексу можна визначити:
- визначення консенсусу (згоди) в суспільних стосунках, узгодженості розуміння та застосування юридичних норм, правомірної поведінки учасників інформаційних відносин, відносин в інформаційній сфері;
- забезпечення інформаційного суверенітету, незалежності України у міжнародних стосунках;
- забезпечення інформаційної безпеки громадян, їх окремих спільнот, суспільства та держави, як складових національної безпеки України;

- визначення правомірної поведінки учасників інформаційних відносин в Україні;
- захист інформації від несанкціонованого доступу, правопорушень (знищення, модифікації, перекручення тощо).довою якої є інформаційна безпека, визначення загроз безпеці суспільним інформаційним відносинам, правове і технічне забезпечення регулювання захисту інформації, в тому числі в автоматизованих системах;
- забезпечення реалізації конституційних прав осіб (приватних немайнових) на режим доступу до персональних даних інформації про громадян та їх спільності (організації) за умов інформатизації державних органів управління;
- державно-правове сприяння формуванню ринку інформаційних ресурсів, послуг, інформаційних систем, технологій, з пріоритетами для вітчизняних виробників інформаційної продукції, засобів, технологій;
- державне стимулювання вдосконалення механізму залучення інвестицій, розробки і реалізації проектів національної програми інформатизації та локальних програм інформатизації (установ, підприємств, організацій, всіх форм власності, міністерств та відомств, регіонів тощо);
- забезпечення правового режиму формування і використання національних інформаційних ресурсів, збору, обробки, накопичення, зберігання, пошуку, поширення та надання споживачам інформації;
- правове регулювання щодо стимулювання створення і використання в Україні новітніх інформаційних технологій.

Важливим аспектом розвитку інформаційного права України є створення реальних правових бар'єрів для профілактики зловживань у сфері документообігу, зокрема, недопущення свавілля державними та недержавними структурами, посадовими особами щодо примушування надавати їм громадянами інформацію, яка існує в інших структурах. Саме тому, в інформаційному законодавстві України повинен утвердитися принцип презумпції невинності громадянина, а не існуючий, на жаль сьогодні порочний принцип недовіри тих чи інших документів, які були видані іншою інстанцією, на взірець («принеси довідку, тоді тобі дамо довідку»). В результаті цього громадяни змушені витрачати багато часу на подолання службових бар'єрів по різних інстанціях, з метою підтвердження правомірності виданих їм раніше документів.

Інформаційне законодавство.

Як констатацію факту, слід зазначити, що сучасне інформаційне законодавство України щодо доктрини його формування, має характер змішаної системи права: зберігши галузевий підхід традиційної континентальної системи права, воно стало на шлях публічно-правового нормотворення за доктриною загального права (англо-американської системи права) – коли окремі проблеми на законодавчому рівні, вирішуються у площині чинних законів за ситуаційним принципом.

Ситуаційний підхід до формування інформаційного законодавства України, з точки зору когнітивного (пізнавального) аспекту, спричинив коло проблем щодо правового регулювання інформаційних відносин. Наприклад:

- відсутність легальної чіткої ієрархічної єдності законів, що викликає суперечливе тлумачення при застосуванні правових норм у практиці.
- в зв'язку з тим, що різні закони та підзаконні акти, що регулюють суспільні відносини, об'єктом яких є інформація, приймались у різні часи розвитку, становлення, і удосконалення державності без узгодження понятійного апарату, тому вони мають ряд термінів, які недостатньо коректні, не викликають відповідної інформаційної рефлексії, або взагалі позбавлені чіткого визначення свого конкретного змісту. Що до інформаційних відносин, то тут доцільно зазначити такі поняття і терміни, як «інформація», «таємна інформація» і «таємниця», «документ» і «документована інформація», «майно», «власність», «володіння», «інтелектуальна власність», «автоматизована система», «суб'єкт суспільних відносин» та «учасники суспільних відносин», «система інформаційних відносин» тощо. Всі ці терміни законодавець використовує для регулювання відносин у різних сферах і галузях права.
- термінологічні неточності, різне тлумачення однакових за назвою та формою понять і категорій призводить до їх неоднозначного розуміння і застосування на практиці.
- велика кількість законів та підзаконних нормативних актів у сфері інформаційних відносин ускладнює їх пошук, аналіз та узгодження для практичного застосування.

Є розбіжність щодо розуміння структури і складу системи законодавства в сфері інформаційних відносин та підходи до їх формування. Нерідко в окремих законах у систему законодавства включають норми, що виражені в підзаконних нормативних актах. Це створює в практиці правозастосування деякими учасниками суспільних відносин колізію норм, ігнорування конституційних положень, норм закону на користь норм підзаконного акта окремих міністерств, комітетів, відомств і організацій.

Потребує удосконалення чинне законодавство України в сфері інформаційних відносин. Проведені дослідження і узагальнення досвіду експертної, слідчої і судової практики дають можливість внести такі рекомендації:

А) пропозиції щодо вдосконалення інформаційного цивільного законодавства.

Треба зазначити, що комп'ютерні програми доцільно віднести до об'єктів інтелектуальної власності. Але на сьогоднішній день згідно Закону України «Про охорону прав на винаходи і корисні моделі» не мають правової охорони …програми для обчислювальних машин. Хоча це не вірно і як по суті, так і по змісту тому що: програма для обчислювальної машини – це результат розумової, творчої діяльності людини. Адже написання програми це не тільки викладення в певній послідовності своїх знань, умінь і навиків у формі алгоритму, а й створення такої програми, яка б забезпечила швидке, правильне, об'єктивне вирішення завдання, питання, функціонування певного механізму, надання інформації тощо; автор програми моделює послідовність виконання поставлених завдань, підбирає колір, зовнішній вигляд, атрибутику програми та ін. У процесі написання програми людина творить новий інтелектуальний продукт;

програми – це також винаходи; вони відповідають всім вимогам винаходу, тобто це технічне рішення (і не тільки; також можливе математичне) в будь-якій галузі суспільнокорисної діяльності, відповідає умовам патентоспроможності (є оригінальним і новим), має винахідницький рівень і придатне для використання в різних сферах людського життя (освіті, науці, практиці).

Комп'ютерна інформація може бути об'єктом такого правового інституту, як нерозкрита (конфіденційна) інформація. Хоча в нашому чинному законодавстві ще не має такого правового інституту. На даний період розвитку України це вже вимога часу. Як відомо, «хто володіє інформацією, той володіє світом»).

Життя, слідча і судова практики вимагають передбачити в цивільному законодавстві відповідальність за порушення порядку ознайомлення з інформацією, правилами користування нею, правом власності тощо.

Б) пропозиції щодо вдосконалення адміністративного законодавства (законодавства в галузі адміністративних правопорушень):

У чинному законодавстві необхідно встановити адміністративну відповідальність за правопорушення у сфері комп'ютерної обробки інформації:

- дрібне комп'ютерне хуліганство – вчинення дій, що заважають нормальному функціонуванню АС, без порушення цілісності інформації, її пошкодження, спотворення, тобто запис на носій інформації завідомо зайвої інформації, зміна назви файлів та ін.;
- несанкціоноване ознайомлення з особистою, не державною інформацією – шляхом втручання в інформаційну базу даних, яка не визнається комерційною або державною таємницею;
- використання запатентованої програми без реєстрації, дозволу або оплати за користування даною програмою;
- користування комп'ютерною мережею через суб'єкта, який надає такі послуги (сервер), без дозволу або оплати за дану послугу;
- порушення правил користування комп'ютерною мережею, що призвело до малозначного - пошкодження фізичного носія інформації (приведення до непридатності байтів (кластерів) диску;

незаконне виготовлення з готових (запатентованих) програм нових програм;

- доповнити статтю 1643 КУпАП «Недобросовісна конкуренція» ч. 4 «Зміна, перекручення, пошкодження інформації (бухгалтерської звітності, бухгалтерії та ін.) іншого підприємця з метою зниження рівня його авторитету ділової репутації, конкурентоспроможності, та підвищення своєї особистої монополії на ринку товарів;
- тиражування фізичних носії комп'ютерної інформації (cd-rom; dvd-rom).

В) пропозиції щодо вдосконалення кримінального законодавства:

- ввести відповідальність за:
- крадіжку інформації (фізичного носія);
- інформаційне шахрайство;
- втручання в роботу АС з метою ознайомлення з інформацією або її копіюванням;
- комп'ютерний грабіж (перехват інформації при її обміні);
- інформаційне вимагання;
- комп'ютерне хуліганство;

- несанкціоноване протиправне ознайомлення або копіювання інформації без втручання в роботу АС (зняття зображення з екрану).

Нові правові акти, які приймають сьогодні в сфері суспільно інформаційних відносин, нерідко неузгоджені концептуально з раніше вже чинними, що призводить до різного тлумачення, а також використання їх на практиці.

Аналіз чинного законодавства України в сфері суспільних відносин щодо інформації (у методологічному аспекті), свідчить, що воно сьогодні ніби будинок, який будується громадою без заздалегідь визначеного єдиного плану. При цьому кожний архітектор, будівельник чи майстер (ініціатор і автор законопроекту чи підзаконного нормативного акта) проводить цю роботу на свій розсуд, не узгоджуючи її з іншими. Без чіткого визначення технології і методики підготовки законопроекту взагалі, і, в галузі інформаційних відносин зокрема, створюється хаос.

Зазначені та інші проблеми сформували практичну потребу визначення методології систематизації і кодифікації права, розробки її концепції, доктрини, техніки і методики підготовки законопроектів, що відповідали вимогам теорії і потребам практики.

Відповідно, до основи систематизації норм інформаційного права повинні покладатися теоретичні положення, напрацьовані юридичною наукою і перевірені практикою основоположні принципи: поєднання традицій і новацій правотворення; інкорпорування норми чинного інформаційного законодавства України в нову систему через агрегацію інститутів права; формування міжгалузевих інститутів права на основі зв'язків з галузевими інститутами тощо.

В зв'язку з цим в українському правознавстві, теорії права виникла потреба узагальнити емпіричний матеріал і на цій основі розробити методологічні засади нового напрямку досліджень, предметом яких є процеси виникнення, зміни і припинення суспільних відносин щодо інформації (відомостей, даних, знань тощо).

Можна констатувати, що існуюча сьогодні сукупність правових норм у сфері інформації і комп'ютеризації досягли за кількістю такої критичної маси, що зумовлює можливість і реальну необхідність виділення, систематизації і кодифікації їх в окрему правову інституцію. Це викликало потребу наукового її дослідження, узагальнення наявного історичного досвіду, визначення тенденцій, проблем та шляхів їх практичного вирішення.

Необхідно підкреслити, що проблематика комп'ютерної злочинності, особливо її складової – організованої комп'ютерної злочинності сьогодні вже має чітко визначений, як національний, так і міжнародний, транснаціональний характер.

Факт економічної відмінності серед держав, який стає очевидний, повинен спонукати країни, які мають нижчий рівень економічного становища, докласти всіх зусиль, щоб наздогнати розвинені країни не тільки щодо технічного розвитку інфраструктури, засобів телекомунікації, але й у формах, методах, способах

боротьби з комп'ютерною злочинністю. Це на сьогодні є актуальною парадигмою і для України.

Введення мережі електронних розрахунків веде до трансформації техніки виконання корисливих злочинів у сфері банківської та пов'язаної з нею кредитною, фінансово-економічною діяльністю, хоча в її основі є ті ж механізми документообігу, що базуються на системі звичайного бухгалтерського обліку. Тому діюча технологія вчинення злочинів автоматично переноситься в умови електронних розрахунків. У той же час технології вчинення комп'ютерних злочинів у сфері економіки мають свої особливості.
Проблемою щодо нашої країни є відсутність кримінально-процесуальних та криміналістичних напрацювань методології, методики та тактики боротьби з комп'ютерною злочинністю, зокрема, у сфері економіки.

Комп'ютерна злочинність все більше й більше, загрожує як економічним основам держави, так і світовій економічній системі, всій безпеці людства.
На погляд зарубіжних спеціалістів, незаконне використання комп'ютерів дає більші прибутки для злочинців з меншими ризиками, ніж скоєння традиційних злочинів шляхом викрадення грошей в банках, тому число таких злочинів з кожним роком буде зростати.

Деякі керівники господарських структур пов'язують надійність електронних (комп'ютерних) систем переважно із засобами їх технічного захисту, у тому числі введенням (системи паролів) для входження не тільки в саму комп'ютерну мережу, а й до різних рівнів інформації у автоматизованій системі, в залежності від допуску її користувачів. Коло працівників, які за технологією виконання господарських операцій мають доступ до широкого діапазону цієї інформації, досить значне. Тому система захисту електронних мереж, що базується тільки на кодуванні входження до різних видів інформації, є малоефективною. Практика потребує пошуку принципово нових підходів для розробки відносно надійної системи захисту комп'ютерних мереж. У зв'язку з цим зусилля в багатьох країнах концентруються на подоланні змін – невизначеності широкого кола громадськості щодо здобутків і загроз інформаційної безпеки.

Не принижуючи ролі організації інженерно-технічних засобів захисту інформації в автоматизованих (комп'ютерних) системах, треба зазначити, що зусилля ряду країн спрямовуються саме на розвиток організаційно-управлінських та організаційно-правових засобів забезпечення інформаційної безпеки в умовах інформатизації.

В Україні, на зразок інших країн, існує потреба формування і розвитку спеціальних підрозділів по боротьбі з комп'ютерною злочинністю: у МВС – у структурі підрозділів по боротьбі з організованою злочинністю, та у підрозділів державної служби по боротьбі з економічною злочинністю; у Державній податковій адміністрації, в складі податкової міліції; у Службі безпеки України, в підрозділах контррозвідки.

Щодо стратегії боротьби з комп'ютерною злочинністю, все більше фахівців у галузі боротьби з нею в нашій країні, як і дослідники в інших сферах боротьби зі злочинністю, стають прихильниками ідеї, вираженій у афоризмі: «Апелювати в позбавленні від злочинності до поліцейських засобів і пенітенційної (кримінально-правової) політики – це все одно, що за допомогою парасольки намагатися зупинити дощ».

Важлива роль у міжнародній практиці боротьби з комп'ютерною злочинністю відводиться удосконаленню законодавчого регулювання суспільних інформаційних відносин, як на національному, так і на міжнародному рівні. Не залишилося поза цим процесом і Україна.
З часу проголошення 24 серпня 1991 року державної незалежності України створюється національна система законів та підзаконних нормативних актів щодо правового регулювання суспільних інформаційних відносин в умовах формування інформаційного суспільства, процесу інформатизації та комп'ютеризації.

Національне (державне, публічне) право України має значний масив нормативних (законів та підзаконних) актів, які прямо чи опосередковано регулюють інформаційні відносини в суспільстві. Це Закони України, Постанови Верховної Ради України (нормативного змісту), Укази Президента України, Розпорядження Президента України, Постанови Кабінету Міністрів України, Розпорядження Кабінету Міністрів України, нормативні акти міністерств і відомств.

В той же час, для упорядкування та врегулювання цих відносин на державному рівні виникла потреба юридично визначитися в найважливіших правових нормах поведінки їх учасників, у тому числі запобігання та боротьбі з правопорушеннями в сфері суспільних інформаційних відносин.

Права на комп'ютерну програму.

Авторські права діляться на дві групи: особисті немайнові й майнові авторські права. Особисті немайнові права, як виходить з їхньої назви, пов'язані з особистістю автора, не можуть відчужуватися або передаватися за договором. Вони можуть належати тільки авторові. Особисті немайнові авторські права охороняються безстроково...

Автором програми визнається фізична особа, у результаті творчої діяльності якої ця програма створена. Якщо програма створена спільною творчою діяльністю двох і більше фізичних осіб, то незалежно від того, чи складається програма із частин, кожна з яких має самостійне значення, або є неподільно, кожна із цих осіб визнається автором такої програми. У випадку якщо частини програми мають самостійне значення, кожний з авторів має право авторства на створену ним частину.

Авторові програми належать наступні особисті **немайнові права**:
— право авторства — тобто право вважатися автором програми. Як би різкими не були повороти в долі автора, хто б не володів програмою — але автором програми

завжди буде вважатися той, чиєю працею вона створена — і це право в автора ніхто не відніме;
— право на ім'я — тобто право визначати форму зазначення імені автора в програмі: під своїм ім'ям, під умовним ім'ям (псевдонімом) або анонімно;
— право на недоторканність (цілісність) — тобто право на захист як самої програми, так й її назви від усякого роду перекручувань або інших зазіхань, здатних завдати шкоди честі й достоїнству автора. Це право, на відміну від прав на авторство й на ім'я, після смерті автора може передаватися в спадщину, щоб спадкоємці могли захищати честь і достоїнство автора.

Друга група авторських прав — **майнові.** Такі права, після створення програми приналежному її автору, можуть передаватися за договором, і в результаті цього власниками таких прав можуть ставати як приватні особи, так й організації. Загальний зміст майнових прав — це право використати програму або дозволяти її використання в будь-якій формі й будь-якому способі. Зокрема, автор (або власник виключних прав на програму) має право здійснювати або дозволяти:
— випуск програми у світ;
— відтворення програми (повне або часткове) у будь-якій формі, будь-якими способами;
— поширення програми. Це право в індустрії shareware порушується найчастіше, коли хтось починає поширювати чужі програми без дозволу правовласника;
— модифікацію програми для ЕОМ або бази даних, у тому числі переклад програми з однієї мови на іншу. Це право також порушується досить часто — наприклад, коли користувачі з неангломовних країн перекладають інтерфейс програми на свою рідну мову, змінивши DLL- або Exe-файли програми. Втім, автори ставляться до таких саморобних модифікацій своїх програм лояльно (якщо, звичайно, інших змін, наприклад злому захисту, немає) — адже це тільки підвищує популярність програми.

Допускаються й інші способи використання комп'ютерних програм, Закон не встановлює їхній точний перелік, завершуючи список словами «інше використання програми». Важливо те, що усі права на будь-яке використання програми належать авторові (або тому, кому ці права автором передані).

Серед користувачів поширене думка, що програму в некомерційних цілях можна використати безкоштовно, це нібито дозволяють статті Закону про авторське право й суміжні права. Це всього лише невдала спроба виправдати використання піратських копій програм «домашніми» користувачами. Дозволу безкоштовного використання програм у некомерційних цілях у законодавстві немає, тільки автор вправі вирішувати, на яких умовах можна користуватися його програмою.
Майнові права на програму, як уже згадувалося вище, можуть бути передані повністю або частково іншим фізичним або юридичним особам. Передача прав здійснюється за договором, що укладається в писемній формі. Цей договір обов'язково повинен визначати обсяг і способи використання програми, порядок виплати й розмір винагороди, термін дії договору. Крім того, майнові права на програму переходять й у спадщину.

Використання програми здійснюється також за письмовим договором із правовласником. Природно, при масовому поширенні програм фізично неможливо з кожним користувачем окремо укладати договір. У цьому випадку допускається застосування особливого порядку укладання договорів, наприклад шляхом викладу типових умов договору на переданих екземплярах програм.

Таким особливим порядком укладання договору на використання програми є **ліцензійна угода**.Ліцензійна угода, що прикладається до копії програми, є юридичним документом, що визначає умови, на яких власник прав на програму дозволяє її використання...
По суті справи, це двосторонній письмовий договір між правовласником і користувачем, договір, що має спрощений порядок укладання: під ним не ставляться підписи його учасників. Така ліцензійна угода вважається укладеною, якщо користувач установлює, копіює або здійснює доступ або іншим способом використовує програму. Якщо користувач не згодний з умовами ліцензійної угоди, то він зобов'язаний припинити використання програми й видалити її файли зі свого комп'ютера. Обсяг прав, надаваних ліцензійною угодою, називається ліцензією. При визначенні обсягу прав, переданих користувачеві, завжди існує ймовірність, що укладач ліцензійної угоди забув указати які-небудь права, які він передає або, навпаки, не передає користувачеві.
Також можлива ситуація, коли після закінчення деякого часу можуть з'явитися нові можливості використання програми, які обумовлені закономірним розвитком науки й техніки. У результаті цього може вийти так, що користувач, керуючись принципом «що не заборонено, те дозволено», буде використати програму способом, проти якого власник прав обов'язково заперечував би.

7. Енерго –інформаційна безпека людини при роботі з інформаційними технологіями.

7.1 Що таке ЕМП, його види і класифікація.

Навколишнє нас простір по суті своєї є електромагнітним океаном, пронизаним радіохвилями різної довжини(частоти), амплітуди(енергії) і модуляції(накладеної інформації). Природа цих хвиль складна і різноманітна. Розділимо їх на дві основні групи: природного і штучного походження. Саме перша група велика і не до кінця охоплена і вивчена. В природі протікає величезна кількість процесів, що супроводжуються викидами енергії електромагнітного характеру, у тому числі народженням радіохвиль. Це життєдіяльність далеких зірок і близького нам Сонця, вибухи сверхнових і народження нових галактик, випромінювання квазарів і реліктове космічне випромінювання, природа якого дотепер не ясна. Також на самій планеті Земля протікає маса процесів, що породжують різні радіохвилі. Це полярні сяйва у верхніх шарах іоносфери і грозові розряди…Все це приводить до того, що нас постійно пронизують радіохвилі самої різної природи. Ми постійно "купаємося" в цьому електромагнітному океані!

Але за останні 100 років ситуація почала кардинально змінюватися. Вагомий

внесок у наполнення цього океану стала вносити людина. Відкриття можливості штучної генерації радіохвиль (Генріх Герц, Німеччина) і передачі з їхньою допомогою інформації (Олександр Попов, Росія) на значні відстані привели до того, що парк технічних пристроїв, які дозволяють це реалізувати на практиці, став дуже швидко нарощуваться і модифікуватися. Люди стали все більше оточувати радіохвилі штучного походження, створені їм же самими! Їх енергетика в більшості випадків більш істотна, ніж у хвиль природного характеру. І цілком закономірно, що через якийсь час стали виникати питання електромагнітної безпеки, тобто впливу радіохвиль на організм людини і навколишнє середовище.

Потрібно відзначити, що пильна увага цій темі стало приділятися лише після відкриття безпосереднього впливу на живу природу радіоактивного випромінювання (випромінювання радіоактивних металів, таких як уран і плутоній). В зв'язку з чим і був зроблений висновок про можливий негативний вплив радіохвиль різних діапазонів частот(довжин) на навколишнє середовище.

На практиці при характеристиці електромагнітної обстановки використовують терміни "електричне поле", "магнітне поле", "електромагнітне поле". Коротко пояснимо, що це означає і який зв'язок існує між ними.

Електричне поле створюється зарядами. Наприклад, в усьому відомих шкільних досвідах по електризації ебоніту, є присутнім саме електричне поле. Магнітне поле створюється при русі електричних зарядів по провіднику.

Для характеристики величини електричного полючи використовується поняття напруженість електричного поля, позначення Е, одиниця виміру В/м (Вольт-на-метр). Величина магнітного поля характеризується напруженістю Н, одиниця А/м (Ампер-на-метр). При вимірі наднизьких і вкрай низьких частот також використовується поняття магнітна індукція В, одиниця Тл(Тесла), одна мільйонна частина Тл відповідає 1,25 А/м.

По визначенню, електромагнітне поле - це особлива форма матерії, за допомогою якої здійснюється вплив між електричними зарядженими частками. Фізичні причини існування електромагнітного поля зв'язані з тим, що електричне поле, що змінюється в часі, Е породжує магнітне поле Н, а якщо змінюється Н - вихрове електричне поле: обидві компоненти Е и Н, безупинно змінюючись, збуджують один одного. ЕМП нерухомих чи рівномірно рухаються заряджених часток нерозривно зв'язано з цими частками. При прискореному русі заряджених часток, ЕМП "відривається" від них і існує незалежно у формі електромагнітних хвиль, не зникаючи з усуненням джерела (наприклад, радіохвилі не зникають і при відсутності струму в їхній антені, що випромінює).

Електромагнітні хвилі характеризуються довжиною хвилі, позначення - λ (лямбда). Джерело, що генерує випромінювання, а по суті создающий електромагнітні коливання, характеризуються частотою, f.

Важлива особливість ЕМП - це розподіл його на так називану "ближню" і "далеку" зони.

У "ближній" зоні, чи зоні індукції, на відстані від джерела $r < l$ ЕМП можна вважати квазистатическим. Тут воно швидко спадає з відстанню, назад пропорційно квадрату чи кубу відстані. У "ближній" зоні випромінювання електромагнітна хвилі ще не сформована. Для характеристики ЕМП, виміри змінного електричного поля Е та змінного магнітного поля Н виконуються роздільно. Поле в зоні індукції

служить для формування складової полів, що біжать, (електромагнітної хвилі), відповідальних за випромінювання.
"Далека" зона - це зона електромагнітної хвилі, що сформувалася, починається з відстані $r > 3\lambda$. У "далекій" зоні інтенсивність поля спадає назад пропорційно відстані до джерела r .
У "далекій" зоні випромінювання є зв'язок між E та H: $E = 377H$,
де 377 - хвильовий опір вакууму, Ом..

Тому вимірється, як правило, тільки E. На частотах вище 300 Мгц вимірється щільність потоку електромагнітної енергії (ЩПЕЕ), чи вектор Пойтинга. Позначається як S, одиниця виміру Вт/м^2. ПЕЕ характеризує кількість енергії, переданою електромагнітною хвилею в одиницю часу через одиницю поверхні, перпендикулярної напрямку поширення хвилі.

Міжнародна класифікація електромагнітних хвиль по частотах:

Найменування частотного діапазону	Границі діапазону	Найменування хвильового діапазону	Границі діапазону
Крайні низькі, КНЧ	3 - 30 Гц	Декамегаметровые	100 - 10 Мм
Наднизькі, СНЧ	30 – 300 Гц	Мегаметровые	10 - 1 Мм
Інфранизькі, ІНЧ	0,3 - 3 кгц	Гектокилометровые	1000 - 100 км
Дуже низькі, ОНЧ	3 - 30 кгц	Мириаметровые	100 - 10 км
Низькі частоти, НЧ	30 - 300 кгц	Кілометрові	10 - 1 км
Середні, СЧ	0,3 - 3 МГц	Гектометровые	1 - 0,1 км
Високі частоти, ВЧ	3 - 30 МГц	Декаметрові	100 - 10 м
Дуже високі, ОВЧ	30 - 300 МГц	Метрові	10 - 1 м
Ультрависокі,УВЧ	0,3 - 3 ГГц	Дециметрові	1 - 0,1 м
Надвисокі, СВЧ	3 - 30 ГГц	Сантиметрові	10 - 1 див
Вкрай високі, КВЧ	30 - 300 ГГц	Міліметрові	10 - 1 мм
Гіпервисокі, ГВЧ	300 – 3000 ГГц	Децимиллиметрові	1 - 0,1 мм

7.2 Основні джерела ЕМП.

Серед основних джерел ЕМВ можна перелічити:

Електротранспорт (трамваї, тролейбуси, потяги,...)
Лінії електропередач (міського висвітлення, високовольтні,...)
Електропроводка (всередині будинків, телекомунікації,...)
Побутові електроприлади
Теле- і радіостанції (антени)
Супутниковий і стільниковий зв'язок (антени)
Радари
Персональні комп'ютери

7.2.1 Електротранспорт.

Транспорт на електричній тязі – електропоїзда (у тому числі потяги метрополітену), тролейбуси, трамваї і т.п. – є відносно могутнім джерелом магнітного поля в діапазоні частот від 0 до 1000 Гц. За даними (Stenzel et al.,1996), максимальні значення щільності потоку магнітної індукції в приміських

"електричках" досягають 75 мктл при середнім значенні 20 мктл. Середнє значення на транспорті з електроприводом постійного струму зафіксовано на рівні 29 мктл.

7.2.2 Лінії електропередач.

Працючі лінії електропередачі створюють у прилягаючому просторі електричне і магнітне поля промислової частоти. Відстань, на яку поширюються ці поля від проводів лінії досягає десятків метрів.

Дальність поширення електричного поля залежить від класу напруги ЛЕП (цифра, що позначає клас напруги коштує в назві ЛЕП - наприклад ЛЕП 220 кв), чим вище напруга - тим більше зона підвищеного рівня електричного поля, при цьому розміри зони не змінюються в перебігу часу роботи ЛЕП. Дальність поширення магнітного поля залежить від величини струму, що протікає, чи від навантаження лінії. Оскільки навантаження ЛЕП може неодноразово змінюватися як протягом доби, так із зміною сезонів року, розміри зони підвищеного рівня магнітного поля також зміняються.

Біологічна дія.

Електричні і магнітні поля є дуже сильними факторами впливу на стан всіх біологічних об'єктів, що попадають у зону їхнього впливу. Наприклад, у районі дії електричного поля ЛЕП у комах виявляються зміни в поведінці: так у бджіл фіксується підвищена агресивність, занепокоєння, зниження працездатності і продуктивності, схильність до втрати маток; у жуків, комарів, метеликів і інших літаючих комах спостерігається зміна поведінкових реакцій, у тому числі зміна напряму руху убік з меншим рівнем поля.

У рослин поширені аномалії розвитку - часто міняються форми і розміри квіток, листів, стебел, з'являються зайві пелюстки. Здорова людина страждає від відносно тривалого перебування в полі ЛЕП. Короткочасне опромінення (хвилини) здатно привести до негативною реакцією тільки в гіперчуттєвих людей та у хворих деякими видами алергії. Наприклад, добре відомі роботи англійських учених на початку 90-х років які показали, що в ряду аллергиків під дією поля ЛЕП розвивається реакція по типі епілептичної.

При тривалому перебуванні (місяці - роки) людей в електромагнітному полі ЛЕП можуть розвиватися захворювання переважно серцево-судинної і нервової систем організму людини. В останні роки в числі віддалених наслідків часто називаються онкологічні захворювання.

Санітарні норми.

Дослідження біологічної дії ЕМП ПЧ, виконані в СРСР у 60-70х роках, орієнтувалися в основному на дію електричної складової, оскільки експериментальним шляхом значимої біологічної дії магнітної складової при типових рівнях не було виявлено. У 70-х роках для населення по ЕП ПЧ були введені тверді нормативи і по дійсний час є одними із самих твердих у світі. Вони викладені в Санітарних нормах і правилах "Захист населення від впливу електричного поля, створюваного повітряними лініями електропередачі перемінного струму промислової частоти"№ 2971-84". Відповідно до цих норм проектуються і будуються всі об'єкти електропостачання.

Незважаючи на те, що магнітне поле в усьому світі зараз вважається найбільш небезпечним для здоров'я, гранично припустима величина магнітного поля не нормується. Причина - немає грошей для досліджень і розробки норм. Велика частина ЛЕП будувалася без обліку цієї небезпеки.
На підставі масових епідеміологічних обстежень населення, що проживає в умовах опромінення магнітними полями ЛЕП, як безпечний чи "нормальний" рівень для умов тривалого опромінення, що не приводить до онкологічних захворювань, незалежно один від одного шведськими й американськими фахівцями, рекомендована величина щільності потоку магнітної індукції **0,2 - 0,3 мктл**.

Принципи забезпечення безпеки населення.

Основний принцип захисту здоров'я населення від електромагнітного поля ЛЕП складається у встановленні санітарно-захисних зон для ліній електропередачі і зниженням напруженості електричного поля в житлових будинках і в місцях можливого тривалого перебування людей шляхом застосування захисних екранів.
Границі санітарно-захисних зон для ЛЕП який на діючих лініях визначаються за критерієм напруженості електричного поля - кв/м.

Границі санітарно-захисних зон для ЛЕП згідно СН № 2971-84.

Напруга ЛЕП	330 кв	500 кв	750 кв	1150 кв
Розмір санітарно-захисної (охоронної) зони	20 м	30 м	40 м	55 м

До розміщення ВЛ ультрависоких напруг (750 і 1150 кв) пред'являються додаткові вимоги за умовами впливу електричного поля на населення. Так, найближча відстань від осі проектованих ВЛ 750 і 1150 кв до границь населених пунктів повинне бути, як правило, не менш 250 і 300 м відповідно.
Як визначити клас напруги ЛЕП? Найкраще звернутися в місцеве енергетичне підприємство, але можна спробувати візуально, хоча не фахівцю це складно:
330 кв - 2 проводи, 500 кв - 3 проводи, 750 кв - 4 проводи.
Нижче 330 кв по одному проводі на фазу, визначити можна тільки приблизно по числу ізоляторів у гірлянді : 220 кв 10 -15 шт., 110 кв 6-8 шт., 35 кв 3-5 шт., 10 кв і нижче - 1 шт.

Припустимі рівні впливу електричного поля ЛЕП

ДР, кв/м	Умови опромінення
0,5	всередині житлових будинків
1,0	на території зони житлової забудови
5,0	в населеній місцевості поза зоною житлової забудови; (землі міст у межах міської зони в границях їх перспективного розвитку на 10 років, приміські і зелені зони, курорти, землі селищ міського типу в межах селищної риси і сільських населених пунктів у межах риси цих пунктів) а також на території городів і садів;
10,0	на ділянках перетинання повітряних ліній електропередачі з автомобільними дорогами 1 – IV категорій;
15,0	в ненаселеній місцевості (незабудовані місцевості, хоча б і часто відвідувані людьми, доступні для транспорту, і сільськогосподарські угіддя);

20,0	у важкодоступній місцевості (недоступної для транспорту і сільськогосподарських машин) і на ділянках, специально выгороженных для виключення доступу населення.

В межах санітарно-захисної зони ВЛ забороняється:
- розміщати житлові і суспільні будинки і спорудження;
- влаштовувати площадки для стоянки і зупинки усіх видів транспорту;
- розміщати підприємства по обслуговуванню автомобілів і склади нафти і нафтопродуктів;
- робити операції з пальним, виконувати ремонт машин і механізмів.

Території санітарно-захисних зон дозволяється використовувати як сільськогосподарські угіддя, однак рекомендується вирощувати на них культури, що не вимагають ручної праці.

В випадку, якщо на якихось ділянках напруженість електричного поля за межами санітарно-захисної зони виявиться вище гранично припустимої 0,5 кв/м усередині будинку і вище 1 кв/м на території зони житлової забудови (у місцях можливого перебування людей), повинні бути прийняті міри для зниження напруженості. Для цього на даху будинку з неметалічною покрівлею розміщається практично будь-яка металева сітка, заземлена не менш чим у двох точках. В будинках з металевим дахом досить заземлити покрівлю не менш чим у двох точках. На присадибних ділянках чи інших місцях перебування людей напруженість поля промислової частоти може бути знижена шляхом встановлення захисних екранів.

7.2.3 Електропроводка.

Найбільший внесок в електромагнітну обстановку житлових приміщень у діапазоні промислової частоти 50 Гц вносить електротехнічне устаткування будинку, а саме кабельні лінії, що підводять електрику до всіх квартир і інших споживачів системи життєзабезпечення будинку, а також розподільні щити і трансформатори. В приміщеннях, суміжних з цими джерелами, звичайно підвищений рівень магнітного поля промислової частоти. Рівень електричного поля промислової частоти при цьому звичайно не високий і не перевищує ДР для населення - 500 В/м.

В даний час результати досліджень не можуть чітко обґрунтувати граничні величини, інші обов'язкові обмеження для тривалого облучення населення низько-частотними магнітними полями малих рівнів.

Дослідники з університету Карнегі в Пітсбурзі (США) сформулювали підхід до проблеми магнітного поля, який вони назвали “розсудливе запобігання”. Вони вважають, що поки наше знання щодо зв'язку між здоров'ям і наслідком опромінення залишаються неповними, але існують сильні підозри щодо наслідків для здоров'я, необхідно починати кроки по забезпеченню безпеки.

Подібний підхід був використаний, наприклад, у початковій стадії робіт із проблеми біологічної дії іонізуючого випромінювання: підозра ризиків збитку для здоров'я, заснована на твердих наукових фактах, повинне саме по собі скласти достатні підстави для виконання захисних заходів.

В даний час багато фахівців вважають гранично припустимої величину магнітної індукції рівної 0,2 - 0,3 мктл. При цьому вважається, що розвиток захворювань -

насамперед лейкемії - дуже ймовірно при тривалому опроміненні людини полями більш високих рівнів.

Рекомендації з захисту

Основна міра захисту - попереджувальна.

- необхідно виключити тривале перебування, (регулярно по кілька годин у день), у місцях підвищеного рівня магнітного полючи промислової частоти;
- ліжко для нічного відпочинку максимально видаляти від джерел тривалого опромінення, відстань до розподільних шаф, силових електрокабелів повинне бути 2,5 – 3 метри;
- якщо в чи приміщенні в суміжному є якісь невідомі кабелі, розподільні шафи, трансформаторні підстанції – видалення повинне бути максимально можливим, оптимально – проміряти рівень електромагнітних полів до того, як жити в такім приміщенні;
- при необхідності встановлення підлоги з електропідігріванням, вибирати системи зі зниженим рівнем магнітного поля.

7.2.4 Побутова електротехніка.

Всі побутові прилади, що працюють з використанням електричного струму, є джерелами електромагнітних полів.

Найбільш потужніми варто визнати Свч-печі, холодильники із системою “без інею”, кухонні витяжки, електроплити, телевізори. Реально створюване ЕМП у залежності від конкретної моделі і режиму роботи може сильно розрізнятися серед устаткування одного типу. Значення магнітного поля тісно зв'язані з потужністю приладу - чим вона вище, тим вище магнітне поле при його роботі. Значення електричного поля промислової частоти практично всіх електропобутових приладів не перевищують декількох десятків В/м на відстані 0,5 м, що значно менше ДР - 500 В/м.

Рівні магнітного поля промислової частоти побутових електроприладів на відстані 0,3 м.

Побутовий електроприлад	Від , мкТл	до, мкТл
Пилосос	0,2	2,2
Дриль	2,2	5,4
Праска	0,0	0,4
Міксер	0,5	2,2
Телевізор	0,0	2,0
Люмінесцентна лампа	0,5	2,5
Кавоварка	0,0	0,2
Пральна машина	0,0	0,3
Мікрохвильова піч	4,0	12
Електрична плита	0,4	4,5

Гранично допустимі рівні електромагнітного поля для продукції, що є джерелом ЕМП:

Джерело	Діапазон	Значення ПДУ		Примітка (умови виміру):
Індукційні печі:	20 - 22 кгц	500 В/м 4 А/м		відстань 0,3 м від корпуса
СВЧ печі :	2,45 ГГц	10 мкВт/см^2		відстань 0,50 м
Відеодисплейний термінал ПЭВМ :	5 Гц - 2 кгц	Епду = 25 В/м	Впду = 250 нТл	відстань0,5 м.
	2 - 400 кгц	Епду = 2,5 В/м	Впду = 25 нТл	
поверхневий електростатичний потенціал:		V = 500 В		відстань 0,1 м від екрана
Інша продукція:	50 Гц	Е = 500 В/м		відстань 0,5 м від корпуса виробу
	0,3 - 300 кгц	Е = 25 В/м		
	0,3 - 3 МГц	Е = 15 В/м		
	3 - 30 МГц	Е = 10 В/м		
	30 - 300 МГц	Е = 3 В/м		
	0,3 - 30 ГГц	ЩПЕ = 10 мкВт/см^2		

Можливі біологічні ефекти.

Людський організм завжди реагує на електромагнітне поле. Однак, для того щоб ця реакція переросла в паталогію і привела до захворювання, необхідний збіг ряду умов – у тому числі досить високий рівень поля і тривалість опромінення. Тому, при використанні техніки з малими рівнями поля майже немає впливу на здоров'я основної частини населення. Потенційна небезпека може грозити лише людям з підвищеною чутливістю до ЕМП і аллергетикам.

Крім того, відповідно до сучасних представлень, магнітне поле промислової частоти може бути небезпечним для здоров'я людини, якщо відбувається тривале опромінення (регулярно, не менш 8 годин на добу, протягом декількох років) з рівнем вище **0,2 мікротесла**.

На думку вчених, шкідливими вважаються електромагнітні поля напруженістю більше 0,2 мкТл. А тепер подивимося, які ж випромінювання нас оточують:

- приміські електрички 20 мктл,
- трамваї, тролейбуси 30 мктл,
- метро 50 - 100 мктл (на платформі, під час чи відправлення ,прибуття потяга),
- 150 - 200 мктл (у вагоні метрополітену),
- електроплити 1-3 мктл (на відстані 20 - 30 см. від передньої панелі),
- побутовий холодильник (у радіусі 10 см від компресора, під час його роботи),
- у холодильниках, оснащених системою “no frost” - на відстані 1 метра від дверцят- 0,2 мктл,
- електричний чайник 0,6 мктл (на відстані 20 см),
- електрична праска 0.2 мктл (20 см, причому тільки в режимі нагрівання),
- пральна машина 1 мктл (на висоті 1 м), 0,5 мктл (збоку, на відстані 50 см),

- пилосос 100 мктл,
- електробритва 100-350 мктл (таким чином, гоління супроводжується магнітною обробкою обличчя),
- будинкова ел.проводка перевищує 0.2 мктл (на відстані 30 см) .

Рекомендації:

-придбавши побутову техніку перевіряйте в сертифікаті оцінку про відповідність виробу вимогам "Міждержавних санітарних норм припустимих рівнів фізичних факторів при застосуванні товарів народного споживання в побутових умовах", Мсанпин 001-96;

-використовуйте техніку з меншою споживаною потужністю: магнітні поля промислової частоти будуть меньші за інших рівних умов;

-до потенційно несприятливих джерел магнітного полюя промислової частоти в квартирі відносяться холодильники із системою “без інею”, деякі типи “теплих підлог”, нагрівачі, телевізори, деякі системи сигналізації, різного роду зарядні пристрої, випрямлячі і перетворювачі струму – спальне місце повинне бути на відстані не менш 2-х метрів від цих предметів якщо вони працюють під час Вашого нічного відпочинку;

При розміщенні в квартирі побутової техніки керуйтеся наступними правилами:

- розміщайте побутові електроприлади по можливості далі від місць відпочинку,
- не розташовуйте побутові електроприлади по-близькості і не ставте їх один на одного.

Мікрохвильова піч у своїй роботі використовує для розігріву їжі електромагнітне поле, називане також мікрохвильовим. Робоча частота мікрохвильових печей складає 2,45 Ггц. Саме цього випромінювання і бояться багато людей. Однак, сучасні мікрохвильові печі обладнані досить надійним захистом, що не дає електромагнітному полю вириватися за межі робочого обєму. Разом з тим, не можна говорити що поле не проникає поза мікрохвильовою піччю. Для забезпечення безпеки при використанні печей у побуті в діють санітарні норми, що обмежують граничну величину витоку мікрохвильової печі. Називаються вони "Гранично припустимі рівні щільності потоку енергії, створюваної мікрохвильовими печами" і мають позначення СН № 2666-83. Згідно цим санітарним нормам, величина щільності потоку енергії електромагнітного поля не повинна перевищувати 10 мквт/см^2 на відстані 50 см від будь-якої точки корпуса печі при нагріванні 1 літра води. На практиці практично всі нові сучасні мікрохвильові печі витримують ця вимогу з великим запасом. Треба пам'ятати, що згодом ступінь захисту може знижуватися, в основному через появу мікрощілин в ущільненні дверцят. Це може відбуватися як через відкладення бруду, так і через механічні ушкодження. Тому дверцята і її ущільнення вимагають акуратності в експлуатації. Термін гарантованої стійкості захисту від витоків електромагнітного поля при нормальній експлуатації - декілька років.

Крім нвч-випромінювання, роботу мікрохвильової печі супроводжує інтенсивне магнітне поле, створюване струмом промислової частоти 50 Гц, що протікає в системі електроживлення печі. При цьому мікрохвильова піч є одним з найбільш могутніх джерел магнітного поля в квартирі. Для населення рівень магнітного поля промислової частоти в нашій країні дотепер не обмежений незважаючи на його істотну дію на організм людини при тривалому опроміненні. У побутових умовах

однократне включення (на декілька хвилин) не зробить істотного впливу на здоров'я людини. Однак, зараз часто побутова мікрохвильова піч використовується для розігріву їжі в виробничих умовах. При цьому працююча з нею людина попадає в ситуацію хронічного опромінення магнітним полем промислової частоти. В такому випадку на робочому місці необхідний обов'язковий контроль магнітного поля промислової частоти і нвч-випромінення. З огляду на специфіку мікрохвильової печі, доцільно включивши її відійти на відстань не менше 1,5 метра - у цьому випадку електромагнітне поле вас не торкнеться взагалі

7.3 Теле- і радіостанції.

Передавальні радіоцентри (ПРЦ) розміщаються в спеціально відведених для них зонах і можуть займати досить великі території (до 1000 га). По своїй структурі вони містять у собі одне чи кілька технічних будинків, де знаходяться радіопередавачі, і антенни, на яких розташовуються до декількох десятків антенно-фідерних систем (АФС). АФС містить в собі антену, що служить для випромінення радіохвиль, і фідерну лінію, що підводить до неї високочастотну енергію, генеруємому передавачем.

Зону можливої несприятливої дії ЕМП, створюваних ПРЦ, можна умовно розділити на дві частини.

Перша частина зони - це власне територія ПРЦ, де розміщені всі служби, що забезпечують роботу радіопередавачів і АФС. Це територія охороняється і на неї допускаються тільки особи, професійно зв'язані з обслуговуванням передавачів, комутаторів і АФС. Друга частина зони - це прилягаючі до ПРЦ території, доступ на який не обмежений і де можуть розміщатися різні житлові будівлі, у цьому випадку виникає загроза опромінення населення, що знаходиться в цій частині зони.

Високі рівні ЕМП спостерігаються на територіях, а нерідко і за межами розміщення передавальних радіоцентрів низької, середньої і високої частоти (ПРЦ НЧ, СЧ і ВЧ). Детальний аналіз електромагнітної обстановки на територіях ПРЦ свідчить про її крайню складність, зв'язаної з індивідуальним характером інтенсивності і розподілу ЕМП для кожного радіоцентра. У зв'язку з цим спеціальні дослідження такого роду проводяться для кожного окремого ПРЦ.

Широко розповсюдженими джерелами ЕМП у населених місцях у даний час є радіотехнічні передавальні центри (РТПЦ), що випромінюють у навколишнє середовище ультракороткі хвилі. Порівняльний аналіз санітарно-захисних зон (СЗЗ) і зон обмеження забудови в зоні дії таких об'єктів показав, що найбільші рівні опромінення людей і навколишнього середовища спостерігаються в районі розміщення РТПЦ «старої будівлі» з висотою антеною опори не більш 180 м. Найбільший внесок у сумарну інтенсивність впливу вносять трьох- і шестиповерхові антени **FM станцій**.

Радіостанції ДХ (частоти 30 - 300 кгц). У цьому діапазоні довжина хвиль відносно велика (наприклад, 2000 м для частоти 150 кгц). На відстані однієї довжини чи хвилі менше від антени поле може бути досить великим, наприклад, на відстані 30 м від антени передавача потужністю 500 квт, що працює на частоті 145 кгц, електричне поле може бути вище 630 В/м, а магнітне - вище 1,2 А/м.

Радіостанції СХ (частоти 300 кгц - 3 Мгц). Дані для радіостанцій цього типу говорять, що напруженість електричного поля на відстані 200 м може досягати 10

В/м, на відстані 100 м - 25 В/м, на відстані 30 м - 275 В/м (приведені дані для передавача потужністю 50 квт).
Радіостанції КХ (частоти 3 - 30 Мгц). Передавачі радіостанцій КВ мають звичайно меншу потужність. Однак вони частіше розміщаються в містах, можуть бути розміщені навіть на дахах житлових будинків на висоті 10- 100 м. Передавач потужністю 100 квт на відстані 100 м може створювати напруженість електричного поля 44 В/м і магнітного поля 0,12 Ф/м.

Телевізійні передавачі.

Телевізійні передавачі розташовуються, як правило, у містах. Передавальні антени розміщаються звичайно на висоті вище 110 м. З погляду оцінки впливу на здоров'я інтерес представляють поля на відстані від декількох десятків метрів до декількох кілометрів. Типові значення напруженості електричного поля можуть досягати 15 В/м на відстані 1 км від передавача потужністю 1 Мвт. В даний час проблема оцінки рівня ЕМП телевізійних передавачів особливо актуальна в зв'язку з різким ростом числа телевізійних каналів і передавальних станцій.

Основний принцип забезпечення безпеки - дотримання встановлених Санітарними нормами і правилами гранично припустимих рівнів електромагнітного поля. Кожен радіопередаючий об'єкт має Санітарний паспорт, у якому визначені границі санітарно-захисної зони. Тільки при наявності цього документа територіальні органи Держсанепіднадзора дозволяють експлуатувати радіопередаючі об'єкти. Періодично вони роблять контроль електромагнітної обстановки на предмет її відповідності встановленим ДР.

7.4 Супутниковий зв'язок.

Системи супутникового зв'язку складаються з приємопередаючої станції на Землі і супутника, що знаходиться на орбіті. Діаграма спрямованості антени станцій супутникового зв'язку має яскраво вираженої вузьконаправленний основний промінь - головний пелюсток. Щільність потоку енергії (ЩПЕ) у головному пелюстку діаграми спрямованості може досягати декількох сотень Вт/м^2 поблизу антени, створюючи також значні рівні поля на великому видаленні. Наприклад, станція потужністю 225 квт, що працює на частоті 2,38 Ггц, створює на відстані 100 км ЩПЕ рівну 2,8 Вт/м^2 . Однак розсіювання енергії від основного променя дуже невелике і відбувається більше всього в районі розміщення антени.

7.5 Стільниковий зв'язок.

Стільникова радіотелефонія є сьогодні однієї з найбільш інтенсивно розвиваючих телекомунікаційних систем. В даний час в усьому світі нараховується більш 85 мільйонів абонентів, що користаються послугами цього виду зв'язку. Передбачається, що до 2007 року їхнє число збільшиться до 500–510 мільйонів .

Основними елементами системи стільникового зв'язку є базові станції (БС) і мобільні радіотелефони (МРТ). Базові станції підтримують радіозв'язок з мобільними радіотелефонами, унаслідок чого БС і МРТ є джерелами електромагнітного випромінювання в УВЧ діапазоні.

Важливою особливістю системи стільникового радіозв'язку є дуже ефективне використання виділюваного для роботи системи радіочастотного спектра (багаторазове використання тих самих частот, застосування різних методів доступу), що уможливлює забезпечення телефонним зв'язком значного числа абонентів. У роботі системи застосовується принцип розподілу деякої території на зони, чи "стільники", радіусом звичайно 0,5–10 кілометрів.

Базові станції.

Базові станції підтримують зв'язок із мобільними радіотелефонами, що знаходяться в їхній зоні дії і працюють у режимі прийому і передачі сигналу. У залежності від стандарту, БС випромінюють електромагнітну енергію в діапазоні частот від 463 до 1880 Мгц.

Антени БС установлюються на висоті 15–100 метрів від поверхні землі на вже існуючих будівлях (суспільних, службових, виробничих і житлових будинках, димарях промислових підприємств і т.д.) чи на спеціально споруджених щоглах.

Серед встановлених в одному місці антен БС маються як передавальні (чи прйомопередаючі), так і прийомні антени, що не є джерелами ЕМП.

Виходячи з технологічних вимог побудови системи стільникового зв'язку, діаграма спрямованості антен у вертикальній площині розрахована таким чином, що основна енергія випромінювання (більш 90 %) зосереджена в досить вузькому "промені". Він завжди спрямований убік від споруджень, на яких знаходяться антени БС, і вище прилягаючих будівель, що є необхідною умовою для нормального функціонування системи.

Короткі технічні характеристики стандартів системи стільникового радіозв'язку:

Найменування стандарту	Діапазон частот БС	Діапазон частот МРТ	потужн БС, потужн МРТ	Радіус
NMT-450 Аналоговий	463 – 467,5 МГц	453 – 457,5 МГц	100 Вт 1 Вт	1 – 40 км
AMPS Аналоговий	869 – 894 МГц	824 – 849 МГц	100 Вт 0,6 Вт	2 – 20 км
D-AMPS (IS-136) Цифровий	869 – 894 МГц	824 – 849 МГц	50 Вт 0,2 Вт	0,5 – 20 км
CDMA Цифровий	869 – 894 МГц	824 – 849 МГц	100 Вт 0,6 Вт	2 – 40 км
GSM-900 Цифровий	925 – 965 МГц	890 – 915 МГц	40 Вт 0,25 Вт	0,5 – 35 км
GSM-1800 (DCS) Цифровий	1805 – 1880 МГц	1710 – 1785 МГц	20 Вт 0,125 Вт	0,5 – 35 км

БС є видом передавальних радіотехнічних об'єктів, потужність випромінювання яких (завантаження) не є постійної протягом 24 години на добу. Завантаження визначається наявністю власників стільникових телефонів у зоні обслуговування конкретної базової станції і їхнім бажанням скористатися телефоном для розмови, що, у свою чергу, докорінно залежить від часу доби, місця розташування БС, дня тижня й ін. У нічне годинни завантаження БС практично дорівнює нулю, тобто станції в основному "мовчать".

Мобільні радіотелефони.

В широкому застосуванні були в основному радіозасоби довгохвильового(частота від 30 до 300 кгц і довжин хвилі від 10000 до 1000 м), середньохвильового(частота від 300 кгц до 3 МГц і довжина хвилі від 1000 до 100 м) і короткохвильового (частота від 3 до 30 МГц і довжина хвилі від 100 до 10 м) діапазонів. Пізніше, (наприкінці 40-х початку 50-х років минулого століття), почалося освоєння ультракороткохвильового (частота від 30 МГц до 1 ГГц і довжина хвилі від 10 до 0,3 м) і (наприкінці 70-х початку 80-х) мікрохвильового(частота від 1 ГГц до 300 ГГц м і довжина хвилі від 0,3 до 0,001 м) діапазонів. Було відзначене, що потрапляючи в зону впливу радіохвиль з високою енергетикою (потужності передавачів у сотні і тисячі Ватів!) навіть на нетривалий час, людин відчуває погіршення самопочуття: швидка втомлюваність, підвищення температури тіла, погіршення зору. А при тривалому впливі можливий навіть розвиток симптомів подібних із променевою хворобою. Однак вчені швидко розібралися в питанні, що не можна ототожнювати вплив радіоактивного випромінювання (також має електромагнітну природу) і радіохвиль на організм людини, тому що фізика процесів не ідентична. У першому випадку це проникаюче вплив потоків бетта і гама часток (електромагнітних хвиль миріаметрового діапазону – довжина хвилі від 10^{-14} до 10^{-16} м), що викликає зміну біохімічних процесів навіть при відносно невисокій енергетиці. В другому, це вплив на біохімічні процеси за рахунок поглинання організмом значних потоків електромагнітної енергії. А подібність кінцевих результатів у даному питанні може привести лише до поверхневих і не до кінця вірних висновків.

Саме тоді був прийнятий основний критерій оцінки впливу радіохвиль на живі організми – це поняття гранично припустимих норм по ЩПЕ (щільності потоку енергії електромагнітного характеру)! Тим самим підкреслювалося, що визначальним фактором у даному питанні є те, скільки електромагнітної енергії може поглинути організм людини без істотних негативних наслідків.

В нашій країні ці норми такі:

• 10 Вт/м^2(десять Ватів на метр квадратний) чи 1000 мкВт/см^2 – для технічного персоналу, зайнятого обслуговуванням випромінюючої апаратури не більше восьми годин на добу;

• 0,1 Вт/м^2(одна десята Вати на метр квадратний) чи 10 мкВт/см^2– для населення, з врахуванням перебування в зоні виміру 24 години на добу.

Були також розроблені і стандартизовані методики виміру ЩПЕ і відповідні прилади. Різниця норм для професійно зайнятих працівників і населення істотна – 100 разів!!!

А які наслідки хвильового характеру впливу на організм? Хвилі яких частот (довжин) більш небезпечні для людини і взагалі всього живого на Землі? І чому в більшості випадків досить обмежуватися тільки виміром щільності потоку енергії (ЩПЕ)?

Будь-яке електромагнітне поле характеризується його напруженістю, що на віддалі від випромінювача, (штучного чи природного), починає носити досить рівномірний характер, тобто в ньому (у полі) відсутні значні енергетичні вузли (мінімуми енергії) і пучності (максимуми енергії). Іншими словами, структура поля вирівнюється. Існує поняття декількох зон електромагнітного поля в міру видалення від випромінювача (передавальної антени) в порівнянні з довжиною випромінюваної радіохвилі:

• Зверхближня зона – зона на відстані менше λ/4 (четверті довжини випромінюваної хвилі);
• Ближня зона – зона на відстані від λ/4 до λ/2 (від четверті до половини довжини хвилі);
• Середня зона – зона на відстані від λ/2 до декількох λ;
• Далека зона – від декількох десятків до сотень і тисяч λ.

Чим же характеризуються ці зони? У перших двох, структура поля, ще не має хвильового характеру, тобто ще не ясно, чи формується взагалі радіохвиля, як стійка структура коливального характеру (чи будуть мати місце періодичні зміна фази її електричної і магнітний складових – це основна ознака будь-якої хвилі, періодична зміна фаз її параметрів). А це значить, що в цих двох зонах безглуздо шукати і вивчати хвильовий характер впливу на що-небудь, що знаходиться в їхніх межах. Мова може йти тільки про поглинання потоку енергії, що виходить від випромінювача. Саме це і визначає основний вплив, тому що не сформована структура не може ні на що вплинути (у даному випадку радіохвилі, ще просто не існує!).

В двох інших зонах хвильова структура електромагнітного поля вже цілком стійка і напруженість поля, особливо в останньої, близька до рівномірного. Дотепер у світі немає яких-небудь серйозних досліджень на цю тему. І не тому, що вчені не знають, з якої сторони підступитися до цього питання, а тому, що дослідження подібного типу повинні охоплювати велику кількість випробуваних на досить тривалому за часом (15...20 років) інтервалі спостереження. Тільки при такому серйозному підході до суті проблеми можна буде говорити про серйозність і вірогідність отриманих результатів. І це стосується не тільки і не стільки вивчення впливу хвильового характеру на живе середовище, але і додаткових уточнюючих досліджень про норми на ППЕ. Однак при цьому приходиться зіштовхнутися з проблемою суспільного характеру. Де набрати велику кількість людей, згодних не тільки піддаватися періодичним впливам радіохвиль різної частоти і потужності, але і проходити після цього скрупульозне медичне обстеження, як відразу після

експерименту, так і через деякий час після нього? І так протягом двох десятків років!

Все це і привело до того, що на сьогоднішній день у світі так і не здійснено яких-небудь серйозних і поглиблених досліджень на вищезазначену тему, що дозволяють зробити однозначні і незаперечні висновки.

Мобільний радіотелефон (МРТ) являє собою малогабаритний приймач-передавач. У залежності від стандарту телефону, передача ведеться в діапазоні частот 453 – 1785 Мгц. Потужність випромінювання МРТ є величиною змінною, у значній мірі залежної від стану каналу зв'язку "мобільний радіотелефон – базова станція", тобто чим вище рівень сигналу БС у місці прийому, тим менше потужність випромінювання МРТ. Максимальна потужність знаходиться в границях 0,125–1 Вт, однак у реальній обстановці вона звичайно не перевищує 0,05 – 0,2 Вт.

Нижче приведені дані про випромінювання, величини щільності потоку (ЩП) електромагнітного випромінювання різних джерел. Щільність потоку виміряється в одиницях потужності (Вт, мвт, мкВт), що приходиться на одиницю площі ($м^2$, $см^2$).

Джерело	**ЩП, мкВт/см^2**	**Ефект**	**Моб телефон***	**БС****	**Перевищення**
Резонанс Шумана	0,0000001	Вплив на мозок	25 км	900 км	-
Природний електромагнітн фон	0,000001		2500 м	90 км	10 разів
Техногенно- змінений фон (середнє значення)	0,01	Зміна рівня мелатоніну в мозку людини, зміна и, незворотні пошкодження ДНК.	25 м	900 м	100000 разів
Нормоване значення ЩП від радіотелефонів.	2	Здатний викликати лейкоз у дітей.	5 м	180 м	20000000 разів

Нормоване значення ЩП від базових станцій (БС) стільниково-го зв'язку.	10	Незворотні пошкодження ДНК	0.8 м	30 м	100000000 разів
Нормоване значення ЩП від стільникових телефонів.	100	Протягом 2 хв. змінює гемато-енцефаличного бар'єра.	25 см	9 м	1000000000 разів
Термічний ефект	10000	Неконтр загибель клітин	0.25 см	9 см	100000000000 разів

* В графі зазначені відстані, на яких формується зазначене значення ЩП від працюючого стільникового телефону.

** В графі зазначені відстані, на яких формується зазначене значення ЩП від працюючої базової станції.

За нульову оцінку узяте значення ЩП резонансу Шумана. Що це таке? Це сверхнизькочастотний електромагнітний вплив, відкритий німецьким фізиком Т.Шуманом, що існувало завжди, при впливі якого відбувалася еволюція всього живого на Землі й в умовах якого відбувався равиток людства. Джерелом наднизького випромінювання є існування двох заряджених сфер гігантських розмірів: струмопровідної земної поверхні внаслідок постійної грозової діяльності (в одну секунду на Землі відбувається в середньому близько 100 гроз), а також іоносфери (шар атмосфери на висоті примерно 100 км від земної поверхні), що заряджається "сонячним вітром". Між цими сферами знаходиться атмосфера, що є слабким провідником електричного струму. Подібна конструкція є причиною виникнення в проміжному шарі стійких низькочастотних коливань, що практично не загасають і мають фіксовані частоти. Серед них виділяється частота близько 8 Гц, що цілком збігається з частотою альфа-ритму мозку людини. Зверніть увагу, така ж частота є обов'язкової під час розмови по мобільному телефоні стандарту GSM .

Ще в 50-ті роки 20 століття було доведено, що інтенсивність резонансу Шумана впливає на вищу нервову діяльність людини, а також інтелектуальні здібності. При цьому варто враховувати, що інтенсивність хвиль Шумана вкрай низька і складає усього частки пікоВат/см^2. Очевидно, що навіть це мале значення здатне впливати на людину. Саме тому воно і було узято як відправну точку.

А тепер порівняйте інші джерела електросмогу і їхньої інтенсивності. Їхній вплив перевищує природний рівень у мільйони і навіть трильйони раз. Отже, ми живемо в умовах надзвичайно сильного електромагнітного шуму, що б'є по нашому організмі. І чи вартує після цього дивуватися, що ми реагуємо на цей впливом зміною свого здоров'я та хворобами.

Стільниковий телефон є малогабаритним приймачем-передатчиком. В залежності від стандарту телефону, передача ведеться в діапазоні частот 453 – 1800 Мгц. Потужність випромінювання є величиною змінної, в значній мірі залежить від стану каналу зв'язку "мобільний телефон – базова станція", тобто чим вище рівень сигналу базової станції в місці прийому, тим менше потужність випромінювання стільникового телефону. Максимальна потужність знаходиться в границях 0,125–1 Вт. Найбільшою вихідною потужністю характеризуються телефони стандарту NMT-450 (номінальна потужність близько 1 Вт), меншої - GSM-900 (0,25 Вт) і найменшого стандарту GSM-1800 (0,125Вт).

Відповідно до тимчасово - припустимим рівням електромагнітних випромінювань щільність потоку (ЩП) для користувачів мобільних телефонів не повинна перевищувати 100 мкВт/см^2. Необхідно відзначити, що в природних умовах значення щільності потоку високочастотного випромінювання мале і складає лише 10^{-15} мкВт/см^2.

Відповідно до міжнародних вимог випромінююча потужність стільникових телефонів вимірюють в одиницях SAR. SAR (Specific Adsorption Rate) - питома поглинена потужність, виражена на одиницю маси чи тіла тканини. В одиницях СІ, SAR визначається у ватах на 1 кг (Вт/кг). Не плутайте цей показник з номінальною потужністю стільникового телефону, що звичайно вказується в інструкції. Донедавна верхньою границею значення SAR у Європі вважалася величина 2 Вт/кг. Загальноприйнята наступна градація величин SAR для мобільних телефонів:

Дуже низька здатність опромінювання	**SAR < 0.2 Вт/кг**
Низька здатність опромінювання	**SAR від 0.2 до 0.5 Вт/кг**
Середня здатність, опромінювання	**SAR від 0.5 до 1.0 Вт/кг**
Висока здатність опромінювання	**SAR > 1.0 Вт/кг**

Величину **SAR** виміряти дуже складно. Потрібно спеціальне устаткування та імітатори тканин людського організму. В світі не існує єдиної методики виміру SAR.Тому дані цього показника, вимірювані в незалежних центрах, можуть відрізнятися навіть у кілька разів. Найбільш реальним є вимір щільності потоку електромагнітного випромінювання (ЩП) стільникового телефону, розрахунок його випромінюючої здатності ,виходячи з потужності апарата. Саме за цими показниками можна реально оцінити безпеку.

Так у чому ж небезпека для здоров'я від мобільних телефонів? В дії будь-якого електромагнітного випромінювання прийнято виділяти два ефекти: термічний і нетермічний (останній часто позначають, як інформаційний).

Термічний ефект. Пояснювати його суть не має особливого змісту. Ви можете його спостерігати по роботі мікрохвильової печі. Приблизно таку ж дію робить випромінювання від стільникового телефону. Врахуйте ще і те, що антена-основний випромінювач телефону, знаходиться в 3-5 сантиметрах від вашого головного мозку, на який електромагнітне поле і діє. Природно температура окремих ділянок мозку підвищується. При тривалій розмові цей ефект можна відчувати по підвищенню температури вушної раковини. Підраховано, що при величині SAR 4 Вт/кг протягом 30 хвилин температура тканини в здорового дорослого індивідуума піднімається на 1 градус Цельсія. Це несприятливий ефект для будь-яких органів, що будуть відповідати порушенням своєї функції. До речі, все нормування мікрохвильового випромінювання від стільникових телефонів базується тільки на термічному ефекті. Інший орган, підданий впливу випромінювання від стільникового телефону, хрусталик ока. Через виконання своїх дуже важливих функцій - підтримки прозорості й акомодації він погано постачається кров'ю і тому особливо підданий дії електромагнітного випромінювання. А це впливає на гостроту зору.

Нетермічний чи інформаційний ефект. Вивчений дуже слабко. Суть його полягає в наступному. Мобільні телефони стандарту GSM здійснюють передачу інформації імпульсами, об'єднаних у блоки. Блок складається з 8 імпульсів. У розпорядженні кожного користувача мається тільки один з восьми імпульсів. Інші сім належать іншим семи абонентам, що у цей момент на даній частоті можуть вести телефонні розмови. Тривалість одного GSM-блоку складає 4,616 мілісекунди(мс), отже, частота пульсації мобільного телефону складає 1/4,616 мс=216,6 Гц чи округленно 217 Гц. З генерацією кожного восьмого імпульсу відбувається і пропорційне виділення енергії. Якщо номінальна потужність стільникового апарата, відповідно до інструкції дорівнює 2 Вт, то потужність, виділювана при кожнім імпульсі буде: 2/8=0,25 Вт. Блоки згаданих імпульсів між мобільним телефоном і базовою станцією групуються в мультиблоки, що складаються з 26 повторень. Отже, другою частотою, що випускається стільниковим телефоном є частота: 217 / 26= 8,35 Гц. Більш того, деякі види мобільних апаратів, що працюють в енергозберігаючому режимі (DTX), здатні генерувати третю частоту - 2 Гц. В наборі низькочастотного випромінювання і складається ще одна небезпека мобільного зв'язку. Справа в тім, що згадані частоти стільникових апаратів збігаються з частотами власної, природної біоелектричної активності головного мозку людини, що реєструються на електроенцефалограмі (ЭЭГ). Так частота **217 Гц** збігається з гамма-ритмом мозку, **8,35 Гц** - з альфа-ритмом, а **2 Гц** - з дельта-ритмом. Отже, ззовні (з безпосередньої близькості), в головний мозок людини переносяться сигнали, що здатні взаємодіяти з власною біоелектричною активністю головного мозку, (наприклад, шляхом резонансу), і тим самим, порушувати його функції. Такі зміни помітні на електроенцефалограмі і не зникають тривалий час після закінчення розмови. Дуже важливо відзначити ще і те, що саме альфа-хвилі надзвичайно індивідуальні, безпосередньо зв'язані з розумовою діяльністю людини і як вважають, є відображенням сканування внутрішніх образів свідомості. Абстрактне мислення зв'язане саме з альфа-ритмом мозку, під час сну переважає дельта-ритм, а гамма-ритм - з активною діяльністю людини. Чи реально негативний вплив пульсуючих джерел енергії на організм людини? Медикам відомий такий

приклад, коли вплив на людину пульсуючим випромінення з частотою 15 Гц , що має приховану форму фоточуттєвої епілепсії приводило до виникненню припадку. Як Вам тепер подобається звичка розташовувати біля узголів'я ліжка стільниковий телефон і використовувати його як будильник. Мобільний телефон вночі не "спить", а постійно, навіть у стані чекання виклику, працює в пульсуючому режимі.

Про більшу схильність впливу випромінювання на молодих людей говорить і дослідження, проведене серед 11.000 користувачів стільникового зв'язку за замовленням Norwegian Radiation Protection Board, Національним Інститутом "Робочого життя" (Швеція), а також SINTEF Unimed (Норвегія). Дослідження показало, що люди, які використовували телефон більше 2 хвилин в день, скаржилися на дискомфорт і сторонні ефекти. Проблеми зі здоров'ям зростають, якщо користатися телефоном довше. Половина опитаних абонентів повідомили, що при використанні стільникових телефонів відчувають неприємний розігрів в області голови, навколо вуха. Найбільшому ризику піддаються молоді люди. Ті, кому ще немає 30, у 3-4 рази частіше піддаються впливу. Особливо чуттєві до високочастотного випромінювання мобільних телефонів діти.

Варто враховувати, що в умовах екранування (автомобіль, залізобетонні будинки) щільність потоку електромагнітного випромінювання, що діє на людину багаторазово підсилюється.

Основними симптомами несприятливого впливу стільникового телефону на стан здоров'я є:

головні болі;

порушення пам'яті і концентрації уваги;

неминуща утома;

депресивні захворювання;

біль і різь в очах, сухість їх слизуватої;

прогресивне погіршення зору;

лабільність артеріального тиску і пульсу

(показано, что після розмови по мобільному

телефону артеріальний тиск може підвищуватися

Дотепер немає однозначної думки про розміри шкоди, заподіюваного нашому організму стільниковими телефонами Причин цьому багато. Мабуть, головні причини - наступні. Перша - порівняно невеликий термін існування самого мобільного зв'язку. Друга - у стільниковому бізнесі обертаються великі гроші, що дозволяє зацікавленим корпораціям спонсорувати одержання будь-якого зручних для них відповідей на питання, що хвилюють багатьох власників радіотелефонів. Проте, всі дослідники одностайні - електромагнітні випромінювання від

стільникових телефонів, звичайно ж, впливають на тканини мозку. Розходяться лише в оцінці ступеня цього впливу. Тим більше що на сьогодні неможливо оцінити, як позначиться цей вплив у віддаленій перспективі. Проте, у багатьох країнах, наприклад у Великобританії, міністерство освіти рекомендує заборонити користатися мобільними телефонами дітям до 16 років, оскільки ряд проведених у Великобританії досліджень показав, що випромінювання мобільних телефонів може впливати на дітей. Досить давно доведена британськими вченими і зв'язок між впливом електромагнітних випромінювань і виникненням лейкозів у дітей.
В результаті досліджень, у яких взяли участь більш 11 тисяч жителів Ірландії, установлено, що навіть ті люди, що користаються мобільними телефонами не більш двох хвилин день, висловлювали скарги на дискомфорт, що відчувається ними, і інші хворобливі симптоми. Ті ж, хто використовує мобільні засоби зв'язку регулярно, відзначають часті головні болі, проблеми з концентрацією уваги, порушення роботи внутрішніх органів. Причому частота виникнення цих проблем прямо пропорційна тривалості телефонних переговорів. Більш того, найбільшою мірою шкідливому впливу електромагнітних випромінювань піддаються молоді люди у віці до 30 років, серед них прояву хворобливих симптомів зустрічаються в три-чотири разів частіше, ніж серед більш старших вікових категорій. У Швеції ж при висновку договорів страхування страховики частенько вводять у договори застереження "... за винятком збитку, заподіяного електромагнітним полем", Національний інститут по вивченню раку (США) вважає високочастотне випромінювання стільникових телефонів фактором ризику. Численні дослідження відзначають частішання таких проблем, як порушення пам'яті, хвороба Альцгеймера. різні пухлини (наприклад, пухлини головного мозку).

Питання про вплив випромінювання МРТ на організм користувача дотепер залишається відкритим. Численні дослідження, проведені вченими різних країн на біологічних об'єктах (у тому числі, на добровольцях), привели до неоднозначних, іноді суперечним один одному, результатам. Незаперечним залишається лише той факт, що організм людини "відгукується" на наявність випромінювання стільникового телефону. Тому власникам МРТ рекомендується дотримувати деякі запобіжні заходи:

- не користайтеся стільниковим телефоном без необхідності;
- розмовляйте безупинно не білбше 3 – 4 хвилин;
- не допускайте, щоб МРТ користалися діти;
- при покупці вибирайте стільниковий телефон з меншою максимальною потужністю випромінювання;
-в автомобілі використовуйте МРТ разом із системою гучномовного зв'язку "hands-free" із зовнішньою антеною.

Для людей, що оточують людину, що розмовляє по мобільному радіотелефоні, електромагнітне поле, створюване МРТ не представляє небезпеки.

Дослідження можливого впливу біологічної дії електромагнітного поля елементів систем стільникового зв'язку викликають великий інтерес у громадськості. Публікації в засобах масової інформації досить точно відбивають сучасні тенденції в цих дослідженнях. Швейцарські тести показали, що випромінювання, поглинене головою людини, знаходиться в припустимих європейськими стандартами межах.

Фахівці Центру електромагнітної безпеки провели медико-біологічні експерименти по дослідженню впливу на фізіологічний і гормональний стан людини електромагнітного випромінювання мобільних телефонів існуючих і перспективних стандартів стільникового зв'язку.

При роботі мобільного телефону електромагнітне випромінювання сприймається не тільки приймачем базової станції, але і тілом користувача, і в першу чергу його головою. Що при цьому відбувається в організмі людини, наскільки цей вплив небезпечний для здоров'я? Однозначної відповіді на це питання дотепер не існує. Однак експеримент російських учених показав, що мозок людини не тільки відчуває випромінювання стільникового телефону, але і розрізняє стандарти стільникового зв'язку.

Керівник дослідницького проекту доктор медичних наук Юрій Григор'єв вважає, що стільникові телефони стандартів NMT-450 і GSM-900 викликали достовірні зміни в біоелектричній активності головного мозку. Однак клінічно значимих наслідків для організму людини однократне 30-хвилинне опромінення електромагнітним полем мобільного телефону не робить. Відсутність достовірних вимірів у електроенцефалограммі у випадку використання телефону стандарту GSM-1800 може характеризувати його як найбільше “оптимальний” для користувача з трьох використаних в експерименті систем зв'язку.

7.6 Радари.

Радіолокаційні станції оснащені, як правило, антенами дзеркального типу і мають вузьконаправленну діаграму випромінювання у виді променя, спрямованого вздовж оптичної осі.

Радіолокаційні системи працюють на частотах від 500 Мгц до 15 Ггц, однак окремі системи можуть працювати на частотах до 100 Ггц. Створюваний ними Ем-сигнал принципово відрізняється від випромінювання інших джерел. Зв'язано це з тим, що періодичне переміщення антени в просторі приводить до просторової переривчастості опромінення. Тимчасова переривчастість опромінення обумовлена циклічністю роботи радіолокатора на випромінювання. Час наробітку в різних режимах роботи радіотехнічних засобів може обчислюватися від декількох годин до доби. Так у метеорологічних радіолокаторів з тимчасовою переривчастістю 30 хв - випромінювання, 30 хв - пауза сумарний наробіток не перевищує 12 год., у той час як радіолокаційні станції аеропортів у більшості випадків працюють цілодобово. Ширина діаграми спрямованості в горизонтальній площині звичайно складає кілька градусів, а тривалість опромінення за період огляду складає десятки міллісекунд.

Радари метрологічні можуть створювати на видаленні 1 км ЩПЕ ~ 100 Вт/м^2 за кожен цикл опромінення. Радіолокаційні станції аеропортів створюють ЩПЕ ~ 0,5 Вт/м^2 на відстані 60 м. Морське радіолокаційне устаткування встановлюється на всіх кораблях, звичайно воно має потужність передавача на порядок меншу, ніж в аеродромних радарів, тому в звичайному режимі сканування ЩПЕ, створюване на відстані декількох метрів, не перевищує 10 Вт/м^2.

Зростання потужності радіолокаторів різного призначення і використання остронаправленных антен кругового огляду приводить до значного збільшення

інтенсивності ЕМВ Свч-діапазона і створює на місцевості зони великої довжини з високою щільністю потоку енергії.

7.7 Персональні комп'ютери.

Основним джерелом несприятливого впливу на здоров'я користувача комп'ютера є засіб візуального відображення інформації на електронно-променевій трубці. Нижче перераховані основні фактори його несприятливого впливу:

- ергономічні параметри екрана монітора ,
- зниження контрасту зображення в умовах інтенсивної зовнішньої засвітки,
- дзеркальні відблиски від передньої поверхні екранів моніторів,
- наявність мерехтіння зображення на екрані монітора,
- випромінювальні характеристики монітора,
- електромагнітне поле монітора в діапазоні частот 20 Гц- 1000 Мгц
- статичний електричний заряд на екрані монітора,
- випромінювання в діапазоні 1050 нм- 1 мм,
- рентгенівське випромінювання > 1,2 кев .

Комп'ютер як джерело змінного електромагнітного поля.

Основними складовими частинами персонального комп'ютера (ПК) є: системний блок (процесор) і різноманітні пристрої введення/висновку інформації: клавіатура, дискові нагромаджувачі, принтер, сканер, і т.п. Кожен персональний комп'ютер включає засіб візуального відображення інформації - монітор, дисплей. Як правило, у його основі - пристрій на основі електронно-променевої трубки. ПК часто оснащують мережними фільтрами (наприклад, типу "Pilot"), джерелами безперебійного харчування й іншим допоміжним електроустаткуванням. Всі ці елементи при роботі ПК формують складну електромагнітну обстановку на робочому місці користувача.

ПК як джерело ЕМП

Джерело (перша гармоніка)	**Діапазон частот**
- монітор мережний трансформатор блоку харчування	50 Гц
- статичний перетворювач напруги в імпульсному блоці живлення	20 - 100 кгц
- блок кадрового розгорнення і синхронізації	48 - 160 Гц
- блок рядкового розгорнення і синхронізації	5 -110 кгц
- анодна напруга монітора, що прискорює, (електростатика)	0 Гц
- системний блок (процесор)	50 Гц - 1000 МГц
-пристрій введення/виводу інформації	0 Гц, 50 Гц

- джерела безперебійного живлення 50 Гц, 20 -100 кгц

Електромагнітне поле, створюване персональним комп'ютером, має складний спектральний склад у діапазоні частот від 0 Гц до 1000 Мгц. Електромагнітне поле має електричну (Е) і магнітну (Н) складові, причому взаємозв'язок їхній досить складний, тому оцінка Е и Н виробляється роздільно.

Максимальні зафіксовані на робочому місці значення ЕМП

Вид поля:	**діапазон частот:**	**одиниця виміру поля:**	**Значення по осі екрана монітора**:
Електричне поле,	100 кгц- 300 МГц ,	В/м	17,0 -24,0
Електричне поле,	0,02- 2 кгц,	В/м	150,0 -155,0
Електричне поле,	2- 400 кгц	В/м	14,0 -16,0
Магнітне поле, нчп нчп	100кгц- 300МГц,	ма/м	
Магнітне поле,	0,02- 2 кгц,	ма/м	550,0 -600,0
Магнітне поле,	2- 400 кгц,	ма/м	35,0 -35,0
Електростатичне поле, кв/м	22,0 -		

Діапазон значень електромагнітних полів, виміряних на робочих місцях користувачів ПК :

Найменування вимірюваних параметрів	Діапазон частот 5 Гц - 2 кгц	Діапазон частот 2 - 400 кгц
Напруженість змінного електричного поля, (В/м):	1,0 - 35,0	0,1 - 1,1
Індукція змінного магнітного поля, (нТл) :	6,0 - 770,0	1,0 - 32,0

Комп'ютер як джерело електростатичного поля.

При роботі монітора на екрані кінескопа накопичується електростатичний заряд, що створює електростатичне поле (Естп). У різних дослідженнях, при різних умовах виміру значення Естп коливалися від 8 до 75 кв/м. При цьому люди, що працюють з монітором, здобувають електростатичний потенціал. Розкид електростатичних потенціалів користувачів коливається в діапазоні від -3 до +5 кв. Коли Естп суб'єктивно відчувається, потенціал користувача служить вирішальним фактором при виникненні неприємних суб'єктивних відчуттів.
Помітний внесок у загальне електростатичне поле вносять клавіатури, що електризуються від тертя поверхні, і миші. Експерименти показують, що навіть після роботи з клавіатурою, електростатичне поле швидке зростає з 2 до 12 кв/м. На

окремих робочих місцях в області рук реєструвалися напруженості статичних електричних полів більш 20 кв/м.

Вплив на здоров'я користувача електромагнітних полів комп'ютера.

По узагальненим даним, у працюючих за монітором від 2 до 6 годин на добу функціональні порушення центральної нервової системи відбуваються в середньому в 4,6 рази частіше, ніж у контрольних групах, хворобі серцево-судинної системи - у 2 рази частіше, хвороби верхніх дихальних шляхів - у 1,9 рази частіше, хвороби опорно-рухового апарата - у 3,1 рази частіше. Зі збільшенням тривалості роботи на комп'ютері співвідношення здорових і хворих серед користувачів різко зростає. Дослідження функціонального стану користувача комп'ютера, проведені в 1996 році в Центром електромагнітної безпеки, показали, що навіть при короткочасній роботі (45 хвилин) в організмі користувача під впливом електромагнітного випромінювання монітора відбуваються значні зміни гормонального стану і специфічні зміни біоструму мозку. Особливо яскраво і стійко ці ефекти виявляються в жінок. Замічено, що в груп осіб, (у даному випадку це склало 20%), негативна реакція функціонального стану організму не виявляється при роботі з ПК менш 1 години. Виходячи з аналізу отриманих результатів зроблений висновок про можливість формування спеціальних критеріїв професійного добору для персоналу, що використовує комп'ютер у процесі роботи.

Вплив аероіонного складу повітря. Зонами, що сприймають аэроіони в організмі людини, є дихальні шляхи і шкіра. Єдиної думки щодо механізму впливу аэроіонів на стан здоров'я людини немає.

Вплив на зір. До зорового стомлення користувача ВДТ відносять цілий комплекс симптомів: поява "завіси" перед очима, ока утомлюються, робляться хворобливими, з'являються головні болі, порушується сон, змінюється психофізичний стан організму. Необхідно відзначити, що скарги на зір можуть бути зв'язані як зі згаданими вище факторами ВДТ, так із умовами освітлення, станом зору оператора й ін.

Синдром тривалого статистичного навантаження (СТСН). У користувачів дисплеїв розвивається м'язова слабість, зміни форми хребта. У США визнано, що СТСН - професійне захворювання з найвищою швидкістю поширення. При змушеній робочій позі, при статичному м'язовому навантаженні м'язів ніг, пліч, шиї і рук довгостроково перебувають у стані скорочення. Оскільки м'язи не розслаблюються, у них погіршується кровопостачання; порушується обмін речовин, накопичуються біопродукти розпаду і, зокрема, молочна кислота.

Стрес. Користувачі дисплеїв часто знаходяться в стані стресу. За даними Національного Інституту охорони праці і профілактики профзахворювань США (1990 р.) користувачі ВДТ у більшому ступені, чим інші професійні групи, включаючи авіадиспетчерів, піддані розвитку стрессорних станів. При цьому в більшості користувачів робота на ВДТ супроводжується значному розумовою напругою. Показано, що джерелами стресу можуть бути: вид діяльності, характерні риси комп'ютера, використовуване програмне забезпечення, організація роботи,

соціальні аспекти. Робота на ВДТ має специфічні стрессорні фактори, такі як час затримки відповіді (реакції) комп'ютера при виконанні команд людини, "навченість командам керування" (простота запам'ятовування, подібність, простота використання і т.зв.), спосіб візуалізації інформації і т.д. Перебування людини в стані стресу може привести до змін настрою людини, підвищенню агресивності, депресії, дратівливості. Зареєстровано випадки психосоматичних розладів, порушення функції шлунково-кишкового тракту, порушення сну, зміна частоти пульсу, менструального циклу. Перебування людини в умовах довгостроково діючого стрес-фактора може привести до розвитку серцево-судинних захворювань.

Скарги користувачів персонального комп'ютера можливі причини їхнього походження.

Суб'єктивні скарги	**Можливі причини**
різь в очах	візуальні эргономические параметри монітора, висвітлення на робочому місці й у приміщенні
головний біль	аероїдний склад повітря в робочій зоні, режим роботи,
підвищена нервозність	електромагнітне поле, колірна гама приміщення, режим роботи ,
підвищена стомлюваність	електромагнітне поле, режим роботи ,
розлад пам'яті	електромагнітне поле, режим роботи ,
порушення сну	режим роботи, електромагнітне поле,
випадання волос	електростатичні поля, режим роботи .
прищі і почервоніння шкіри	електростатичні поле, аэроионный і пиловий склад повітря в робочій зоні
болю в животі попереку	неправильна посадка, викликана неправильним пристроєм робочого місця
біль у зап'ястях і пальцях	неправильна конфігурація робочого місця, у тому числі висота столу не відповідає росту і висоті крісла
	незручна клавіатура; режим роботи

Широко відомі шведські технічні стандарти безпеки моніторів **TCO92/95/98 і MPR II**. Ці документи визначають вимоги до монітора персонального комп'ютера по параметрах, здатним впливати на здоров'я користувача.

Найбільш тверді вимоги до монітора пред'являє **TCO 95.** Він обмежує параметри випромінювання монітора, споживання електроенергії, візуальні параметри, так що робить монітор найбільш лояльним до здоров'я користувача. У частині випромінювальних параметрів йому відповідає і **TCO 92**. Розроблено стандарт Шведською конфедерацією профспілок.

Стандарт MPR II менш твердий – установлює граничні рівні електромагнітного поля приблизно в 2,5 рази вище. Розроблений Інститутом захисту від випромінювань (Швеція) та інш. організацій, у тому числі найбільших виробників моніторів.

В частині електромагнітних полів стандарту MPR II відповідають російські санітарні норми Санпин 2.2.2.542-96 “Гігієнічні вимоги до відеодисплейних терміналів, персональним електронно-обчислювальним машинам і організації робіт”.

Засобу захисту користувачів ПК від ЕМП.

В основному з засобів захисту пропонуються захисні фільтри для екранів моніторів. Вони використовується для обмеження дії на користувача шкідливих факторів з боку екрана монітора, поліпшує ергономічні параметри екрана монітора і знижує випромінювання монітора в напрямку користувача.

7.8 Як діє ЕМП на здоров'я.

В СРСР широкі дослідження електромагнітних полів були початі в 60-і роки. Був накопичений великий клінічний матеріал про несприятливу дію магнітних і електромагнітних полів, було запропоновано ввести нове нозологічне захворювання "Радіохвильова хвороба" чи "Хронічна пораження мікрохвилями". Надалі, роботами вчених у Росії було встановлено, що, по-перше, нервова система людини, особливо вища нервова діяльність, чуттєва до ЕМП, і, по-друге, що ЕМП володіє т.зв. інформаційною дією при впливі на людину в інтенсивностях нижче граничної величини теплового ефекту. Результати цих робіт були використані при розробці нормативних документів у Росії. В результаті нормативи в Росії були встановлені дуже твердими і відрізнялися від американських і європейських (наприклад, у Росії ДР для професіоналів 0,01 мвт/см^2; у США - 10 мвт/см^2).

7.8.1 Біологічна дія електромагнітних полів.

Експериментальні дані як вітчизняних, так і закордонних дослідників свідчать про високу біологічну активність ЕМП у всіх частотних діапазонах. При відносно високих рівнях, що опромінює ЕМП сучасна теорія визнає тепловий механізм впливу. При відносно низькому рівні ЕМП (приміром, для радіочастот вище 300 Мгц це менш 1 мвт/см^2) прийнято говорити про нетепловий чи інформаційний характер впливу на організм. Механізми дії ЕМП у цьому випадку ще мало вивчені.

Численні дослідження в області біологічної дії ЕМП дозволять визначити найбільш чуттєві системи організму людини: нервова, імунна, ендокринна і статева. Ці системи організму є критичними. Реакції цих систем повинні обов'язково враховуватися при оцінці ризику впливу ЕМП на населення.

Біологічний ефект ЕМП в умовах тривалого багаторічного впливу накопичується, у результаті можливий розвиток віддалених наслідків, включаючи дегенеративні процеси центральної нервової системи, рак крові (лейкози), пухлини мозку, гормональні захворювання.

Особливо небезпечні ЕМП можуть бути для дітей, вагітних (ембріон), людей із захворюваннями центральної нервової, гормональної, серцево-судинної системи, аллергиків, людей з ослабленим імунітетом.

7.8.2 Вплив на нервову систему.

Велике число досліджень, і зроблені монографічні узагальнення, дають підставу віднести нервову систему до однієї з найбільш чуттєвих систем в організмі людини до впливу ЕМП. На рівні нервової клітки, структурних утворень по передачі нервових імпульсів, на рівні ізольованих нервових структур виникають

істотні відхилення при впливі ЕМП малої інтенсивності. Змінюється вища нервова діяльність, пам'ять у людей, що мають контакт із ЕМП. Ці особи можуть мати схильність до розвитку стрессорних реакцій. Визначені структури головного мозку мають підвищену чутливість до ЕМП. Зміни проникності гемато-енцефаличного бар'єра може привести до несподіваних несприятливих ефектів. Особливу високу чутливість до ЕМП виявляє нервова система ембріона.

7.8.3 Вплив на імунну систему.

В даний час накопичено досить даних, що вказують на негативний вплив ЕМП на імунологічну реактивність організму. Результати досліджень вчених Росії дають підставу вважати, що при впливі ЕМП порушуються процеси іммуногенеза. Встановлено також, що у тварин, опромінених ЕМП, змінюється характер інфекційного процесу - плин інфекційного процесу обтяжується. Виникнення автоіммунітету зв'язують не стільки зі зміною антигенної структури тканин, скільки з патологією імунної системи, в результаті чого вона реагує проти нормальних тканевих антигенів. Відповідно до цієї концепції. основу всіх автоіммунних станів складає в першу чергу імунодефіцит по клітинній популяції лімфоцитів. Вплив ЕМП високих інтенсивностей на імунну систему організму виявляється в гнітючому ефекті на Т-систему клітинного імунітету. ЕМП можуть сприяти неспецифічному гнобленню іммуногенеза, посиленню утворення антитіл до тканин плоду і стимуляції аутоіммунної реакції в організмі.

7.8.4 Вплив на ендокринну, статеву систему і нейрогуморальну реакцію.

В роботах вчених Росії ще в 60-і роки в трактуванні механізму функціональних порушень при впливі ЕМП ведуче місце приділявся змінам у гіпофіз-надниркові системі. Дослідження показали, що при дії ЕМП, як правило, відбувалася стимуляція гіпофізарно-адреналінової системи, що супроводжувалося збільшенням змісту адреналіну в крові, активацією процесів згортання крові. Було визнано, що однієї із систем, рано і закономірно втягує у відповідну реакцію організму на вплив різних факторів зовнішнього середовища, є система кір-гіпоталамус-гіпофіз-кора наднирників. Результати досліджень підтвердили це положення.

Порушення статевої функції звичайно зв'язані зі зміною її регуляції з боку нервової і нейроендокринної систем. З цим повязані результати роботи з вивчення стану гонадотропної активності гіпофіза при впливі ЕМП. Багаторазове опромінення ЕМП викликає зниження активності гіпофіза. Фактор навколишнього середовища, що впливає на жіночий організм під час вагітності та вплив на ембріональний розвиток, вважається тератогенним. Багато вчених відносять ЕМП до цієї групи факторів. Першорядне значення в дослідженнях тератогенеза має стадія вагітності, під час якої впливає ЕМП. Прийнято вважати, що ЕМП можуть, наприклад, викликати каліцтва, впливаючи в різні стадії вагітності. Найбільш вразливими періодами є

звичайно ранні стадії розвитку зародка, що відповідають періодам імплантації і раннього органогенезу.

Була висловлена думка про можливість специфічної дії ЕМП на статеву функцію жінок, на ембріон. Встановлено, що чутливість ембріона до ЕМП значно вище, ніж чутливість материнського організму, а внутрішньоутробне пошкодження плоду ЕМП може відбутися на будь-якому етапі його розвитку. Результати проведених епідеміологічних досліджень дозволять зробити висновок, що наявність контакту жінок з електромагнітним випромінюванням може привести до передчасних родів, вплинути на розвиток плоду і, нарешті, збільшити ризик розвитку вроджених каліцтв.

7.8.5 Інші медико-біологічні ефекти.

З початку 60-х років проведені широкі дослідження з вивчення здоров'я людей, що мають контакт із ЕМП на виробництві. Результати клінічних досліджень показали, що тривалий контакт із ЕМП у СВЧ діапазоні може привести до розвитку захворювань, клінічну картину якого визначають, насамперед, зміни функціонального стану нервової і серцево-судинної систем. Було запропоновано виділити самостійне захворювання - радіохвильова хвороба. Це захворювання, на думку авторів, може мати три синдроми в міру посилення ваги захворювання:

- астенічний синдром;

- астено-вегетативный синдром;

- гіпоталамічний синдром.

Найбільш ранніми клінічними проявами наслідків впливу Ем-випромінення на людину є функціональні порушення з боку нервової системи, що виявляються насамперед у виді вегетативних дисфункций неврастенічного й астенічного синдрому. Особи, що знаходилися в зоні Ем-випромінення тривалий час, пред'являють скарги на слабість, дратівливість, швидку втомлюваність, ослаблення пам'яті, порушення сну. Нерідко до цих симптомів приєднуються розлади вегетативних функцій. Порушення з боку серцево-судинної системи виявляються, як правило в нейроциркуляторній дистонії: лабільність пульсу й артеріального тиску, схильність до гіпотонії, болю в області серця й ін. Відзначаються також фазові зміни складу периферичної крові (лабільність показників) з наступним розвитком помірної лейкопенії, нейропенії, эритроцитопенії. Зміни кісткового мозку носять характер реактивної компенсаторної напруги регенерації. Працюючі з МП і ЕМП, а також населення, що живе в зоні дії ЕМП скаржаться на дратівливість, нетерплячість. Через 1-3 року з'являється почуття внутрішньої напруженості, метушливість. Порушуються увага і пам'ять. Виникають скарги на малу ефективність сну і на втомлюваність. З огляду на важливу роль кори великих півкуль і гіпоталамуса в здійсненні психічних функцій людини, можна говорити, що тривалий повторний вплив гранично припустимих Ем-випромінення, (особливо в дециметровому діапазоні хвиль), може повести до психічних розладів.

7.9 Як захиститися від ЕМП.

Організаційні заходи щодо захисту від ЕМП.

До організаційних заходів щодо захисту від дії ЕМП відносяться: вибір режимів роботи випромінюючого устаткування, що забезпечує рівень випромінювання, що не перевищує гранично припустимий, обмеження місця і часу перебування в зоні дії ЕМП (захист відстанню і часом), позначення й огородження зон з підвищеним рівнем ЕМП.

Захист часом застосовується, коли немає можливості знизити інтенсивність випромінювання в даній крапці до гранично припустимого рівня. У діючих ДР передбачена залежність між інтенсивністю щільності потоку енергії і часом опромінення.

Захист відстанню ґрунтується на падінні інтенсивності випромінювання, що назад пропорційно квадрату відстані і застосовується, якщо неможливо послабити ЕМП іншими мірами, у тому числі і захистом часом. Захист відстанню покладена в основу зон нормування випромінювань для визначення необхідного розриву між джерелами ЕМП і житловими будинками, службовими приміщеннями і т.п.

Для кожної установки, що випромінює електромагнітну енергію, повинні визначатися санітарно-захисні зони в який інтенсивність ЕМП перевищує ДР. Границі зон визначаються расчетно для кожного конкретного випадку розміщення випромінюючої установки при роботі їх на максимальну потужність випромінювання і контролюються за допомогою приладів. Відповідно до ДСТ 12.1.026-80 зони випромінювання відгороджуються або встановлюються попереджуючі знаки з написами: «Не входити, небезпечно!».

Інженерно-технічні заходи щодо захисту населення від ЕМП.

Інженерно-технічні захисні заходи будуються на використанні явища екранування електромагнітних полів безпосередньо в місцях перебування людини або на заходах щодо обмеження емісійних параметрів джерела полючи. Останнє, як правило, застосовується на стадії розробки виробу, що служить джерелом ЕМП.

Для екранування оглядових вікон, вікон приміщень, заскління стельових ліхтарів, перегородок застосовується металізоване скло, що володіє властивостями, що екранують. Така властивість скла додає тонка прозора плівка або окислів металів, найчастіше олова, або металів - мідь, нікель, срібло і їхні сполучення. Плівка володіє достатньої оптичної прозорість і хімічна стійкість. Будучи нанесеної на одну сторону поверхні скла вона послабляє інтенсивність випромінювання в діапазоні 0,8 – 150 див на 30 дб (у 1000 разів). При нанесенні плівки на обох поверхонь скла ослаблення досягає 40 дб (у 10000 разів).

Для захисту населення від впливу електромагнітних випромінювань у будівельних конструкціях як захисні екрани можуть застосовуватися металева сітка, металевий лист чи будь-яке інше провідне покриття, в тому числі і спеціально розроблені будівельні матеріали. В ряді випадків досить використання заземленої металевої сітки, що поміщається під лицювальний чи штукатурний шар. Як екрани можуть застосовуватися також різні плівки і тканини з металізованим покриттям.

В останні роки в якості радіоекрануючих матеріалів одержали металізовані тканини на основі синтетичних волокон. Їх одержують методом хімічної металізації (з розчинів) тканин різної структури і щільності. Існуючі методи одержання дозволяють регулювати кількість наносимого металу в діапазоні від сотих часток до одиниць мкм і змінювати поверхневий питомий опір тканин від десятків до часток Ом. Текстильні матеріали, що екранують, мають малу товщину, легкістю, гнучкістю; вони можуть дублюватися іншими матеріалами (тканинами, шкірою, плівками), добре сполучаються зі смолами і латексами.

Загальноприйняті терміни і скорочення:

А/м ампер на метр – одиниця виміру напруженості магнітного поля
БС Базова станція системи стільникового радіозв'язку
В/м вольт на метр – одиниця виміру напруженості електричного поля
ВДТ відеодисплейний термінал
ТПР тимчасово припустимий рівень
ВООЗ Всесвітня Організація Охорони здоров'я
Вт/м^2 ват на квадратний метр – одиниця виміру щільності потоку енергії
ДСТ Державний Стандарт
Гц герц – одиниця виміру частоти
ЛЕП лінія електропередачі
МГц мегагерц – одиниця кратна Гц, дорівнює 1000000 Гц
мкТл мікротесла – одиниця кратна Тл, дорівнює 0,000001 Тл
МП магнітне поле
МП ПЧ магнітне поле промислової частоти
НЕМВ неіонізуюче електромагнітне випромінювання
ДР допустимий рівень
ПК персональний комп'ютер
ЗМП змінне магнітне поле
ЩПЕ щільність потоку енергії
ПРТО передавальний радіотехнічний об'єкт
ПЧ промислова частота, дорівнює 50 Гц
ПЕОМ персональна електронно-обчислювальна машина
РЛС радіолокаційна станція
РТПЦ радіотехнічний передавальний центр
Тл тесла – одиниця виміру магнітної індукції, щільності потоку магнітної індукції
ЕМП електромагнітне поле
ЕП електричне поле

Джерела посилань

1. Алексеева И. Возникновение идеологии информационного общества // Информационное общество. Вып. 1. М., 1999. То же [on-line]. Метод доступа: <http://www.iis.ru/events/19981130/alexeeva.ru.html>
2. Арефьев П.Г. Интеграция российского академического сообщества в глобальные коммуникации // Социологический журнал. 2001. N 2. То же [on-line]. Метод доступа: http://www.nir.ru/Socio/scipubl/sj/sj2-01aref.html
3. Бодрийяр Ж. Система вещей. – М., 1995.
4. Гейтс Б. Бизнес со скоростью мысли. Изд. 2. М.: ЭКСМО-Пресс, 2001
5. Генисаретский О. Навигатор: методологические расширения и продолжения. М.: Путь,]
6. Даниел. Б. Грядущее постиндустриальное общество. – М., 1999.– 783 с.2002
7. Диббелл Дж. Конец виртуального сообщества? [On-line]. Метод доступа: <http://www.intellectualcapital.ru/iss3-1/icopin1-1.htm>
8. Емелин В. Информационные технологии в контексте постмодернистской философии: Автореферат дисс. … кандидата философских наук. М.: МГУ, 1999. То же [on-line]. Метод доступа: <http://www.geocities.com/emelin_vadim/abstract.htm>
9. Зуев С.Э. Измерения информационного пространства (политики, технологии, возможности) // Музей будущего: информационный менеджмент / Сост. А.В.Лебедев. М.: Прогресс-Традиция, 2001. - С.230-250. То же [on-line]. Метод доступа: <http://www.future.museum.ru/part01/010601.htm>
10. Иванов Д.В. Виртуализация общества. СПб.: "Петербургское Востоковедение", 2000. То же [on-line]. Метод доступа: <http://m16.medport.ru/USSR/chapters/society.htm>
11. Ильин И.П. Постструктурализм. Деконструктивизм. Постмодернизм.– М., 1996
12. Иванов Д.В. Феномен компьютеризации как социологическая проблема // Проблемы теоретической социологии. Вып. 3. СПб.: Издательство Санкт-Петербургского университета, 2000.
13. Кастельс М. Информационная эпоха: экономика, общество и культура. М.: ГУ ВШЭ, 2000
14. Кастельс М., Киселева Э. Россия в информационную эпоху // Мир России. 2001. N 1.
15. Кастельс М., Киселева Э. Россия и сетевое сообщество // Мир России. 2000. N 1.] Лиотар Ж. -Ф. Состояние постмодерна. – М., 1998
16. Кузнецов М.М. Виртуальная реальность: взгляд с точки зрения философа // Виртуальная реальность: Философские и психологические аспекты. – М., 1997.
17. Паринов С. Информационное общество: контуры будущего // Аудиториум. [On-line]. Метод доступа: <http://www.auditorium.ru/v/vconf.php?a=vconf&c=getForm&r=thesisDesc&id_thesis=54>>
18. Паринов С. Истоки Интернет-цивилизации. // Интернет. 1999. N 15. То же [on-line]. Метод доступа: http://ok.msk.ru/gagin/internet/15/31.html, То же: <http://rvles.ieie.nsc.ru/parinov/net-istoki.htm>
19. Паринов С. Онлайновые сообщества: методы исследования и практическое конструирование. Автореферат дисс. … доктора технических наук. Новосибирск, 2000. То же [on-line]. Метод доступа:
20. Поппер К.Р. Открытое общество и его враги. В 2-х томах. М.: Феникс, Международный фонд "Культурная инициатива", 1992
21. Розин В.М. Виртуальная реальность как форма современного дискурса // Виртуальная реальность: Философские и психологические аспекты. – М., 1997.; Розин В.М. На пороге нового мира (опыт методологического осмысления).// Аналитический альманах "Россия и мир: политические реалии и перспективы".– № 15.
22. Современные представления об информационном обществе / Русский Гуманитарный Интернет-Университет.
23. Тираспольский Л., Новиков В. Духовный смысл интернета.– http://www.isn.ru/info/seminar-doc/Novikov.doc
24. Тоффлер Э. Шок будущего. М.: АСТ, 2001
25. Тоффлер О. Смещение власти: знание, богатство и принуждение на пороге XXI века. – М.: Изд-во АН СССР, 1991
26. Тоффлер Э., Тоффлер Х. Создание новой цивилизации. Политика третьей волны // Центральная Азия и культура мира. 1998. N 2-3 (5-6). Бишкек, 1998. То же [on-line]. Метод доступа: <http://www.freenet.bishkek.su/jornal/n5/JRNAL511.htm>
27. Хантингтон С.Ф. Двадцать лет спустя: Будущее третьей волны. [On-line]. Метод доступа: <http://www.russ.ru/journal/peresmot/97-12-29/hantin.htm>
28. Цвылев Р.И., Постиндустриальное развитие. Уроки для России. М.: Наука, 1996
29. Шрадер Х. Глобализация, (де)цивилизация и мораль // Журнал социологии и социальной антропологии. Том II. N 2. СПб., 1998. То же [on-line]. Метод доступа: <http://www.soc.pu.ru:8101/publications/jssa/1998/2/6schrad.html>
30. Штихве Р. К генезису мирового общества. Инновации и механизмы // Журнал социологии и социальной антропологии. Том III. N 3. СПб., 1999.
31. Castells M. The Information Age: Economy, Society and Culture. Vol. I. The Rise of the Network Society. Blackwell Publishers. Maiden, Oxford, 1996
32. Castells M. The Rise of the Network Society. London, Blakwell Publishers, 1996
I in the Sky: Visions of the Information Future / Ed. by Alison Scammell. Aslib, 1999
33. Information Insights: Case Studies in Information Management / Ed. by Sylvia Simmons. Aslib, 1999
34. Masuda Y. Managing in the Information Society: Releasing Synergy Japanese Style. Oxford. 1990
35. Rheingold H. The Virtual Community: Homesteading on the Electronic Frontier. Reading, MA: AddisonWesley, 1993

36. Toffler A. Future Shock. Bantam Books, 1991
37. Toffler A. Powershift. Bantam Books, 1991
38. Toffler A. The Third Wave. L., 1981
39. <http://www.soc.pu.ru:8101/publications/jssa/1999/3/5stichw.html>
40. <http://dll.botik.ru/libr/cit/maclu.koi8.html>
41. <http://www.i-u.ru/biblio/arhiv/articles/cshadrin_spoio/default.asp>
42. <http://kovalevsky.webs.com.ua/publ.htm>
43. <http://www.i-u.ru/biblio/arhiv/articles/cshadrin_spoio/default.asp>
44. <http://rvles.ieie.nsc.ru/~parinov/autoref.htm>
45. http://www.isu.org.ua/pages/projects.html
46. www.refine.org.ua/pageid-4110-2.html
47. Фонд "Інформаційне суспільство України"
Україна, 01034, м. Київ, вул. Паторжинського 6
Тел/Факс: (+380 44) 502 - 00 –

48. Комп'ютер в школі та сім'ї №8, 2005, с3-7.

ДОДАТОК.

РЕКОМЕНДАЦІЇпарламентських слухань з питань розвитку інформаційного суспільства в Україні.

Учасники парламентських слухань з питань розвитку інформаційного суспільства в Україні, які відбулися 21 вересня 2005 долі, відмічають, що ці слухання викликали велику заінтересованість громадськості, наукових і освітянських установ, органів державної влади та органів місцевого самоврядування, а також відповідних міжнародних організацій, предметом діяльності яких є розбудова інформаційного суспільства.

Учасники парламентських слухань вважають, що в Україні є необхідний історичний та сучасний досвід для розвитку інформаційного суспільства, зокрема:

ще на початку 50-х років XX століття в Україні було створено третій у світі комп'ютер (після США та Великобританії), сформоване всесвітньо відому школу кібернетики та обчислювальної техніки під керівництвом академіків Лебедєва С.А. і Глушкова В.М.,
започатковано наукові напрями - штучний інтелект, багатопроцесорні електронні обчислювальні машини, теорія самоорганізації, системний аналіз та інші, завдяки яким світова кібернетика піднялася на новий якісний рівень;

сформовано правові засади побудови інформаційного суспільства; прийнято закони України "Про Концепцію Національної програми інформатизації" (75/98-ВР) та "Про Національну програму інформатизації" (74/98-ВР), інші нормативно-правові акти, які регулюють суспільні відносини щодо створення інформаційних електронних ресурсів, захисту інтелектуальної власності на ці ресурси, впровадження електронного документообігу, захисту інформації тощо;

Україна має висококваліфікований кадровий потенціал у інформаційній сфері, постійно зростаючий та поновлюваний парк комп'ютерної техніки, сучасні системи та засоби телекомунікацій, зв'язку, високу ступінь інформатизації банківської сфери.

Ці та інші передумови дозволяють вважати, що вітчизняний ринок інформаційно-комунікаційних технологій перебуває в стані
активного становлення та за певних розумів може стати фундаментом розвитку інформаційного суспільства в Україні.

Разом з тім учасники парламентських слухань зазначають, що стан розбудови інформаційного суспільства в Україні порівняно із світовими тенденціями є недостатнім і не відповідає потенціалу та можливостям України, оскільки:

відсутні національна стратегія розвитку інформаційного суспільства в Україні та план дій щодо її реалізації;

немає координації зусиль державного і приватного секторів для ефективного використання наявних ресурсів;

ефективність використання фінансових, матеріальних, кадрових ресурсів, спрямованих на виконання Національної програми інформатизації (74/98-ВР), впровадження інформаційно-комунікаційних технологій у соціально-економічну сферу, зокрема в сільське господарство, є низькою;

є відставання у впровадженні технологій електронного бізнесу, електронних бірж та аукціонів, електронних депозитаріїв, використанні безготівкових розрахунків за товари та послуги тощо;

рівень інформатизації окремих галузей економіки, деяких регіонів країни є низьким;

розвиток нормативно-правової бази інформаційної сфери є недостатнім;

створення національної інформаційної інфраструктури для надання органами державної влади та органами місцевого самоврядування юридичним і фізичним особам інформаційних послуг з використанням Інтернету відбувається повільно;

рівень комп'ютерної грамотності населення єнедостатнім, впровадження нових методів навчання із застосуванням сучасних інформаційно-комунікаційних технологій - повільним;

рівень інформаційної представленості України в Інтернет-просторі є низьким, а присутність в Інтернеті україномовних інформаційних ресурсів - недостатньою;

рівень державної підтримки виробництва засобів інформатизації, програмних засобів та впровадження інформаційно-комунікаційних технологій не забезпечує всіх потреб економіки і суспільного життя;

спостерігаються нерівномірність забезпечення можливості доступу населення до комп'ютерних та телекомунікаційних засобів, поглиблення "інформаційної нерівності" між окремими регіонами, галузями економіки та різними верствами населення;

не вирішуються в повному обсязі питання захисту авторських прав на програмну продукцію, відсутні системні державні рішення, спрямовані на створення національних структур (центрів, технополісів і технопарків) з розробки конкурентоздатного програмного забезпечення.

Враховуючи світовий і вітчизняний досвід з розбудови інформаційного суспільства і визнаючи необхідність його подальшого розвитку в Україні з метою підвищення конкурентоспроможності країни, якості життя населення, результативності науки, якості освіти й охорони здоров'я, а також забезпечення створення нових робочих місць та надання можливостей для реалізації здібностей кожною людиною, учасники парламентських слухань п р о п о н у ю т ь:

Визнати розвиток інформаційного суспільства в Україні та впровадження новітніх інформаційно-комунікаційних технологій в усі сфери суспільного життя й у діяльність органів державної влади та органів місцевого самоврядування одним із пріоритетних напрямів державної політики.

Основними стратегічними цілями розвитку в Україні інформаційного суспільства вважати:

прискорення впровадження новітніх інформаційно-комунікаційних технологій в усі сфери суспільного життя, економіку України й у діяльність органів державної влади та органів місцевогосамоврядування;

забезпечення комп'ютерної грамотності населення, насамперед шляхом створення освітньої системи, орієнтованої на використаннянових інформаційно-комунікаційних технологій у формуванні всебічно розвиненої особистості;

створення національної інформаційно-комунікаційної інфраструктури та інтеграцію її із світовою інфраструктурою;

державну підтримку економічного зростання нових "електронних" секторів економіки (торгівлі, надання комунальних і банківських послуг тощо), вирішення нормативно-правових питань щодо електронної взаємодії;

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

збереження культурної спадщини України шляхом електронного її документування;

державну підтримку використання новітніх інформаційно-комунікаційних технологій засобами масової інформації;

широке використання інформаційно-комунікаційних технологій для удосконалення державного управління, відносин між державою і громадянами, становлення електронних форм спілкування між державними органами і фізичними та юридичними особами;

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

захист інформаційних прав громадян, насамперед щодо доступності інформації, захисту інформації про особу, підтримку демократичних інститутів, удосконалення правового урегулювання питань інтелектуальної власності та мінімізації ризику інформаційної нерівності;

удосконалення законодавства з регулювання інформаційних відносин;

удосконалення засобів інформаційної безпеки в умовах широкого використання новітніх інформаційно-комунікаційних технологій.

З метою забезпечення розвитку інформаційного суспільства в Україні визначити стратегічними такі напрями і р е к о м е н д у в а т і:

1. Розробка та реалізація національної стратегії розвитку інформаційного суспільства в Україні

1) Президенту України розглянути можливість:

визнання розвитку в Україні інформаційного суспільства та впровадження новітніх інформаційно-комунікаційних технологій у усіх сферах суспільного життя, діяльності органів державної влади та органів місцевого самоврядування одним із пріоритетів державної політики;

утворення при Президентові України консультативно-дорадчого органу - Національної заради з питань розвитку інформаційного суспільства;

включення основних питань з розбудови інформаційного суспільства в Україні до щорічних послань Президента України до Верховної Заради України про внутрішнє і зовнішнє становище України;

спрямування діяльності певного центрального органу виконавчої влади на проведення державної політики з розвитку інформаційногосуспільства в Україні;

2) Верховній Раді України:

забезпечити першочерговий розгляд відповідних законодавчих ініціатив з метою створення цілісної законодавчої системи з питань розвитку інформаційного суспільства;

ініціювати заходи із створення єдиного парламентського інформаційного простору для забезпечення ефективного міжпарламентського співробітництва;

3) Кабінету Міністрів України:

розробити із залученням представників наукових установ і громадських організацій, провідних фахівців та підприємців сфери інформаційно-комунікаційних технологій національну стратегію розвитку інформаційного суспільства в Україні та план дій з її реалізації, забезпечити включення основних питань з розбудови інформаційного суспільства в Україні до програм діяльності Кабінету Міністрів України, проектів державних програм економічного і соціального розвитку України;

провести роботу щодо удосконалення інформаційного законодавства України, зокрема стосовно приведення його в відповідність із правилами в цій сфері, визначеними міжнародно-правовими актами;

розробити концепцію інформаційного законодавства України, яка регулюватиме послідовність підготовки відповідних нормативно-правових актів, їх склад та змістовні вимоги до цих документів, пропозиції щодо внесення змін до цивільного, адміністративного і кримінального законодавства, пов'язаних з урахуванням особливостей розвитку інформаційного суспільства вУкраїні;

розробити проект інформаційного кодексу, проекти законів: про інформацію (нова редакція); про Національну депозитарну систему та особливості електронного обігу ринку цінних паперів в Україні (нова редакція); про внесення змін до Національної програми інформатизації (74/98-ВР) стосовно визначення стратегічних напрямів розвитку інформаційного суспільства і вдосконалення механізмів реалізації державної політики в цій сфері, про програму впровадження електронного документообігу, здійснення експортно-імпортних операцій, сертифікаційних процедур з використанням електронного цифрового підпису; про електронну торгівлю, про охорону баз даних, про дистанційне навчання, про надання медичних послуг із застосуванням інформаційно-комп'ютерних технологій, про електронні послуги (щодо надання органами державної влади та органами місцевого самоврядування юридичним та фізичним особам інформаційних послуг з використанням Інтернету), про встановлення відповідальності за незаконне розповсюдження рекламних електронних повідомлень;

забезпечити безумовне виконання норми статті 9 Закону України "Про Національну програму інформатизації" (74/98-ВР) стосовно щорічного подання на розгляд Верховної Заради України разом з проектом Закону України про Державний бюджет України на наступний рік доповіді про стан інформатизації в Україні, завдань Національної програми інформатизації на наступні три роки, програми завдань (робіт) з інформатизації на наступний бюджетний рік із визначенням джерел фінансування;

розглянути можливість включення завдань з розвиткуінформаційного суспільства до міжнародно-правових договорів щодо науково-технічного співробітництва та міжнародної технічної допомоги;

забезпечити уточнення змісту та завдань державних наукових і науково-технічних програм з пріоритетних напрямів розвитку науки і техніки з метою актуалізації виконання заходів з розвитку інформаційного суспільства в Україні, сприяння підвищенню конкурентоспроможності вітчизняних інформаційно-комунікаційних технологій;

доручити Державному комітету України з питань технічного регулювання та споживчої політики розробити та впровадити нові національні стандарти та інші нормативні документи, технічні регламенти з питань інформаційно-комунікаційних технологій, гармонізувавши їх з відповідними міжнародними документами, зокрема електронного документа, електронного видання, у тому числі електронних підручників, навчальних посібників та засобів навчання;

доручити Національній академії наук України, Міністерству освіти і науки України, галузевим академіям наук внести пропозиції щодо забезпечення розширення участі українських вчених у міжнародних міждисциплінарних дослідженнях з питань інформаційного суспільства та впровадження новітніх інформаційно-комунікаційних технологій;

доручити Державному комітету статистики України забезпечити організацію і проведення державних статистичних спостережень за процесами розвитку інформаційного суспільства в Україні, узгодивши їх з міжнародними стандартами і методологією та підготувати пропозиції щодо внесення відповідних змін до Стратегії розвитку державної статистики на період до 2008 долі, затвердженої Постановою Кабінету Міністрів України від 13 липня 2004 долі N 910 (910-2004-п).

2. Розвиток інформаційної інфраструктури

Кабінету Міністрів України:

1) забезпечити сприятливі умови для:

створення та розвитку національної, галузевих і регіональних інформаційних систем, мереж та електронних ресурсів, у тому числі електронної інформаційної системи "Електронний Уряд"; інтегрованих інформаційно-аналітичних систем органів державної влади та органів місцевого

самоврядування, зокрема в сфері охорони здоров'я, освіти, науки, культури, довкілля;

становлення та розвитку національної системи супутникового зв'язку, ефірного та кабельного цифрового телебачення, прискорення переходу телерадіомовлення на цифрові технології, оптимізацію використання радіочастотного ресурсу, призначеного для телерадіомовлення;

розвитку національного сегмента мережі Інтернет, впровадженнясистем радіодоступу до цієї мережі в населених пунктах України,передусім - у центрах колективного доступу;

створення на основі фундаментальних та прикладних досліджень вітчизняними виробниками новітніх конкурентоспроможних інформаційно-комунікаційних технологій, засобів інформатизації і комп'ютерних програм, зокрема з відкритими кодами; підтримки діяльності спеціалізованих бізнес-інкубаторів, технопарків, центрів високих інформаційних технологій та інших інноваційних структур;

прискорення робіт, пов'язаних із розробкою, створенням та застосуванням суперкомп'ютерних систем;

сприяння розвитку підприємницької діяльності в сфері інформаційно-комунікаційних технологій, зокрема формування системи адміністративних, правових і економічних механізмів, які стимулюватимуть попит на інформаційну продукцію, залучення інвестицій в інформаційно-комунікаційні технології; розвиткуконкуренції, просування вітчизняної продукції на міжнародний ринок; забезпечення оптимізації митного та податкового законодавства, при цьому розглянувши можливість зміни порядку проведення амортизаційних відрахувань на програмні, комп'ютерні та телекомунікаційні засоби і спрощення процедури тимчасового ввезення інноваційної продукції із застосуванням інформаційно-комунікаційних технологій;

активізації впровадження платіжних карток для безготівкових розрахунків за придбані товари, виконані роботи та надані послуги;

створення в електронній формі фондів архівів, бібліотек, музеїв та закладів культури, формування відповідних інформаційно-бібліотечних та інформаційно-пошукових систем з історії, культури, народної творчості, сучасного мистецтва України тощо, а також забезпечення широкого доступу населення до зазначених систем та ресурсів, зокрема шляхом розвитку систем електронних інформаційних ресурсів з відкритим доступом;

виконання зобов'язань щодо міжнародного співробітництва, спрямованого на розвиток інформаційної інфраструктури та забезпечення розширення участі України у відповідних міжнародних ініціативах;

2) доручити:

Міністерству транспорту та зв'язку України розробити державнупрограму розвитку телекомунікацій, передбачивши, зокрема, виконання завдань переходу на цифрове телерадіомовлення, у тому числі кабельне, підвищення якості послуг зв'язку і доступу до Інтернету, становлення та розвиток національної системи супутникового зв'язку, широке застосування безпроводових технологій доступу до телекомунікаційних мереж, прискорення переходу на цифрові телекомунікаційні технології;

Міністерству освіти і науки України та Національній академії наук України розглянути питання формування державної програми створення високопродуктивних засобів обчислювальної техніки, розробити концепцію та проект створення в Україні міжвідомчого суперкомп'ютерного центру, зокрема комп'ютерної інфраструктури на основі Grid-технологій.

3. Забезпечення повсюдного доступу до телекомунікаційних послуг

1) Кабінету Міністрів України:

сприяти створенню спеціалізованих бізнес-інкубаторів, технопарків, технополісів, центрів високих інформаційних технологій та інших інноваційних структур з інформаційно-комунікаційних технологій;

забезпечити створення в усіх населених пунктах України можливостей для доступу до Інтернету, зокрема шляхом розбудови мережі пунктів колективного доступу;

провести конверсію радіочастотного ресурсу на користь цивільних користувачів;
визначити стратегію розвитку універсальних телекомунікаційних послуг, створити фонд універсальних послуг для забезпечення доступу малозабезпечених верств населення до цих послуг, розробити юридичний та фінансово-економічний механізми функціонування зазначеного фонду;

2) Національній комісії з питань регулювання зв'язку України:

завершити створення нормативної бази, формування якої передбачено Законом України "Про телекомунікації" (1280-15);
визначити найбільш сприятливі технічні, організаційні,економічні і комерційні умови взаємопідключення телекомунікаційних мереж різних операторів, розробивши методику формування тарифів за доступ до телекомунікаційних мереж;
забезпечити прозорість механізмів розподілу радіочастотного ресурсу.

4. Стимулювання розвитку послуг для населення та в сфері бізнесу із застосуванням інформаційно-комунікаційних технологій

1) Кабінету Міністрів України:

розробити заходи щодо впровадження механізмів надання органами державної влади та органами місцевого самоврядування юридичним та фізичним особам інформаційних послуг з використанням Інтернету; продовжити роботи зі створення інтегрованих інформаційно-аналітичних систем органів державної влади, зокрема єдиної автоматизованої системи контролю за виконанням Державного бюджету України, елементом якої має стати інформаційно-аналітичнасистема Рахункової палати; забезпечити підвищення ефективності та прозорості державних закупівель, передбачивши здійснення електронних державних закупівель;

урахувати завдання, пов'язані з розвитком інформаційного суспільства в Україні, при підготовці концепції соціальної політики на період до 2015 долі та концепції подальшого реформування соціального захисту населення, передбачивши, зокрема,вжиття заходів, спрямованих на створення сприятливих розумів длявикористання інформаційно-комунікаційних технологій особами з обмеженими фізичними можливостями;

забезпечити розробку та впровадження заходів щодо стимулювання інвестиційної діяльності в сфері інформаційно-комунікаційних технологій;

доручити Міністерству охорони здоров'я України розробити
програму інформатизації охорони здоров'я, передбачивши, зокрема, формування єдиного інформаційного простору системи охорони здоров'я із застосуванням стандартів ведення електронної інформації про пацієнта, розширення надання медичних послуг із застосуванням інформаційно-комп'ютерних технологій;

доручити Міністерству аграрної політики України розробити проект програми впровадження інформаційно-комунікаційних технологій в аграрному секторі економіки;

доручити Міністерству економіки України розробити заходи щодорозвитку і впровадження інформаційно-комунікаційних технологій у сфері бізнесу, передбачивши розробку відповідних технічних регламентів ведення електронного бізнесу;

2) Верховній Раді Автономної Республіки Крим, обласним, Київській і Севастопольській міським радам, Раді міністрів Автономної Республіки Крим, обласним, Київській та Севастопольській міським державним адміністраціям у межах своїх овноважень враховувати в програмах соціально-економічного розвитку регіонів завдання з розвитку інформаційного суспільства.

5. Створення загальнодоступних електронних інформаційних ресурсів

Кабінету Міністрів України:

активізувати роботи зі створення загальнодоступних національних електронних інформаційних ресурсів, зокрема науково-технічної та економічної інформації в електронній формі;

розробити пропозиції щодо законодавчого врегулювання суспільних відносин, пов'язаних із захистом авторських прав стосовно творів в електронній формі, зокрема розміщених у Інтернеті;

організувати розробку і затвердження комплексу науково-технічних програм на період 2006-2010 років, спрямованих на забезпечення розвитку інформаційного суспільства в Україні, зокрема програм та проектів з питань нанофізики та наноелектроніки, розвитку техніки та технологій надвисоких частот, розвитку національних електронних інформаційних ресурсів та інтегрованого знання, створення української лінгвістичної системи та лінгвістичного порталу в Інтернеті;

забезпечити істотне розширення доступу населення до інформаційних ресурсів та систем надання інформаційних послуг органами державної влади та органами місцевого самоврядування із застосуванням Інтернету, зокрема щодо оприлюднення проектів відповідних нормативно-правових актів, впровадження нових форм взаємодії з громадськістю з використаннямінформаційно-телекомунікаційних технологій (стосовно опитувань, консультацій, громадських експертиз тощо);

розробити типове положення про архів електронних документів,
затвердити правила щодо обов'язкового зберігання цих документів;

доручити Міністерству культури і туризму України підготувати пропозиції щодо розвитку електронних бібліотек, збереження культурної спадщини України шляхом її електронного документування та забезпечення розміщення інформації закладів культури України в Інтернеті;

доручити Міністерству освіти і науки України прискорити розробку проекту державної програми стосовно впровадження інформаційно-комунікаційних технологій у сфері освіти і науки, передбачивши заходи із забезпечення комп'ютерної грамотності населення, створення національної науково-освітньої мережі, розбудови єдиного цифрового науково-освітнього простору, централізованого доступу до світових електронних ресурсів та інтеграцію у світовий науково-освітній простір, розробку відповідних навчальних програмних засобів та електронних науково-технічних, освітніх та навчально-методичних ресурсів, зокрема підручників, навчальних посібників, методичних розробок та забезпечення відкритого безкоштовного Інтернет-доступу до цих ресурсів, створених за рахунок коштів Державного бюджету України.

6. Забезпечення інформаційної безпеки

1) Президенту України доручити Раді національної безпеки і оборони України:

проаналізувати стан та перспективи забезпечення інформаційної безпеки як невід'ємної складової національної безпеки України, зокрема виконання віднесених до її повноважень завдань (проектів) Національної програми інформатизації (74/98-ВР);

розробити програму заходів із забезпечення інформаційноїбезпеки України;

підготувати пропозиції щодо вдосконалення нормативно-правової бази в сфері забезпечення інформаційної безпеки, у тому числі щодо складу, послідовності і порядку підготовки відповідних актів;

внести пропозиції щодо підвищення рівня координації діяльності органів виконавчої влади щодо виявлення, оцінки і прогнозування загроз інформаційної безпеки, запобігання цим загрозам та забезпечення ліквідації їх наслідків;

2) Верховній Раді України:

прискорити розгляд проектів законів, які регулюють суспільні відносини та права громадян, пов'язані з інформаційною безпекою, зокрема щодо захисту персональних даних та перехоплення телекомунікацій;

розглянути питання щодо впровадження програмних засобів лінгвістичної підтримки й експертизи законопроектів;

3) Кабінету Міністрів України:

вжити заходів щодо приєднання до Конвенції про захист осібстосовно автоматизованої обробки даних особистого характеру (994_326), прийнятої Радою Європи 28 січня 1981 р;

прискорити підготовку пропозицій щодо внесення змін до законів України в зв'язку з ратифікацією Верховною Радою України Конвенції про кіберзлочинність (994_575), прийнятої Радою Європи 23 листопаду 2001 року;

розглянути питання щодо розробки державної програми з протидії комп'ютерній злочинності;

4) Службі безпеки України:

вжити заходів щодо розвитку інфраструктури систем криптографічного та технічного захисту інформації;

забезпечити подальший розвиток Національної системи конфіденційного зв'язку;

вжити необхідних заходів, у тому числі попереджувального та профілактичного характеру, з протидії комп'ютерній злочинності;

активізувати роботи з розробки та впровадження у виробництво сучасних високошвидкісних засобів криптографічного захисту інформації;

підготувати пропозиції щодо підвищення ефективності координації створення і впровадження спеціальних технічних засобів на телекомунікаційних мережах;

підготувати пропозиції щодо визначення та захисту критичних інформаційних інфраструктур.

7. Доля громадськості в прийнятті рішень

1) Верховній Раді України регулярно проводити "Дні Уряду України" та парламентські слухання з питань розбудови інформаційного суспільства в Україні;

2) Кабінету Міністрів України забезпечити підготовку і подання на розгляд Верховної ради України щорічної національної доповіді про стан розвитку інформаційного суспільства, її опублікування та розміщення в мережі Інтернет;

3) органам державної влади та органам місцевого самоврядування забезпечити оприлюднення інформації про виконання Рекомендацій парламентських слухань з питань розвитку інформаційного суспільства в Україні, залучати представників громадськості до розробки галузевих та регіональних програм (заходів) з питань розвитку інформаційного суспільства;

4) представникам об'єднань громадян та їх спілок здійснювати постійний громадський контроль за виконанням Рекомендацій парламентських слухань з питань розвитку інформаційного суспільства в Україні, а свої пропозиції з цього питання подавати до комітетів Верховної ради України з питань науки й освіти та з питань будівництва, транспорту, житлово-комунального господарства і зв'язку;

5) Комітету Верховної ради України з питань науки й освіти разом з Консультативною радою з питань інформатизації при Верховній Раді України щорічно проводити відповідні слухання або відкриті засідання, на яких розглядати стан виконання Рекомендацій парламентських слухань з питань розвитку інформаційного суспільства в Україні, заслуховуючи відповідну інформацію Кабінету Міністрів України, та про результати слухань і засідань інформувати Верховну Раду України.

ДЕРЖАВНА ПРОГРАМА "Інформаційні та комунікаційні технологіїв освіті і науці" на 2006-2010 роки.

Загальна частина

Однією з найважливіших особливостей нашого години є перехід розвинутих країн світу від постіндустріального до інформаційного суспільства, що зумовлює необхідність вжиття невідкладних заходів із впровадження інформаційних та комунікаційних технологій у сфері освіти і науки. Створення глобальних відкритих освітніх та наукових систем, з одному боку, сприятиме накопиченню наукових знань, а з іншого, розширенню доступу широких верств населення до різноманітних інформаційних ресурсів.

Не менш важливим завданням в умовах інформаційного суспільства є навчити дітей користуватися інформаційними технологіями. Від успішного його вирішення визначальною мірою залежатиме розвиток країни і її місце у світовій спільноті.

Інформаційні та комунікаційні технології становлять вагому частку світового виробництва, що спричиняє глобальний перерозподіляк ринку праці, так і ринку освітніх послуг. Крім того, створення єдиного європейського освітнього простору в рамках Болонського процесу істотно підвищує їх роль в освіті, сприяє розвитку так званих відкритих університетів.

Українське науково-освітнє середовище також не може існувати без інфраструктури національної науково-освітньої телекомунікаційної мережі (УРАН), основним завданням якої є проведення українськими вченими спільних досліджень, налагодження ними кооперативних зв'язків із західними науковими колективами. У удосконаленні телекомунікаційної мережі насамперед заінтересовані українські наукові співтовариства, які працюють у галузях фундаментальної і прикладної науки, де циркулюють потужні потоки даних, що зумовлює необхідність створення сучасних засобів їх обробки. Це, зокрема, медицина, фізика високих енергій ірадіаційна безпеку, радіоастрономія і космічні дослідження, аеродинаміка, геологія і розвідка корисних копалин, океанологія і метеорологія тощо.

Позначка Програми

Метою Програми є створення розумів для розвитку освіти і науки, підвищення ефективності державного управління шляхом впровадження інформаційних та комунікаційних технологій, забезпечення реалізації прав на вільний пошук, одержання, передачу, виробництво і поширення інформації, здійснення підготовки необхідних спеціалістів і кваліфікованих користувачів, сприяння розвитку вітчизняного виробництва високотехнологічної продукції і насамперед - конкурентоспроможних комп'ютерних програм як найважливішої складової інформаційних та комунікаційних технологій сприяння переходу економіки на інноваційний шлях розвитку.

Основні завдання Програми

Програма передбачає виконання комплексу завдань, які повиннізабезпечити:

підвищення загальної інформаційної грамотності населення;

оснащення навчальних закладів сучасним комп'ютерним тателекомунікаційним обладнанням;

впровадження інформаційних та комунікаційних технологій у навчальний процес і проведення наукових досліджень, забезпеченнядоступу до національних і світових інформаційних ресурсів;

розроблення, впровадження та легалізацію програмного забезпечення;

залучення мережевих технічних ресурсів для забезпечення підключення наукових установ та навчальних закладів до Інтернет;

розвиток технологій дистанційного навчання і використання їх для запровадження в Україні системи навчання протягом усього життя;

забезпечення захисту прав інтелектуальної власності (авторів та розробників);

підвищення кваліфікації та перепідготовку кадрів;

розбудову інфраструктури науково-освітньої телекомунікаційної мережі (УРАН), підключення до неї наукових установ, наукових бібліотек, центрів науково-технічної інформації за допомогою каналів передачі даних, інтеграцію її з європейською науково-дослідницькою мережею (GEANT);

розширення мережі електронних бібліотек навчальних закладів та наукових установ;

розроблення систем забезпечення інформаційної безпеки функціонування мереж та інформаційних ресурсів.

Виконання завдань Програми здійснюватиметься з урахуванням стратегії соціально-економічного розвитку регіонів, стану та перспектив розвитку інформаційних і комунікаційних технологій, новітніх досягнень в інформаційній сфері.

Для виконання основних завдань Програми необхідно здійснитизаходи згідно з додатком.

Фінансування Програми

Фінансування Програми здійснюється за рахунок коштів, які щороку передбачаються в державному бюджеті, із залученням інших джерел, у тому числі міжнародної технічної допомоги, внесків заінтересованих міжнародних організацій тощо.

Контроль за використанням бюджетних коштів, передбачених дл забезпечення виконання Програми, здійснюється в порядку, встановленому законодавством.

Очікувані результати

Виконання Програми дасть змогу:

підвищити якість, доступність та конкурентоспроможність національної освіти і науки на світовому ринку праці та освітніхпослуг; надати нові можливості для наукового пошуку татехнологічного розвитку;

підвищити ефективність наукових досліджень, створити умови для ефективного міжнародного наукового співробітництва, розв'язати соціальні проблеми, пов'язані із створенням рівних розумів доступу до освіти і науки;

забезпечити доступ громадян до науково-освітніх ресурсів і створити умови для безперервного навчання протягом усього життя;

підвищити ефективність державного управління за рахунок впровадження і масового поширення інформаційних та комунікаційних технологій;

забезпечити реалізацію права громадян на вільний пошук, одержання, передачу, виробництво і поширення інформації;

забезпечити прискорення інтеграції України до світового науково-освітнього простору

"Окинавская хартия глобального информационного общества. (Окинава, 22 июля 2000 года)

1. Информационно-коммуникационные технологии (ИТ) являются одним из наиболее важных факторов, влияющих на формирование общества XXI века. Их революционное воздействие касается образажизни людей, их образования и работы, а также взаимодействияправительства и гражданского общества. ИТ быстро становятсяжизненно важным стимулом развития мировой экономики. Они такжедают возможность частным лицам, фирмам и сообществам, занимающимсяпредпринимательской деятельностью, более эффективно и творческирешать экономические и социальные проблемы. Перед всеми намиоткрываются огромные возможности.

2. Суть стимулируемой ИТ экономической и социальнойтрансформации заключается в ее способности содействовать людям иобществу в использовании знаний и идей. Информационное общество,как мы его представляем, позволяет людямшире использовать свойпотенциал и реализовывать свои устремления. Для этого мы должныделать так, чтобы ИТ служили достижению взаимодополняющих целейобеспечения устойчивого экономического роста, повышения общественного благосостояния, стимулирования социального согласияи полной реализации их потенциала в области укрепления демократии,транспарентного и ответственного управления, прав человека,развития культурного многообразия и укрепления международного мираи стабильности. Достижение этих целей и решение возникающих проблем потребует разработки эффективных национальных имеждународных стратегий.

3. Стремясь к достижению этих целей, мы вновь подтверждаемнашу приверженность принципу участия в этом процессе: все людиповсеместно, без исключения должны иметь возможность пользоваться преимуществами глобального информационного общества. Устойчивостьглобального информационного общества основывается на стимулирующихразвитие человека демократических ценностях, таких как свободныйобмен информацией и знаниями, взаимная терпимость и уважение кособенностям других людей.

4. Мы будем осуществлять руководство в продвижении усилий правительств по укреплению соответствующей политики и нормативнойбазы, стимулирующих конкуренцию и новаторство, обеспечениеэкономической и финансовой стабильности, содействующихсотрудничеству по оптимизации глобальных сетей, борьбе созлоупотреблениями, которые подрывают целостность сети, посокращению разрыва в цифровых технологиях, инвестированию в людей и обеспечению глобального доступа и участия и этом процессе.

5. Настоящая Хартия является прежде всего призывом ко всемкак в государственном, так и в частном секторах ликвидироватьмеждународный разрыв в области информации и знаний. Солиднаяоснова политики и действий в сфере ИТ может изменить методы нашего взаимодействия по продвижению социального и экономическогопрогресса во всем мире. Эффективное партнерство среди участников, включая совместное политическое сотрудничество, также является ключевым элементом рационального развития информационногообщества.

Использование возможностей цифровых технологий

6. Потенциальные преимущества ИТ, стимулирующие конкуренцию,способствующие расширению производства, создающие и поддерживающиеэкономический рост и занятость, имеют значительные перспективы.Наша задача заключается не только в стимулировании и содействии переходу к информационному обществу, но также и в полнойреализации его экономических, социальных и культурных преимуществ.

Для достижения этих целей важно строить работу на следующих ключевых направлениях:

- проведение экономических и структурных реформ в целяхсоздания обстановки открытости, эффективности, конкуренции и использования нововведений, которые дополнялись бы мерами по адаптации на рынках труда, развитию людских ресурсов и обеспечению социального согласия;
- рациональное управление макроэкономикой, способствующееболее точному планированию со стороны деловых кругов и потребителей, и использование преимуществ новых информационных технологий;
- разработка информационных сетей, обеспечивающих быстрый,надежный, безопасный и экономичный доступ с помощью конкурентных рыночных условий и соответствующих нововведений к сетевым технологиям, их обслуживанию и применению;
- развитие людских ресурсов, способных отвечать требованиям века информации, посредством образования и пожизненного обучения и удовлетворение растущего спроса на специалистов в области ИТ во многих секторах нашей экономики;
- активное использование ИТ в государственном секторе исодействие предоставлению в режиме реального времени услуг, необходимых для повышения уровня доступности власти для всех граждан.

7. Частный сектор играет жизненно важную роль в разработке информационных и коммуникационных сетей в информационном обществе. Однако задача создания предсказуемой, транспарентной инедискриминационной политики и нормативной базы, необходимой для информационного общества, лежит на правительствах. Нам необходимо позаботиться о том, чтобы правила и процедуры, имеющие отношение кИТ, соответствовали коренным изменениям в экономических сделках с учетом

принципов эффективного партнерства между государственным и частным сектором, а также транспарентности и технологической нейтральности. Такие правила должны быть предсказуемыми и способствовать укреплению делового и потребительского доверия. В целях максимизации социальной и экономической выгоды информационного общества мы согласны со следующими основными принципами и подходами и рекомендуем их другим:

- продолжение содействия развитию конкуренции и открытию рынков для информационной технологии и телекоммуникационнойпродукции и услуг, включая недискриминационное и основанное назатратах подключение к основным телекоммуникациям;

- защита прав интеллектуальной собственности наинформационные технологии имеет важное значение для продвижения нововведений, связанных с ИТ, развития конкуренции и широкого внедрения новых технологий; мы приветствуем совместную работу представителей органов власти по защите интеллектуальнойсобственности и поручаем нашим экспертам обсудить дальнейшиенаправления работы в этой сфере;

- важно также вновь подтвердить обязательство правительств использовать только лицензированное программное обеспечение;

- ряд услуг, включая телекоммуникации, транспорт, доставку посылок, имеют важное значение для информационного общества иэкономики; повышение их эффективности и конкурентоспособностипозволит расширить преимущества информационного общества; таможенные и экспедиторские процедуры также важны для развития информационных структур;

- развитие трансграничной электронной торговли путемсодействия дальнейшей либерализации, улучшения сетей и соответствующих услуг и процедур в контексте жестких рамок Всемирной торговой организации (ВТО), продолжение работы в области электронной торговли в ВТО и на других международных форумах и применение существующих торговых правил ВТО к электронной торговле;

- последовательные подходы к налогообложению электронной торговли, основанные на обычных принципах, включая недискриминацию, равноправие, упрощенность и прочие ключевые элементы, согласованные в контексте работы Организации экономического сотрудничества и развития (ОЭСР);

- продолжение практики освобождения электронных переводов от таможенных пошлин до тех пор, пока она не будет рассмотрена вновь на следующей министерской конференции ВТО;

- продвижение рыночных стандартов, включая, например, технические стандарты функциональной совместимости;

- повышение доверия потребителя к электронным рынкам всоответствии с руководящими принципами ОЭСР, в том числе посредством эффективных саморегулирующих инициатив, таких как кодексы поведения, маркировка, другие программы подтверждения надежности, и изучение вариантов устранения сложностей, которые испытывают потребители в ходе трансграничных споров, включая использование альтернативных механизмов разрешения споров;

- развитие эффективного и значимого механизма защиты частной жизни потребителя, а также защиты частной жизни при обработке личных данных, обеспечивая при этом свободный поток информации; а акже - дальнейшее развитие и эффективное функционирование электронной идентификации, электронной подписи, криптографии и других средств обеспечения безопасности и достоверности операций.

8. Усилия международного сообщества, направленные на развитие глобального информационного общества, должны сопровождаться согласованными действиями по созданию безопасного и свободного отпреступности киберпространства. Мы должны обеспечить осуществление эффективных мер - как это указано в Руководящих принципах по безопасности информационных систем ОЭСР - в борьбе с преступностью в компьютерной сфере. Будет расширено сотрудничество стран "Группывосьми" в рамках Лионской группы по транснациональной организованной преступности. Мы будем и далее содействовать установлению диалога с представителями промышленности, развивая, таким образом, успех, достигнутый на недавно прошедшей Парижскойконференции "Группы восьми" "Диалог между правительством и промышленностью о безопасности и доверии в киберпространстве". Необходимо также найти эффективные политические решения актуальных проблем, как, например, попытки несанкционированного доступа и компьютерные вирусы. Мы будем и далее привлекать представителей промышленности и других посредников для защиты важных информационных инфраструктур.

Преодоление электронно-цифрового разрыва

9. Вопрос о преодолении электронно-цифрового разрыва внутри государств и между ними занял важное место в наших национальных дискуссиях. Каждый человек должен иметь возможность доступа кинформационным и коммуникационным сетям. Мы подтверждаем нашу приверженность предпринимаемым в настоящее время усилиям по разработке и осуществлению последовательной стратегии, направленной на решение данного вопроса. Мы также приветствуем то, что и промышленность, и гражданское общество все более склоняются к признанию необходимости преодоления этого разрыва. Мобилизациянаших знаний и ресурсов в этой области является необходимым условием для урегулирования данной проблемы. Мы будем и далее стремиться к эффективному сотрудничеству между правительствами и гражданским обществом, чутко реагирующим на высокие темпы развития технологий и рынка.

10. Ключевой составляющей нашей стратегии должно стать непрерывное движение в направлении всеобщего доступа для всех. Мыбудем и далее:

- содействовать установлению благоприятных рыночных условий, необходимых для предоставления населению услуг в областикоммуникаций;

- изыскивать дополнительные возможности, включая доступ через учреждения, открытые для широкой публики;

- уделять приоритетное внимание совершенствованию сетевого доступа, в особенности в отсталых городских, сельских и отдаленныхрайонах;

- уделять особое внимание нуждам и возможностям людей, пользующихся меньшей социальной защищенностью, людей с ограниченной трудоспособностью, а также пожилых граждан, и активно осуществлять меры, направленные на предоставление им более легкогодоступа;

- содействовать дальнейшему развитию "удобных для пользования", "беспрепятственных" технологий, включая мобильный доступ к сети Интернет, а также более широкое использование бесплатного, общедоступного информационного наполнения и открытых для всех пользователей программных средств, соблюдая при этомправа на интеллектуальную собственность.

11. Стратегия развития информационного общества должнасопровождаться развитием людских ресурсов, возможности которых соответствовали бы требованиям информационного века. Мы обязуемся предоставить всем гражданам возможность освоить и получить навыки работы с ИТ посредством образования, пожизненного обучения и подготовки. Мы будем и далее стремиться к осуществлению этой масштабной цели, предоставляя школам, классам и библиотекамкомпьютерное оборудование, способное работать в режиме реального времени, а также направлять туда преподавателей, имеющих навыки работы с ИТ и мультимедийными средствами. Кроме того, мы будем осуществлять меры по поддержке и стимулированию малых и среднихпредприятий, а также людей, работающих не по найму, предоставляя им возможность подключаться к сети Интернет и эффективно ею пользоваться. Мы также будем поощрять использование ИТ в целях предоставления гражданам возможности пожизненного обучения с применением передовых методик, в особенности тем категориям граждан, которые в противном случае не имели бы доступа кобразованию и профессиональной подготовке.

Содействие всеобщему участию

12. ИТ открывает перед развивающимися странами великолепные возможности. Страны, которым удалось направить свой потенциал в нужное русло, могут надеяться на преодоление препятствий, традиционно возникающих в процессе развития инфраструктуры, более эффективное решение своих насущных задач в области развития, таких как сокращение бедности, здравоохранение, улучшение санитарных условий и образование, а также использование преимуществ быстрого роста глобальной электронной торговли. Некоторые развивающиеся страны уже достигли значительных успехов в этих областях.

13. Тем не менее не стоит недооценивать проблему мирового масштаба, связанную с преодолением существующих различий в области информации и знаний. Мы отдаем должное тому вниманию, которое уделяют этой проблеме многие развивающиеся страны. В действительности, все те развивающиеся страны, которые не успевают за все более высокими темпами развития ИТ, оказываются лишенными возможности в полной мере участвовать в жизни информационного общества и экономике. Этот вопрос особенно остро стоит в тех странах, где распространению ИТ препятствует отставание в развитии основных экономических и социальных инфраструктур, в частности энергетического сектора, телекоммуникаций и образования.

14. Мы признаем, что при решении этой проблемы следует учитывать разнообразие условий и потребностей, которое сложилось в развивающихся странах. Здесь не может быть "уравнительного" решения. И это в свою очередь говорит о той важной роли, которую должны сыграть развивающиеся страны, выдвигая собственные инициативы о принятии последовательных национальных программ с целью осуществления политических мер, направленных на поддержку развития ИТ и конкуренции в этой сфере, а также создания нормативной базы, использование ИТ в интересах решения задач в области развития и в социальной сфере, развитие людских ресурсов, имеющих навыки работы с ИТ, а также с целью поощрения выдвигаемых на локальном уровне инициатив и местного предпринимательства.

Дальнейшее развитие

15. Усилия по преодолению международной разобщенности в решающей степени зависят от эффективного сотрудничества междувсеми участниками. Для создания рамочных условий для развития ИТ важную роль и в дальнейшем будет играть двустороннее и многостороннее сотрудничество. Международные финансовые институты, включая многосторонние банки развития (МБР), особенно Всемирный банк, весьма пригодны для этой цели и могут разрабатывать и осуществлять программы, которые будут способствовать росту и борьбе с бедностью, а также расширять связи, доступ и обучение. Международная сеть телекоммуникаций, ЮНКТАД и ЮНДП и другие соответствующие международные фонды также могут сыграть важную роль. Центральной остается роль частного сектора в продвижении ИТ в развивающихся странах. Он может также существенно способствовать международным усилиям по преодолению цифрового разрыва. НПО, обладающие уникальными возможностями донести идеи до общественности, также могут способствовать развитию человеческих и общественных ресурсов. ИТ глобальна по своей сути и требует глобального подхода.

16. Мы приветствуем уже предпринимаемые усилия по преодолению международного электронно-цифрового разрыва посредством двусторонней помощи в области развития и по

линии международных организаций и частных групп. Мы также приветствуем вклад частного сектора в лице таких организаций, как Глобальная инициатива по ликвидации электронно-цифрового разрыва Всемирного экономического форума (ВЭФ) и Глобальный диалог бизнеса по вопросам электронной торговли (ГДБ), а также Глобальный форум.

17. Как отмечается в Декларации о роли информационных технологий в контексте основанной на знаниях глобальной экономики, которая была принята Экономическим и Социальным Советом ООН (ЭКОСОС) на уровне министров, существует необходимость расширения международного диалога и сотрудничества в целях повышения эффективности программ и проектов в области информационных технологий совместно с развивающимися странами и сведения воедино "наилучшего опыта", а также мобилизации ресурсов всех участников для того, чтобы способствовать ликвидации электронно-цифрового разрыва. "Восьмерка" будет и далее содействовать укреплению партнерства между развитыми и развивающимися странами, гражданским обществом, включая частные фирмы и НПО, фонды и учебные заведения, а также международные организации. Мы будем также работать над тем, чтобы развивающиеся страны в партнерстве с другими участниками могли получать финансовое, техническое и политическое обеспечение в целях создания благоприятного климата для использования информационных технологий.

18. Мы договорились об учреждении Группы по возможностям информационной технологии (Группа ДОТ), чтобы объединить наши усилия в целях формирования широкого международного подхода. Группа ДОТ будет созвана в кратчайшие сроки для изучения наилучших возможностей подключения к работе всех участников. Эта группа высокого уровня в режиме тесных консультаций с другими партнерами и воспринимая потребности развивающихся стран будет:

- активно содействовать диалогу с развивающимися странами, международными организациями и другими участниками для продвижения международного сотрудничества с целью формирования политического, нормативного и сетевого обеспечения, а также улучшения технической совместимости, расширения доступа, снижения затрат, укрепления человеческого потенциала, а также поощрения участия в глобальных сетях электронной торговли;
- поощрять собственные усилия "восьмерки" в целях сотрудничества в осуществлении экспериментальных программ и проектов в области информационных технологий;
- содействовать более тесному политическому диалогу между партнерами и работать над тем, чтобы мировая общественность больше знала о стоящих перед ней вызовах и имеющихся возможностях;
- изучит вопрос о том, какой вклад вносит частный сектор и другие заинтересованные группы, например Глобальная инициатива по ликвидации электронно-цифрового разрыва;
- представит доклад по итогам работы нашим личным представителям до следующей встречи в Генуе.

19. Для выполнения этих задач группа будет изыскивать пути к принятию конкретных мер в указанных ниже приоритетных областях:

формирование политического, нормативного и сетевого обеспечения:

- поддержка политического консультирования и укрепление местного потенциала, с тем чтобы способствовать проведению направленной на создание конкуренции гибкой и учитывающей социальные аспекты политики, а также нормативному обеспечению;
- содействие обмену опытом между развивающимися странами и другими партнерами;
- содействие более эффективному и широкому использованию информационных технологий в области развития, включая такие широкие направления, как сокращение бедности, образование, здравоохранение и культура;
- совершенствование системы управления, включая изучение новых методов комплексной разработки политики;
- поддержка усилий МБР и других международных организаций в целях объединения интеллектуальных и финансовых ресурсов в контексте программ сотрудничества, таких как программа "InfoDev".

улучшение технической совместимости, расширение доступа и снижение затрат:

- мобилизация ресурсов в целях улучшения информационной и коммуникационной инфраструктуры, уделение особого внимания "партнерскому" подходу со стороны правительств, международных организаций, частного сектора и НПО;
- поиск путей снижения затрат для развивающихся стран в обеспечении технической совместимости;
- поддержка программ доступа на местном уровне;
- поощрение технологических исследований и прикладных разработок в соответствии с конкретными потребностями развивающихся стран;
- улучшение взаимодействия между сетями, службами и прикладными системами;
- поощрение производства современной информационно-содержательной продукции, включая расширение объема информации на родных языках.

укрепление человеческого потенциала:

- уделение повышенного внимания базовому образованию, а также расширению возможностей пожизненного обучения с упором на развитие навыков использования информационных технологий;
- содействие подготовке специалистов в сфере информационных технологий и других актуальных областях, а также в нормативной сфере;
- разработка инновационных подходов в целях расширения традиционной технической помощи, включая дистанционное обучение и подготовку на местном уровне;
- создание сети государственных учреждений и институтов, включая школы, научно-исследовательские центры и университеты.

поощрение участия в работе глобальных сетей электронной торговли:

- оценка и расширение возможностей использования электронной торговли посредством консультирования при открытии бизнеса в развивающихся странах, а также путем мобилизации ресурсов в целях содействия предпринимателям в использовании информационных технологий для повышения эффективности их деятельности и расширения доступа к новым рынкам;

- обеспечение соответствия возникающих "правил игры" усилиям в сфере развития и укрепление способности развивающихся стран играть конструктивную роль в определении этих правил.

Дипломатический вестник. 2000. N 8. С. 51 - 56.

Декларация принципов построение информационного общества – глобальная задача в новом тысячелетии.

12 декабря 2003 года

А. Наша общая концепция информационного общества

1. Мы, представители народов мира, собравшиеся в Женеве 10-12 декабря 2003 года для проведения первого этапа Всемирной встречи на высшем уровне по вопросам информационного общества, заявляем о нашем общем стремлении и решимости построить ориентированное на интересы людей, открытое для всех и направленное на развитие информационное общество, в котором каждый мог бы создавать информацию и знания, иметь к ним доступ, пользоваться иобмениваться ими, с тем чтобы дать отдельным лицам, общинам и народам возможность в полной мере реализовать свой потенциал, содействуя своему устойчивому развитию и повышая качество своей жизни на основе целей и принципов Устава Организации Объединенных Наций (995_010) и соблюдая в полном объеме и поддерживая Всеобщую декларацию прав человека (995_015).

2. Наша задача состоит в том, чтобы использовать потенциал информационных и коммуникационных технологий для достижения сформулированных в Декларации тысячелетия (995_621) целей развития, а именно ликвидации крайней нищеты и голода, обеспечения всеобщего начального образования, содействия равенству мужчин и женщин и расширению прав и возможностей женщин, сокращения детской смертности, улучшения охраны материнства, борьбы с ВИЧ/СПИДом, малярией и другими заболеваниями, содействия экологической устойчивости и формирования глобального партнерства в целях развития для обеспечения более мирного, справедливого и процветающего мира. Мы также подтверждаем свою приверженность достижению устойчивого развития и согласованных целей развития, изложенных в йоханнесбургских Декларации и Плане выполнения решений и Монтеррейском консенсусе, а также в других документах соответствующих встреч на высшем уровне в рамках Организации Объединенных Наций.

3. Мы вновь подтверждаем универсальность, неделимость, взаимозависимость и взаимосвязь всех прав человека и основных свобод, включая право на развитие, как это закреплено в Венской декларации (995_504).

Мы вновь подтверждаем также, что демократия, устойчивое развитие и соблюдение прав человека и основных свобод, а также надлежащее государственное управление на всех уровнях являются взаимозависимыми и взаимоукрепляющими. Мы далее решаем укреплять уважение верховенства права в области внешней и внутренней политики.

4. Мы вновь подтверждаем, что мы признаем в качестве необходимого фундамента информационного общества провозглашенное в статье 19 Всеобщей декларации прав человека (995_015) право каждого человека на свободу убеждений и на свободное их выражение; это право включает свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ. Общение является одним из основополагающих социальных процессов, одной из базовых человеческих потребностей и фундаментом любой социальной организации. Оно составляет сердцевину информационного общества.

Каждый, где бы он ни находился, должен иметь возможность участвовать в информационном обществе, и никого нельзя лишить предлагаемых этим обществом преимуществ.

5. Мы вновь подтверждаем далее свою приверженность положениям статьи 29 Всеобщей декларации прав человека (995_015), согласно которым каждый человек имеет обязанности перед обществом, в котором только и возможно свободное и полное развитие его личности, и при осуществлении своих прав и свобод каждый человек должен подвергаться только таким ограничениям, какие установлены законом исключительно с целью обеспечения должного признания и уважения прав и свобод других и удовлетворения справедливых требований морали, общественного порядка и общего благосостояния в демократическом обществе. Осуществление таких прав и свобод ни в коем случае не должно вступать в противоречие с целями и принципами Организации Объединенных Наций. Тем самым мы будем содействовать созданию информационного общества, в котором уважается достоинство человеческой личности.

6. В соответствии с духом настоящей Декларации мы вновь заявляем о своей решимости соблюдать принцип суверенного равенства всех государств.

7. Мы сознаем, что наука играет центральную роль в развитии информационного общества. Многие компоненты информационного общества являются результатом научно-технических достижений, ставших возможными благодаря совместному использованию результатов исследований.

8. Мы сознаем, что образование, знания, информация и общение составляют основу развития, инициативности и благополучия человеческой личности. Наряду с этим информационные и коммуникационные технологии (ИКТ) оказывают огромное влияние практически на все аспекты нашей жизни. Стремительный прогресс этих технологий открывает совершенно новые перспективы достижения более высоких уровней развития. Способность этих технологий ослабить воздействие многих традиционных препятствий, в особенности связанных с временем и расстоянием, впервые в истории дает возможность использовать потенциал этих технологий во благо миллионов людей во всех уголках земного шара.

9. Мы осознаем, что ИКТ следует рассматривать как инструмент, а не как самоцель. При благоприятных условиях эти технологии способны стать мощным инструментом повышения производительности, экономического роста, создания новых рабочих мест и расширения возможностей трудоустройства, а также повышения качества жизни для всех. Они также могут содействовать ведению диалога между народами, странами и цивилизациями.

10. Мы также в полной мере осознаем, что сегодня преимущества революции в области информационных технологий неравномерно распределены между развитыми и развивающимися странами, а также внутри стран. Мы полны решимости превратить этот разрыв в цифровых технологиях в цифровые возможности для всех, прежде всего для тех, кому грозят отставание и дальнейшая маргинализация.

11. Мы привержены идее претворения в жизнь нашей общей концепции информационного общества на благо нынешнего и будущих поколений. Мы сознаем, что молодежь представляет собой будущий трудовой ресурс, играет ведущую роль в создании ИКТ и быстрее других осваивает эти технологии. Поэтому следует предоставить ей возможность учиться, творить, вносить свой вклад, заниматься предпринимательской деятельностью и участвовать в принятии решений. Особое внимание мы должны уделять тем молодым людям, которые пока не имеют возможности в полной мере пользоваться преимуществами, предоставляемыми ИКТ. Мы также признаем необходимым обеспечить соблюдение прав ребенка, равно как и защиту детей и их благополучие при разработке приложений и предоставлении услуг на базе ИКТ.

12. Мы подтверждаем, что развитие ИКТ открывает грандиозные перспективы для женщин, которые должны составлять неотъемлемую часть информационного общества и стать его ключевыми участниками. Мы признаем необходимым обеспечить, чтобы в информационном обществе женщинам предоставлялись все права и возможности и чтобы они в полной мере участвовали на равных основаниях во всех сферах жизни общества и во всех процессах принятия решений. Для этого мы должны включить в основные направления нашей деятельности принцип равноправия женщин и мужчин и применять ИКТ как инструмент для достижения этой цели.

13. При построении информационного общества мы должны уделять первоочередное внимание особым потребностям маргинализированных и уязвимых групп общества, в том числе мигрантов, внутренне перемещенных лиц и беженцев, безработных и обездоленных людей, меньшинств и кочевых народов. Мы должны также учитывать особые потребности престарелых и лиц с ограниченными возможностями.

14. Мы преисполнены решимости расширить возможности неимущих, прежде всего проживающих в отдаленных, сельских и маргинализированных городских районах, в отношении доступа к информации и использования ИКТ как инструмента, помогающего им в их усилиях избавиться от нищеты.

15. При становлении информационного общества первоочередное внимание следует уделять особому положению коренных народов, а также сохранению их наследия и культурного достояния.

16. Мы продолжаем уделять особое внимание специфическим потребностям жителей развивающихся стран, стран с переходной экономикой, наименее развитых стран, малых островных развивающихся государств, развивающихся стран, не имеющих выхода к морю, бедных стран с крупной задолженностью, оккупированных стран и территорий, стран, преодолевающих последствия конфликтов, а также стран и регионов с особыми потребностями, равно как и представляющим серьезную угрозу для развития обстоятельствам, в том числе стихийным бедствиям.

17. Мы сознаем, что для создания открытого для всех информационного общества требуются новые формы солидарности, партнерства и сотрудничества между органами государственного управления и другими заинтересованными сторонами, то есть частным сектором, гражданским обществом и международными организациями.

Осознавая, что поставленная в настоящей Декларации масштабная задача - преодоление разрыва в цифровых технологиях и обеспечение гармоничного, справедливого и равноправного развития для всех - потребует твердой решимости всех заинтересованных сторон, мы призываем к цифровой солидарности как на национальном, так и на международном уровне.

18. Ничто в настоящей Декларации не должно истолковываться как посягательство на положения Устава Организации Объединенных Наций (995_010), Всеобщей декларации прав человека (995_015), любых других международных документов или национального законодательства, принятых в поддержку этих документов, как противоречие им, их ограничение или отступление от них.

B. Информационное общество для всех: основные принципы

19. Мы преисполнены решимости, строя информационное общество, обеспечить, чтобы каждый мог воспользоваться возможностями, которые могут предоставить ИКТ. Мы согласны в том, что для решения этих задач все заинтересованные стороны должны работать сообща над расширением доступа к информационным и коммуникационным инфраструктурам и технологиям, а также к информации и знаниям, наращивать потенциал, повышать доверие и безопасность при использовании ИКТ, создавать на всех уровнях благоприятную среду, разрабатывать приложения ИКТ и расширять сферу их применения, содействовать культурному разнообразию и уважать его, признавать роль средств массовой информации, уделять внимание этическим аспектам информационного общества и поощрять международное и региональное сотрудничество. Мы согласны в том, что это - ключевые принципы построения открытого для всех информационного общества.

1) Роль органов государственного управления и всех заинтересованных сторон в содействии применению ИКТ в целях развития

20. Органам государственного управления, а также частному сектору, гражданскому обществу, Организации Объединенных Наций и другим международным организациям надлежит сыграть важную роль в развитии информационного общества, взять на себя за это ответственность и в надлежащих случаях участвовать в процессах принятия решений. Построение информационного общества, ориентированного на интересы людей, является общим делом, требующим сотрудничества и партнерских отношений между всеми заинтересованными сторонами.

2) Информационная и коммуникационная инфраструктура - необходимый фундамент открытого для всех информационного общества

21. Обеспечение подключения является одним из главных факторов построения информационного общества. Предоставление универсального, повсеместного, справедливого и приемлемого в ценовом отношении доступа к инфраструктуре ИКТ и услугам на базе ИКТ составляет одну из задач информационного общества и должно стать целью всех заинтересованных сторон, участвующих в его построении. Обеспечение подключения также предусматривает доступ к услугам энергоснабжения и почтовой связи, который следует обеспечивать в соответствии с национальным законодательством каждой страны.

22. Хорошо развитая инфраструктура информационных и коммуникационных сетей и приложения, отвечающие региональным, национальным и местным условиям, легкодоступные и приемлемые в ценовом отношении, позволяющие в большей степени использовать широкополосную связь и другие инновационные технологии там, где это возможно, способны ускорить социально-экономический прогресс стран и повысить благосостояние всех людей, общин и народов.

23. Политика, создающая на всех уровнях благоприятные условия для стабильности, предсказуемости и добросовестной конкуренции, должна разрабатываться и осуществляться так, чтобы не только в больших масштабах привлекать частные инвестиции в развитие инфраструктуры ИКТ, но и обеспечивать выполнение обязательств по универсальному обслуживанию в тех областях, где не действуют традиционные рыночные механизмы. В находящихся в неблагоприятных условиях районах создание публичных пунктов доступа к ИКТ в таких структурах, как почтовые отделения, школы, библиотеки и архивы, может служить эффективным способом обеспечения универсального доступа к инфраструктуре и услугам информационного общества.

3) Доступ к информации и знаниям

24. Обеспечение каждому возможности иметь доступ к информации, идеям и знаниям и вносить в эти области свой вклад является необходимым элементом открытого для всех информационного общества.

25. Совместному использованию и расширению глобальных знанийв целях развития может способствовать устранение барьеров на пути достижения равноправного доступа к информации для осуществления деятельности в области экономики, в социальной сфере, политике, здравоохранении, культуре, образовании и науке, а также упрощение доступа к информации, являющейся публичным достоянием, в том числе путем обеспечения универсального дизайна и использования ассистивных технологий.

26. Наличие обширного публичного достояния - важнейшая составляющая развития информационного общества, обеспечивающая такие многочисленные преимущества, как получение населением образования, создание новых рабочих мест, инновационная

деятельность, открытие перспектив в хозяйственной сфере и научный прогресс. Информация, относящаяся к публичному достоянию, должна быть легкодоступной в интересах развития информационного общества и должна быть защищена от незаконного присвоения. Следует укреплять публичные учреждения, такие как библиотеки и архивы, музеи, собрания культурных ценностей и другие коллективные пункты доступа, с тем чтобы содействовать сохранению документальных
записей и свободному и равноправному доступу к информации.

27. Доступу к информации и знаниям можно способствовать путем повышения осведомленности всех заинтересованных сторон овозможностях, предоставляемых различными моделями программного
обеспечения, в том числе разрабатываемого отдельными компаниями, программного обеспечения с открытыми кодами и свободно распространяемого программного обеспечения, с тем чтобы усиливать конкуренцию, расширять доступ к ним пользователей и диапазон их
выбора, а также дать всем пользователям возможность решать, какой вариант наилучшим образом удовлетворяет их потребностям.

Приемлемый в ценовом отношении доступ к программномуобеспечению является важным компонентом действительно открытого
для всех информационного общества.

28. Мы стремимся содействовать обеспечению всеобщего и равноправного универсального доступа к научным знаниям и созданию
и распространению научно-технической информации, включая инициативы по организации свободного доступа к научным публикациям.

4) Наращивание потенциала

29. Каждый человек должен иметь возможность овладевать навыками и знаниями, необходимыми для понимания сути информационного общества и базирующейся на знаниях экономики, активного участия в них и полномасштабного использования их
преимуществ.

Грамотность и всеобщее начальное образование являются ключевыми факторами при построении открытого для всех без исключения информационного общества, при этом первоочередное внимание должно уделяться особым потребностям девочек и женщин. С
учетом потребности на всех уровнях в большом числе специалистов в области ИКТ и информатики особого внимания заслуживает наращивание институционального потенциала.

30. Необходимо содействовать применению ИКТ на всех уровнях образования, профессиональной подготовки и развития людских ресурсов с учетом особых потребностей лиц с ограниченными возможностями, а также находящихся в неблагоприятных условиях и уязвимых слоев населения.

31. Непрерывное образование и образование для взрослых, переподготовка, обучение в течение всей жизни, дистанционное
обучение и другие специальные услуги, такие как телемедицина, могут внести решающий вклад в расширение возможностей трудоустройства и содействовать людям в использовании новых перспектив, открываемых ИКТ в отношении традиционных рабочих мест, самозанятости и освоения новых профессий. Необходимым фундаментом
для этого являются информированность и грамотность в области ИКТ.

32. Активную роль в формировании информационного общества должны играть разработчики, издатели и производители контента, а также преподаватели, инструкторы, работники архивов и библиотек и учащиеся, в особенности в наименее развитых странах.

33. Для обеспечения устойчивого развития информационного общества следует наращивать национальный потенциал в области научно-технических и опытно-конструкторских работ в сфере ИКТ.

Наряду с этим партнерские отношения, в первую очередь между развитыми и развивающимися странами и внутри этих групп стран, включая страны с переходной экономикой, в области научно-технических и опытно-конструкторских работ, передачи технологий, производства и использования продуктов и услуг на базе ИКТ, являются важнейшим условием содействия наращиванию потенциала
и всеобщему участию в информационном обществе. Производство продукции ИКТ открывает широкие перспективы для создания материальных благ.

34. Реализация наших общих стремлений, прежде всего к тому, чтобы развивающиеся страны и страны с переходной экономикой стали полноправными членами информационного общества, и позитивный
процесс их интеграции в экономику, базирующуюся на знаниях, во многом зависят от ускорения наращивания потенциала в областиобразования, технологий, ноу-хау и доступа к информации. Эти факторы являются решающими в определении уровня развития и
конкурентоспособности.

5) Укрепление доверия и безопасности при использовании ИКТ

35. Упрочение основы для доверия, включая информационную безопасность и безопасность сетей, аутентификацию, защиту неприкосновенности частной жизни и прав потребителей, является предпосылкой становления информационного общества и роста доверия

со стороны пользователей ИКТ.

Необходимо формировать, развивать и внедрять глобальную культуру кибербезопасности в сотрудничестве со всеми заинтересованными сторонами и компетентными международными организациями. Данные усилия должны опираться на расширяющееся международное сотрудничество. В рамках этой глобальной культуры кибербезопасности важно повышать безопасность и обеспечивать защиту данных и неприкосновенность частной жизни, расширяя при этом доступ и масштаб торговых операций. Кроме того, необходимо принимать во внимание уровень социально экономического развития каждой страны и учитывать связанные с ориентацией на развитие аспекты информационного общества.

36. Признавая принципы универсального и недискриминационного доступа к ИКТ для всех стран, мы поддерживаем деятельность Организации Объединенных Наций, направленную на предотвращение возможности использования ИКТ в целях, которые несовместимы с задачами обеспечения международной стабильности и безопасности и способны оказать отрицательное воздействие на целостность государственных инфраструктур, нанося ущерб их безопасности. Следует предотвращать использование информационных ресурсов и технологий в преступных и террористических целях, соблюдая при этом права человека.

37. Спам представляет для пользователей, сетей и в целом дляИнтернет серьезную проблему, масштабы которой возрастают. Вопросы, касающиеся спама и кибербезопасности, следует рассматривать на соответствующем национальном и международном уровнях.

6) Благоприятная среда

38. Необходимым условием существования информационного общества является благоприятная среда на национальном и международном уровнях. ИКТ следует применять как важный инструмент надлежащего государственного управления.

39. Верховенство права, наряду с благоприятной, прозрачной, способствующей конкуренции, основанной на принципе технологической нейтральности и предсказуемой политической и регламентарной базой, учитывающей национальные особенности, необходимо для создания ориентированного на интересы людей информационного общества. Органы государственного управления должны принимать в надлежащих случаях меры для компенсации неэффективности рыночных механизмов, поддержания добросовестной конкуренции, привлечения инвестиций, содействия развитию инфраструктуры ИКТ и приложений на базе ИКТ, использования в максимальной степени экономических и социальных выгод и учета национальных приоритетов.

40. Жизненно важными дополнительными компонентами относящихся к ИКТ национальных усилий в области развития являются динамичная и благоприятная международная среда, способствующая привлечению прямых иностранных инвестиций, передаче технологий и международному сотрудничеству, в первую очередь в областях финансов, задолженности и торговли, а также полномасштабное и эффективное участие развивающихся стран в принятии решений на мировом уровне. Расширение приемлемой в ценовом отношении возможности глобального подключения может значительно способствовать эффективности этих усилий в области развития.

41. ИКТ, способствуя повышению эффективности и производительности, прежде всего предприятий малого и среднего бизнеса (МСП), являются мощным катализатором экономического роста. В этом отношении развитие информационного общества важно для экономического роста на широкой основе как в развитых, так и в развивающихся странах. Следует поощрять обусловливаемый ИКТ рост производительности и внедрение инноваций в секторы экономики. Справедливое распределение создаваемых благ способствует ликвидации нищеты и социальному развитию. Наиболее благоприятное воздействие будут, вероятно, оказывать те политические стратегии, которые способствуют продуктивным инвестициям и дают возможность предприятиям, в первую очередь МСП, осуществлять перемены, необходимые для извлечения выгоды из применения ИКТ.

42. Для поощрения инновационной деятельности и творчества в информационном обществе важно обеспечивать защиту интеллектуальной собственности; аналогичным образом, широкое распространение, популяризация и совместное использование информации также важны для поощрения инновационной деятельности и творчества. Содействие осознанному участию всех в решении вопросов интеллектуальной собственности и совместном использовании знаний посредством полномасштабного информирования и наращивания потенциала является одним из основополагающих элементов открытого для всех информационного общества.

43. В информационном обществе устойчивому развитию может в наибольшей степени способствовать полномасштабная интеграция относящихся к ИКТ мероприятий и программ в национальные и региональные стратегии развития. Мы приветствуем Новое партнерство в интересах развития Африки (НЕПАД) и призываем международное сообщество поддержать принимаемые в рамках этой инициативы

меры, касающиеся ИКТ, а также аналогичные мероприятия, которые осуществляются в других регионах. Распределение выгод от экономического роста, получаемых благодаря применению ИКТ, способствует ликвидации нищеты и обеспечению устойчивого развития.

44. К важнейшим составляющим построения информационного общества относится стандартизация.

Особое внимание следует уделять разработке и принятию международных стандартов. Разработка и использование открытых, обеспечивающих возможность взаимодействия, недискриминационных и определяемых спросом стандартов с учетом потребностей пользователей и потребителей, - одно из основных условий развития и расширения распространения ИКТ и обеспечения более приемлемого вценовом отношении доступа к ним, прежде всего в развивающихся странах. Международные стандарты имеют целью создание среды, в которой потребители могли бы пользоваться соответствующими услугами в любой точке мира, независимо от применяемой технологии.

45. Управление использованием радиочастотного спектра должно осуществляться в интересах общества, в соответствии с принципом законности, при неукоснительном соблюдении национальных законов и норм, а также соответствующих международных соглашений.

46. Государства настоятельно призываются принимать при построении информационного общества меры, направленные на недопущение и отказ от каких-либо односторонних действий, не соответствующих международному праву и Уставу Организации Объединенных Наций (995_010) и препятствующих полномасштабному обеспечению социально-экономического развития затрагиваемых стран и благосостояния их населения.

47. Поскольку ИКТ постепенно изменяют наши методы работы, основополагающее значение имеет создание защищенных, безопасных и не наносящих ущерба здоровью условий труда, предусматривающих использование ИКТ, при соблюдении всех соответствующих международных норм.

48. Интернет превратился в публичный ресурс глобального масштаба, и управление его использованием должно стать одним из основных вопросов повестки дня информационного общества. Управление использованием Интернет на международном уровне необходимо осуществлять на многосторонней, прозрачной и демократической основе при полномасштабном участии органов государственного управления, частного сектора, гражданского общества и международных организаций.

Это управление должно обеспечивать справедливое распределение ресурсов, способствовать доступу для всех, гарантировать стабильное и защищенное функционирование Интернет с учетом многоязычия.

49. Управление использованием Интернет охватывает как технические вопросы, так и вопросы государственной политики, и в нем должны участвовать все заинтересованные стороны исоответствующие межправительственные и международные организации.

В связи с этим признается, что:

a) политические полномочия по связанным с Интернет вопросам государственной политики являются суверенным правом государств.

Государства имеют права и обязанности в отношении связанных с Интернет вопросов государственной политики международного уровня;

b) частный сектор играет и должен продолжать играть важную роль в развитии Интернет, как в технической, так и в экономической сфере;

c) гражданское общество также играет важную роль в относящихся к Интернет вопросах, в особенности на уровне общин, и должно продолжать играть такую роль;

d) межправительственные организации играют и должны продолжать играть роль, способствующую координации связанных с Интернет вопросов государственной политики;

e) международные организации также играют и должны продолжать играть важную роль в разработке относящихся к Интернет техническихстандартов и соответствующей политики.

50. Вопросы управления использованием Интернет намеждународном уровне следует решать согласованным образом. Мы обращаемся к Генеральному секретарю Организации Объединенных Наций с просьбой учредить рабочую группу по управлению использованием Интернет в рамках открытого и всеобъемлющего процесса, обеспечивающего механизм для полномасштабного и активного участия органов государственного управления, частного сектора и гражданского общества как из развивающихся, так и из развитых стран, в том числе соответствующих межправительственных и международных организаций и форумов, в целях изучения вопроса об управлении использованием Интернет и представления к 2005 году в надлежащих случаях предложений для принятия решения в отношении организации управления использованием Интернет.

7) Приложения на базе ИКТ: преимущества во всех аспектах жизни

51. Использование и развертывание ИКТ должны быть направлены на создание преимуществ во всех аспектах нашей повседневной жизни.

Приложения на базе ИКТ потенциально важны для деятельности органов государственного управления и предоставляемых ими услуг здравоохранения и информации об охране здоровья, образования и профессиональной подготовки, занятости, создания рабочих мест, предпринимательства, сельского

хозяйства, транспорта, охраны окружающей среды и рационального использования природных ресурсов, предотвращения катастроф, для развития культуры, а также для ликвидации нищеты и достижения иных согласованных целей в области развития. Кроме того, ИКТ должны способствовать устойчивости структур производства и потребления и преодолению традиционных барьеров, давая тем самым возможность всем получить доступ на местные и глобальные рынки на более равноправной основе. Приложения ИКТ должны быть удобными для пользователей, доступными для всех, приемлемыми в ценовом отношении, соответствовать местным потребностям благодаря адаптации к местным языкам и культуре и поддерживать устойчивое развитие. Для этого местные органы власти должны играть важную роль в предоставлении услуг на базе ИКТ во благо своих граждан.

8) Культурное разнообразие и культурная самобытность, языковое разнообразие и местный контент

52. Культурное разнообразие - это общее наследие человечества.

Информационное общество должно основываться на уважении культурной самобытности, разнообразия культур и языков, традиций и религий, стимулировать это уважение и содействовать диалогу между культурами и цивилизациями. Популяризация, укрепление и сохранение
различных культур и языков, что отражено в соответствующих документах, принятых Организацией Объединенных Наций, в том числе
во Всеобщей декларации ЮНЕСКО о культурном разнообразии, будут далее обогащать информационное общество.

53. При построении открытого для всех информационного общества приоритет следует отдавать созданию, распространению и сохранению контента на разных языках и в различных форматах, при этом особое внимание необходимо уделять разнообразию предложения творческих произведений и должному признанию прав авторов и деятелей искусств. Необходимо содействовать производству и обеспечению доступности всего контента - образовательного, научного, культурного и развлекательного - на разных языках и в различных форматах. Развитие местного контента, отвечающего
национальным или региональным потребностям, будет способствовать социально-экономическому развитию и стимулировать участие всех заинтересованных сторон, включая жителей сельских, отдаленных и маргинальных районов.

54. Сохранение культурного наследия представляет собой один из важнейших элементов самобытности и самосознания людей и связывает общество с его прошлым. Информационное общество должно всеми соответствующими методами, включая перевод в цифровую форму, собирать и сохранять культурное наследие для будущих поколений.

9) Средства массовой информации

55. Мы вновь подтверждаем нашу приверженность принципамсвободы печати и свободы информации, а также независимости, плюрализма и разнообразия средств массовой информации, которые являются основной составляющей информационного общества. Свобода искать, получать, передавать и использовать информацию для создания, накопления и распространения знаний имеет существенное значение для информационного общества. Мы призываем средства массовой информации ответственно использовать информацию и обращаться с ней, в соответствии с высочайшими этическими и профессиональными стандартами. Традиционные средства массовой информации во всех их видах играют важную роль в информационном обществе, и ИКТ должны способствовать этому. Следует поощрять развитие разнообразных форм собственности на средства массовой информации, в соответствии с национальным законодательством, учитывая при этом соответствующие международные конвенции. Мы вновь подтверждаем необходимость сокращения диспропорций в средствах массовой информации на международном уровне, особенно в том, что касается инфраструктуры, технических ресурсов и развития навыков и умений.

10) Этические аспекты информационного общества

56. В информационном обществе необходимо уважать мир иотстаивать основные ценности, такие как свобода, равенство, солидарность, терпимость, коллективная ответственность и бережное отношение к природе.

57. Мы признаем важность для информационного общества этических норм, которые должны способствовать справедливости, а также поддерживать достоинство и ценность человеческой личности.

Максимально надежную защиту следует обеспечить семье, с тем чтобы дать ей возможность играть в обществе решающую роль.

58. При использовании ИКТ и при создании контента следует уважать права человека и основные свободы других людей, включая неприкосновенность частной жизни и право на свободу мысли, совести и религии, согласно положениям соответствующих международных документов.

59. Все участники информационного общества должны предпринимать соответствующие действия и принимать установленные законодательством меры по предотвращению ненадлежащего использования ИКТ, такого как противоправные деяния и прочие действия на почве расизма, расовой дискриминации,

ксенофобии и связанные с ними проявления нетерпимости, ненависти, насилия, все формы жестокого обращения с детьми, включая педофилию и детскую порнографию, а также торговля людьми и их эксплуатация.

11) Международное и региональное сотрудничество

60. Мы намереваемся в полной мере использовать предоставляемые ИКТ возможности в нашем стремлении достичь согласованных на международном уровне целей в области развития, в том числе содержащихся в Декларации тысячелетия (995_621), атакже отстаивать ключевые принципы, изложенные в этой Декларации.Информационное общество глобально по своей сути, и предпринимаемые на национальном уровне усилия необходимо поддерживать посредством эффективного международного и регионального сотрудничества между органами государственного управления, частным сектором, гражданским обществом и другими заинтересованными сторонами, включая международные финансовые учреждения.

61. Для построения открытого для всех глобального информационного общества мы будем изыскивать и эффективно применять на международном уровне конкретные подходы и механизмы, в том числе оказывать финансовую и техническую помощь. Поэтому, оценивая по достоинству сотрудничество в области ИКТ, которое осуществляется в рамках различных механизмов, мы призываем все заинтересованные стороны обязаться принять "Повестку дня цифровой солидарности", содержащуюся в Плане действий. Мы убеждены в том, что согласованная на мировом уровне цель заключается в содействии преодолению разрыва в цифровых технологиях, расширении доступа к ИКТ, создании цифровых возможностей и использовании заключенного в ИКТ потенциала в интересах развития. Мы признаем желание некоторых заинтересованных сторон создать международный добровольный "Фонд цифровой солидарности" и желание других сторон провести исследования, касающиеся существующих механизмов, а также эффективности и целесообразности создания такого фонда.

62. Региональная интеграция способствует развитию глобального информационного общества и делает необходимым тесное сотрудничество в рамках регионов и между ними. Региональный диалог должен содействовать наращиванию потенциала на национальном уровне и приведению национальных стратегий в соответствие с целями настоящей Декларации принципов с учетом национальных и региональных особенностей. В связи с этим мы призываем международное сообщество поддержать принимаемые в рамках таких инициатив меры, касающиеся ИКТ.

63. Мы принимаем решение оказывать содействие развивающимся странам, НРС и странам с переходной экономикой посредством мобилизации средств из всех источников финансирования, предоставления финансовой и технической помощи и путем создания среды, способствующей передаче технологий, в соответствии с целями настоящей Декларации и Плана действий.

64. Основные сферы компетенции Международного союза электросвязи (МСЭ) в областях ИКТ - содействие в преодолении разрыва в цифровых технологиях, международное и региональное сотрудничество, управление использованием радиочастотного спектра, разработка стандартов и распространение информации - имеютрешающее значение для построения информационного общества.

С. К информационному обществу для всех, основанному на совместном использовании знаний

65. Мы берем на себя обязательство укреплять сотрудничество, с тем чтобы сообща находить решения проблем и выполнять План действий, претворяя в жизнь концепцию открытого для всех информационного общества, основанного на ключевых принципах, содержащихся в настоящей Декларации.

66. Мы берем на себя, далее, обязательство оценивать в количественном отношении процесс преодоления разрыва в цифровых технологиях и осуществлять наблюдение за этим процессом, учитывая различия в уровнях развития, с тем чтобы достичь согласованных на международном уровне целей в области развития, в том числе содержащихся в Декларации тысячелетия (995_621), и определять эффективность инвестиций и усилий в сфере международного сотрудничества для построения информационного общества.

67. Мы твердо убеждены, что все вместе мы вступаем в новую эру огромных возможностей - эру информационного общества и расширения сферы человеческого общения. В этом зарождающемся обществе информацию и знания можно производить, обмениваться ими, совместно их использовать и передавать по всем сетям мира. Если мы предпримем необходимые действия, вскоре все люди смогут сообща построить новое информационное общество, основанное на совместном использовании знаний, на базе глобальной солидарности и более полного взаимопонимания между народами и странами. Мы верим, что эти меры откроют путь к дальнейшему развитию общества, действительно основанного на знаниях.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Технічний коледж Тернопільського Державного Технічного Університету ім.І.Пулюя.
Тернопільське вище професійне училище №4 ім М. Паращука.

Семків Юрій Мирославович, Радчик Галина Іванівна

ПРАВОВІ ОСНОВИ РОЗВИТКУ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА ТА БЕЗПЕКА ЛЮДИНИ ПРИ ВИКОРИСТАННІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Навчальний посібник

Автори щиро вдячні за всі повідомлення про помилки та інші недоліки, а також за інформацію про всі зміни.

Підписано до друку 20.01. 2007. Формат 60х84/16. Папір офсетний №1.
Обл. вид. арк. 4,7. Гарнітура Times. Ум. – друк. арк 5,5. Тираж 100.

Друк
ТзОВ "ІНФОТЕХЦЕНТР"
М. Тернопіль, вул. Танцорова, 25
Тел 8(0352) 43-10-52.