ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
Навчально-науковий інститут захисту інформації
Кафедра управління інформаційною та кібернетичної безпекою

Т.М.Мужанова

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ

Навчальний посібник

Київ – 2019

Зміст

Вступ

У навчальному посібнику розглянуто концептуальні засади інформаційної безпеки держави, зокрема наведено основні терміни й визначення у сфері інформаційної безпеки, з'ясовано сутність та класифікації національних інтересів та загроз інформаційній безпеці, відслідковано історію розвитку інформаційної безпеки держави через призму еволюції засобів зв'язку.

У рамках вивчення системи забезпечення інформаційної безпеки України проаналізовано вітчизняну нормативно-правову базу у зазначеній сфері, напрями державної політики інформаційної безпеки, розглянуто структуру та повноваження органів, що забезпечують інформаційну безпеку в Україні. Також висвітлено теоретичні основи кібербезпеки держави, розкрито особливості сучасного стану та перспективи забезпечення кібербезпеки України.

Встановлено сутність понять інформаційного простору, інформаційних ресурсів та інфраструктури держави, проаналізовано проблеми національного інформаційного простору України, розглянуто напрями його розвитку і забезпечення інформаційної безпеки.

ТЕМА 1. Теоретичні та нормативно-правові засади інформаційної безпеки України.

1.1. Інформація: сутність та основні характеристики.

Інформація (від латинського слова «informacio» - роз'яснення, виклад) - це відомості (або їх сукупність) про предмети, явища і процеси оточуючого нас світу. Інформація - це абстрактне поняття. Інформація не існує сама по собі - вона укладена в структурі об'єкта або системи, в знаках і символах, зафіксованих на матеріальних носіях. Інформація проявляється в інформаційних процесах в природі, в суспільстві і техніці, а також в процесі розумової діяльності людини щодо сприйняття навколишньої дійності.

«Відкриття» поняття інформації сучасною наукою відбулося в середині XX століття і, на сьогодні представлено багато підходів до розуміння поняття «інформація», які часто несумісні і протирічать одна одній.

На думку засновника вчення про *кібернетику* Н. Вінера, інформація є інформація, а не матерія і не енергія. З цього визначення випливає, що інформація - не існуючий реально об'єкт, а розумова абстракція, тобто вона є створена людським розумом.

Однією з перших є *статистична теорія інформації*, розроблена К.Шенноном і викладена в серії його робіт в 1948 році. Саме він увів термін «інформація», яку розумів у вузькому технічному аспекті, основний акцент робив на кількісній її оцінці. Недоліком подібного підходу є те, що він абстрагується від осмисленості і цінності інформації для споживача.

Комунікативна концепція розглядає інформацію як сферу спілкування і сферу загальнонаукової рефлексії, передбачає взаємоактуалізацію смислів (а не механічне переміщення інформації) і становить зміст комунікативних процесів.

Функціональна концепція інформації представлена двома різновидами: кібернетичною, яка вважає, що інформація (інформаційні процеси) є у всіх самоврядних (технічних, біологічних, соціальних) системах, і антропоцентристською, у рамках якої інформація інтерпретується як особливість живих, самоврядних систем або ж свідомих істот, як основна передумова і умова оптимального управління.

Атрибутивна концепція використовує більш широке поняття, розуміючи інформацію як віддзеркалення різноманітності в будь-яких об'єктах і процесах, як у живій, так і в неживій природі. При цьому інформація визначається як міра неоднорідності розподілу матерії та енергії в просторі і в часі.

У логіко-семантичних теоріях інформації інформація розглядається як зменшення або подолання невизначеності.

Отже, під інформацією нині розуміють:

– відомості, повідомлення про що-небудь, якими обмінюються люди;

– сигнали, імпульси, образи, що циркулюють у технічних (кібернетичних) пристроях;

– кількісну міру усунення невизначеності (ентропії), міру організації системи;

– відображення різноманітності в будь-яких об'єктах і процесах неживої і живої природи.

Відповідно до визначення спеціалізованої установи ООН з питань освіти, науки і культури ЮНЕСКО: «інформація – це універсальна субстанція, що пронизує усі сфери людської діяльності, слугує провідником знань та думок, інструментом спілкування, взаєморозуміння та співробітництва, утвердження стереотипів мислення та поведінки».

В Україні на законодавчому рівні (Закон України «Про інформацію») закріплено таке визначення: «інформація – це документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі».

До основних *ознак* інформації відносять:

– невичерпність. Інформація є невичерпною, тиражується, але не витрачається, може поширюватися в необмеженій кількості екземплярів практично без зміни її змісту і втрати якості, може належати багатьом особам, може бути використана необмежену кількість разів;

– вимірність. Інформація може бути кількісно виміряна (кількість символів, знаків);

– двоєдинство інформації та її носія. Інформація передається і поширюється в більшості випадків на матеріальному носії і за допомогою матеріального носія;

– фізична невідчужуваність інформації від її творця, власника, споживача;

– наявність організаційної форми, структури у вигляді інформаційних систем, документів, бібліотек тощо;

– цінність. Інформація має певну цінність (може продаватися).

– поширюваність. Інформація не локалізована в просторі, може легко розповсюджуватися.

Серед основних *властивостей* інформації виділяють: об'єктивність, достовірність, повнота, точність, актуальність, корисність, цінність, зрозумілість, доступність, стислість тощо.

Об'єктивність. Інформація існує поза і незалежно від людської свідомості. Інформація - це відображення зовнішнього об'єктивного світу. Відображаючись у свідомості людини, інформація може спотворюватися залежно від думки, судження, досвіду, знань конкретного суб'єкта, і, таким чином, перестати бути об'єктивною.

Достовірність. Інформація достовірна, якщо вона відображає справжній стан справ. Об'єктивна інформація завжди достовірна, але достовірна інформація може бути як об'єктивною, так і суб'єктивною.

Повнота інформації. Інформацію можна назвати повною, якщо її достатньо для розуміння і прийняття рішень.

Точність інформації визначається ступенем її близькості до реального стану об'єкта, процесу, явища.

Актуальність інформації - важливість для теперішнього часу, злободенність, нагальність. Тільки вчасно отримана інформація може бути корисна.

Корисність (цінність) інформації. Корисність може бути оцінена через задоволення потреб конкретних її споживачів.

У науці представлено багато підходів до *класифікації інформації.* Інформацію умовно поділяють на естетичну та семантичну. Естетична інформація зобов'язана своїм походженням виникаючим у природі різним поєднанням звуків, запахів, світла, квітів і тіней. Різні твори мистецтва (музика, живопис, література) також відносять до естетичної інформації.

Семантична інформація виникає в результаті різної діяльності людей. Залежно від способу передачі і сприйняття виділяють такі види інформації: візуальна (передається і сприймається візуальними образами); аудіальна (звуками); тактильна (відчуттями); смакова (запахами); машинно-орієнтована (сприймається і обробляється електронними пристроями).

За соціальною орієнтацією в науці виділяють масову, особисту і спеціальну інформацію. Якщо масова інформація адресується широкому колу споживачів, то особиста орієнтована на певну особу або групу осіб. Спеціальна інформація розрахована на фахівців, наприклад наукова, художня, технічна, гуманітарна. Спеціальну інформацію часто підрозділяють за сферами людської діяльності за галузевим принципом: машинобудівна, приладобудівна, енергетична, юридична, медична тощо.

Закон України «Про інформацію» поділяє інформацію на такі види:

- статистична інформація - офіційна документована державна інформація, що дає кількісне характеристику подій та явищ, які відбуваються в економічній, соціальній, культурній та інших сферах життя України;

- масова інформація - публічно поширювана друкована та аудіовізуальна інформація. Друкованими засобами масової інформації є періодичні друковані видання (преса) - газети, журнали, бюлетені і т.д. і разові видання з визначеним тиражем. Аудіовізуальних засобами масової інформації є: радіомовлення, телебачення, кіно, звукозапис, відеозапис тощо;

- інформація про діяльність державних органів влади та органів місцевого і регіонального самоврядування - офіційна документована інформація, яка створюється в процесі поточної діяльності законодавчої, виконавчої та судової влади, органів місцевого і регіонального самоврядування. Основними джерелами цієї інформації є: законодавчі акти України, інші акти, що приймаються Верховною Радою та її органами, акти Президента України, підзаконні нормативні акти, ненормативні акти державних органів, акти органів місцевого і регіонального самоврядування;

- правова інформація - сукупність документованих або публічно оголошених відомостей про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику;

- інформація про особу - сукупність документованих або публічно оголошених відомостей про особу;

- інформація довідково-енциклопедичного характеру - систематизовані, документовані або публічно оголошені відомості про суспільне, державне життя та навколишнє середовище;

- соціологічна інформація - документовані або публічно оголошені відомості про ставлення окремих громадян і соціальних груп до суспільних подій та явищ, процесів, фактів;

- екологічна інформація;

- інформація про товар (роботу, послугу);

- науково-технічна інформація;

- податкова інформація.

1.2. Інформаційна безпека: основні підходи до визначення. Об'єкти і суб'єкти інформаційної безпеки.

Розглядаючи значення терміна «інформаційна безпека» доцільно з'ясувати сутність поняття безпека. Так, під безпекою розуміють, зокрема, такий стан складної системи, коли дія зовнішніх і внутрішніх факторів не призводить до погіршення системи або до неможливості її функціонування і розвитку.

Загалом безпеку можна розглядати у різних аспектах: як потребу й інтерес, відчуття, цінність для особи чи суспільства, соціальні відносини, соціальну функцію, яку насамперед виконує держава, систему заходів тощо.

Інформаційна безпека – стан захищеності інтересів будь-якого об'єкта в інформаційній сфері (в тому числі – соціального, починаючи з людства, держав, закінчуючи організацією, групою, особою, та технічного - інформаційно-телекомунікаційних систем, засобів звязку, автоматизованих систем управління, окремих комп'ютерів та інших засобів обробки й передачі інформації).

Далі під терміном «інформаційна безпека» розумітимемо інформаційну безпеку держави, суспільства, особи.

У науковій літературі, а також на рівні національного законодавства існує досить багато варіантів визначення поняття інформаційної безпеки.

Основну групу становлять бачення, у рамках яких інформаційну безпеку держави розглядають як стан, тенденції розвитку, умови життєдіяльності соціуму, його структур, інститутів і установ, за яких забезпечується збереження їх якісного, вільного, відповідного власній природі та інноваційного функціонування.

Деякі з них представлені нижче.

Інформаційна безпека – стан захищеності інтересів особи, суспільства та держави в інформаційній сфері, який виключає можливість заподіяння їм шкоди через неповноту, несвоєчасність і недостовірність інформації, а також негативні наслідки використання інформаційних технологій або законодавчо забороненої чи обмеженої для поширення інформації.

Інформаційна безпека - це стан захищеності об'єкта (людини, суспільства, держави) від інформаційних загроз, який визначається рівнем шкоди, яку може бути заподіяно існуванню, функціонуванню чи діяльності об'єкта в разі реалізації цих загроз через

- використання неповної, несвоєчасної та недостовірної інформації;
- здійснення негативного інформаційного впливу;
- протиправного застосування інформаційних технологій;
- несанкціонованого розповсюдження і використання інформації, порушення її цілісності, конфіденційності та доступності.

Інформаційна безпека – це стан захищеності потреб в інформації особи, суспільства й держави, при якому забезпечується їхнє існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз. Стан інформованості визначає ступінь адекватності сприйняття суб'єктами навколишньої дійсності і як наслідок – обґрунтованість прийнятих рішень і дій.

Інформаційна безпека - це стан захищеності свідомості і буття соціальних суб'єктів від інформаційних загроз, який визначається рівнем реальної або потенційної шкоди, заподіяної внаслідок деструктивного інформаційного впливу або порушення безпеки інформації.

Інші науковці розглядають інформаційну безпеку через призму розвитку інформаційного простору держави, суспільства і розуміють під нею стан захищеності інформаційного середовища, за якого забезпечується його формування, використання й розвиток в інтересах особистості, суспільства, держави незалежно від впливу внутрішніх та зовнішніх інформаційних загроз. Під інформаційним середовищем мають на увазі сферу діяльності суб'єктів, пов'язану із створенням, обробленням та обміном інформації.

Розглядаючи сутність поняття «інформаційна безпека», слід відзначити, що в англійській мові є два терміни, які одинаково перекладаються на українську мову, однак мають відмінний зміст: «safery» і «security». Перший з них означає стан захищеності об'єкта, другий – акцентує на діяльності із забезпечення цього стану.

Тому інформаційну безпеку визначають і як стан, який характеризується відсутністю небезпеки, тобто чинників і умов, які загрожують безпосередньо об'єкту (індивіду, спільноті, державі) з боку інформаційно-комунікаційного середовища, і як можливість, здатність об'єкта надійно захиститися, нейтралізувати, протидіяти різним інформаційним загрозам.

У цьому контексті можна розглянути такі визначення інформаційної безпеки.

Інформаційна безпека – це стан захищеності життєво важливих інтересів особистості, суспільства й держави від негативних інформаційних впливів в економіці, внутрішній і зовнішній політиці, в науково-технологічній, соціокультурній і оборонній сферах, системі державного управління,

забезпечення самостійного й незалежного розвитку всіх елементів національного інформаційного простору та забезпечення інформаційного суверенітету країни,

захищеності від маніпулювання інформацією і дезінформування та впливів на свідомість, підсвідомість і психіку як індивіда, так і суспільства в цілому,

спроможність держави нейтралізувати чи послабити дію внутрішніх і зовнішніх інформаційних загроз.

Інформаційна безпека – це стан захищеності особи, суспільства і держави від зовнішніх та внутрішніх небезпек і загроз, який базується на діяльності людей, суспільства, держави, світового співтовариства з виявлення (вивчення), попередження, послаблення, ліквідації і відбиття небезпек і загроз, здатних знищити їх, позбавити фундаментальних матеріальних і духовних цінностей, завдати неприйнятної шкоди, закрити шлях для прогресивного розвитку.

На нашу думку, в українській мові доцільно використовувати два терміни, які відображають зазначену різницю.

Під інформаційною безпекою розуміти стан захищеності і, отже, стійкості основних сфер людської діяльності (політичної, економічної, наукової, технічної, культурної, військової сфер, сфери державного управління та суспільної свідомості тощо), по відношенню до можливих небезпечних інформаційних впливів.

Термін «забезпечення інформаційної безпеки» означає діяльність, сукупність заходів і загалом здатність суспільства і держави гарантувати бажаний захищений стан.

На думку фахівців, забезпечення інформаційної безпеки передбачає наявність таких трьох складових: діяльність, засоби та суб’єкти (Рис.1).

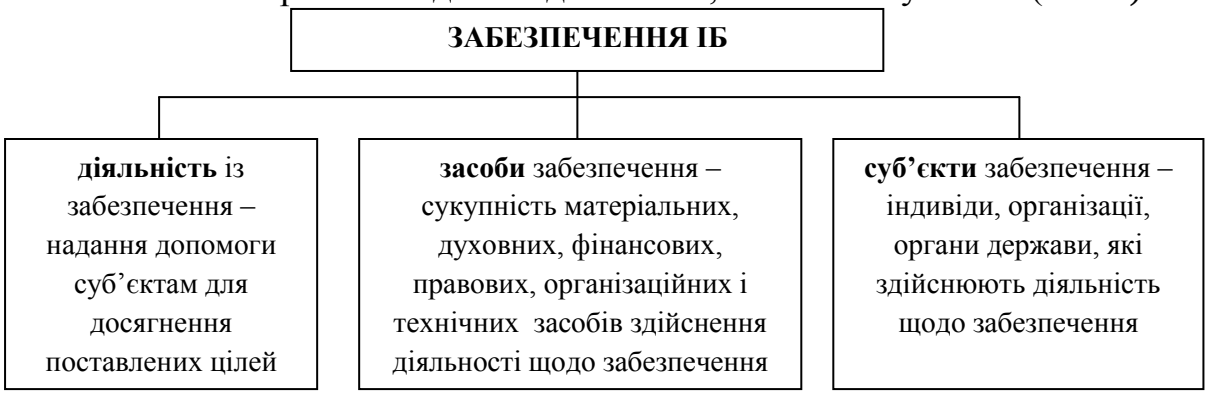

Рис.1. Структура забезпечення інформаційної безпеки.

На основі розглянутих визначень виділимо такі основні аспекти інформаційної безпеки:

– забезпечення доступу суб'єктів до повної, достовірної інформації для їх життєдіяльності, освіти та розвитку, реалізації прав та обов'язків в суспільстві;

– захист суб'єкта від деструктивних інформаційних впливів;

– реалізація гарантій конституційних прав і свобод людини і громадянина, що стосуються діяльності в інформаційній сфері,

– захист від несанкціонованого впливу на інформацію, що належить суб'єкту (охорона персональних даних, державної таємниці, службової інформації та інших видів інформації обмеженого доступу);

– захист інформаційної інфраструктури групи суб'єктів (організації, держави) від руйнівних впливів (випадкових або навмисних, природного або штучного характеру).

Аналізуючи сутність поняття «інформаційна безпека», нагадаємо, що інформаційна сфера сучасного суспільства має дві складові: інформаційно-технічну (штучна сфера техніки, технологій, ресурсів тощо) та інформаційно-психологічну (психіка людини, пізнання, безпосереднє спілкування). Відповідно, в загальному випадку інформаційну безпеку представляють двома складовими: інформаційно-технічною безпекою та інформаційно-психологічною безпекою.

Отже, інформаційна безпека - стан захищеності особистості, суспільства, держави від інформації шкідливого або протиправного характеру, яка здійснює негативний вплив на людську свідомість та перешкоджає сталому розвитку особистості, суспільства і держави. Інформаційна безпека - це також стан захищеності інформації та інформаційної інфраструктури, включаючи комп'ютери та інформаційно-телекомунікаційну інфраструктуру, які забезпечують її зберігання, обробку й передавання.

Побіжно встановимо співвідношення між поняттями «інформаційна безпека» та «безпека інформації». Очевидно, що значення першого терміну є значно ширшим і включає друге. Так, безпека інформації (даних) – це стан захищеності інформації (даних), при якому забезпечуються її конфіденційність, доступність і цілісність. Окрім власне інформації часто до об’єктів безпеки інформації додають також інфраструктуру, яка забезпечує їх обробку та передавання.

Важливо розуміти, що інформаційна безпека є однією зі складових національної безпеки держави нарівні з економічною, енергетичною, військовою, соціальною та іншими. При цьому цілком очевидно, що роль інформаційної безпеки та її місце в системі національної безпеки держави стає все значнішою. Це відбувається внаслідок таких чинників:

– національні інтереси, загрози їм і забезпечення захисту від цих загроз у всіх галузях національної безпеки виражаються, реалізуються і здійснюються через інформацію та інформаційну сферу;

– особа та її права, інформація та інформаційні системи і права на них - це основні об'єкти не тільки інформаційної безпеки, а й основні елементи всіх об'єктів безпеки в усіх її галузях;

– вирішення завдань національної безпеки пов'язане з використанням інформаційно-комунікаційних засобів та технологій як основних на сучасному етапі;

– проблема національної безпеки має яскраво виражений інформаційний характер.

У визначенні, представленому вітчизняними науковцями, інформаційну безпеку України розуміють як складову національної безпеки і виділяють такі напрями її забезпечення:

– гарантування інформаційного суверенітету України;

– вдосконалення державного регулювання розвитку інформаційної сфери, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;

– активне залучення засобів масової інформації до боротьби з корупцією, зловживанням службовим становищем, іншими явищами, які загрожують національній безпеці України;

– неухильне дотримання конституційних прав громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції;

– вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

Цікавим є визначенням зарубіжних фахівців, у якому зроблено акцент на необхідності проактивної позиції держави, суспільства й особистості в умовах прискореного розвитку та впровадження інформаційно-телекомунікаційних технологій у всі сфери життєдіяльності суспільства, виникнення нових видів загроз та потреби вироблення інноваційних форм поведінки для забезпечення інформаційної безпеки.

Таким чином, інформаційна безпека - це здатність держави, суспільства, соціальної групи, особистості,

по-перше, забезпечити з певною ймовірністю достатні і захищені соціальний інтелект та інформаційний ресурс, оптимальну соціальну впорядкованість та інфосередовище для підтримки життєдіяльності та життєздатності, стійкого функціонування і розвитку соціуму;

по-друге, протистояти інформаційним небезпекам і загрозам, негативним інформаційним впливам на індивідуальну і суспільну свідомість і психіку людей, а також на комп'ютерні мережі та інші технічні джерела інформації;

по-третє, виробляти особистісні та групові навички та вміння безпечної поведінки;

по-четверте, підтримувати постійну готовність до адекватних заходів в інформаційному протиборстві;

по-п'яте, постійно і послідовно за певною безпечною програмою «вмонтовувати» штучний інтелект в соціальне середовище.

Сьогодні в умовах розвитку інформаційного суспільства інформаційна безпека виступає в якості базової цінності держави, забезпечення якої гарантує її стабільне функціонування та прогресивний розвиток.

З огляду на виділення двох складових інформаційної безпеки держави, суспільства (інформаційно-технічної та інформаційно-психологічної), визначають дві групи об'єктів інформаційної безпеки:

– *соціальні:* особа - її права та свободи в інформаційній сфері, психіка, в т.ч. свідомість та підсвідоме, особиста інформація; суспільство - його духовні цінності, засади солідарної діяльності; держава - її конституційний лад, суверенітет, ефективне функціонування;

– *технічні:* інформаційні ресурси, інформаційно-комунікаційна інфраструктура, в тому числі інформаційно-комунікаційні системи різного масштабу і різного призначення, технології та засоби обробки, зберігання, передавання інформації.

Схема об’єктів інформаційної безпеки держави показана на рис. 2.

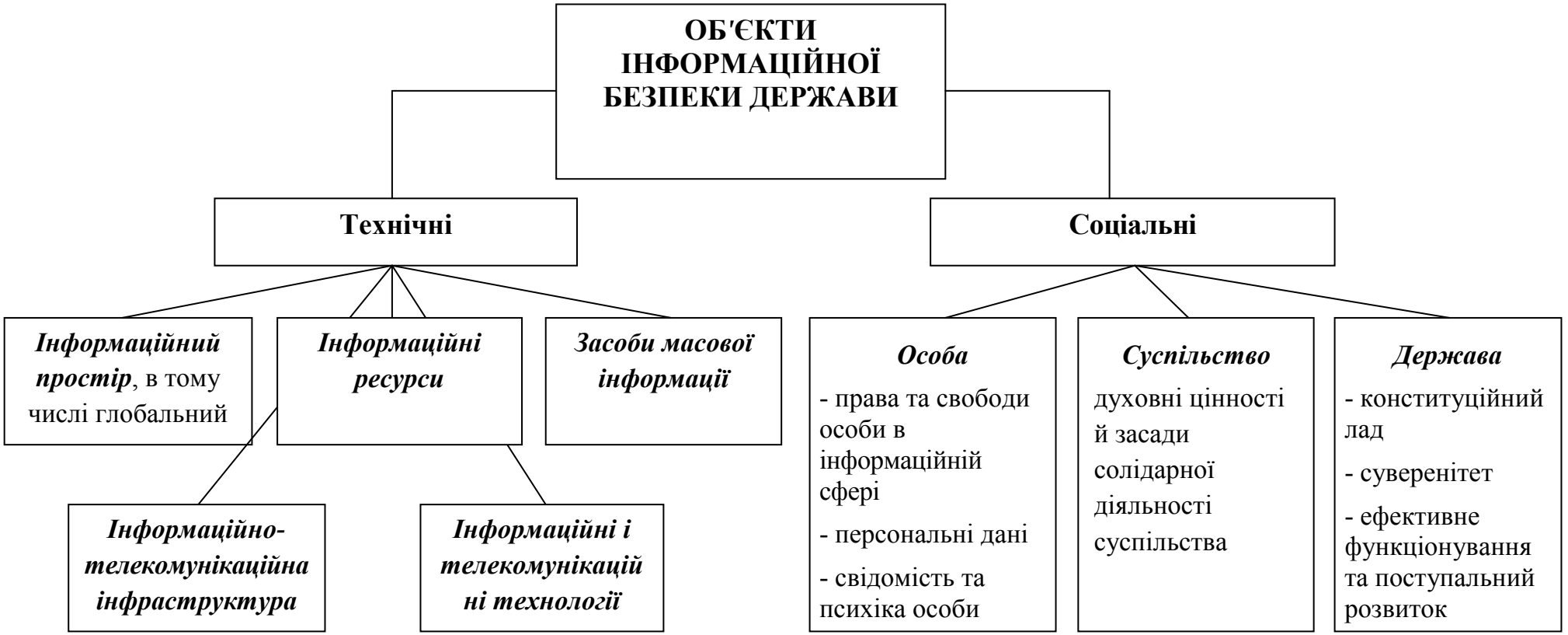

Рис. 2. Об’єкти інформаційної безпеки держави.

Суб'єктами забезпечення інформаційної безпеки є:

– держава, яка здійснює функції у цій галузі через органи законодавчої, виконавчої та судової влади;

– комерційні, громадські, інші організації та об'єднання;

– громадяни, які відповідно до законодавства мають права й обов'язки щодо участі у забезпеченні безпеки держави.

Головну роль при цьому відіграє держава, яка відповідно до чинного законодавства повинна забезпечувати інформаційну безпеку на рівні особи (дотримання прав і свобод особи в інформаційній сфері, сприяння формуванню раціонального, критичного мислення на основі принципів свободи вибору, забезпечення захисту конфіденційної інформації особи), суспільства (формування якісного інформаційно-аналітичного простору, забезпечення плюралізму, багатоканальності отримання інформації, незалежної діяльності ЗМІ) і держави (інформаційно-аналітичне забезпечення діяльності державних органів, інформаційне забезпечення внутрішньої і зовнішньої політики держави, функціонування системи захисту інформації з обмеженим доступом, протидія правопорушенням в інформаційній сфері, комп'ютерним злочинам тощо).

У залежності від об’єктного складу (особи, суспільства або держави, що є об’єктом) визначають такі види інформаційної безпеки:

– особисту (безпеку конкретної особи),

– суспільну (безпека суспільства),

– державну (безпеку окремої держави),

– міжнародну (безпеку багатьох держав, світового співтовариства загалом).

На нашу думку, модель інформаційної безпеки держави можна представити у такому вигляді (рис.3.). Детальніше окремі її елементи розглянемо у наступних темах.

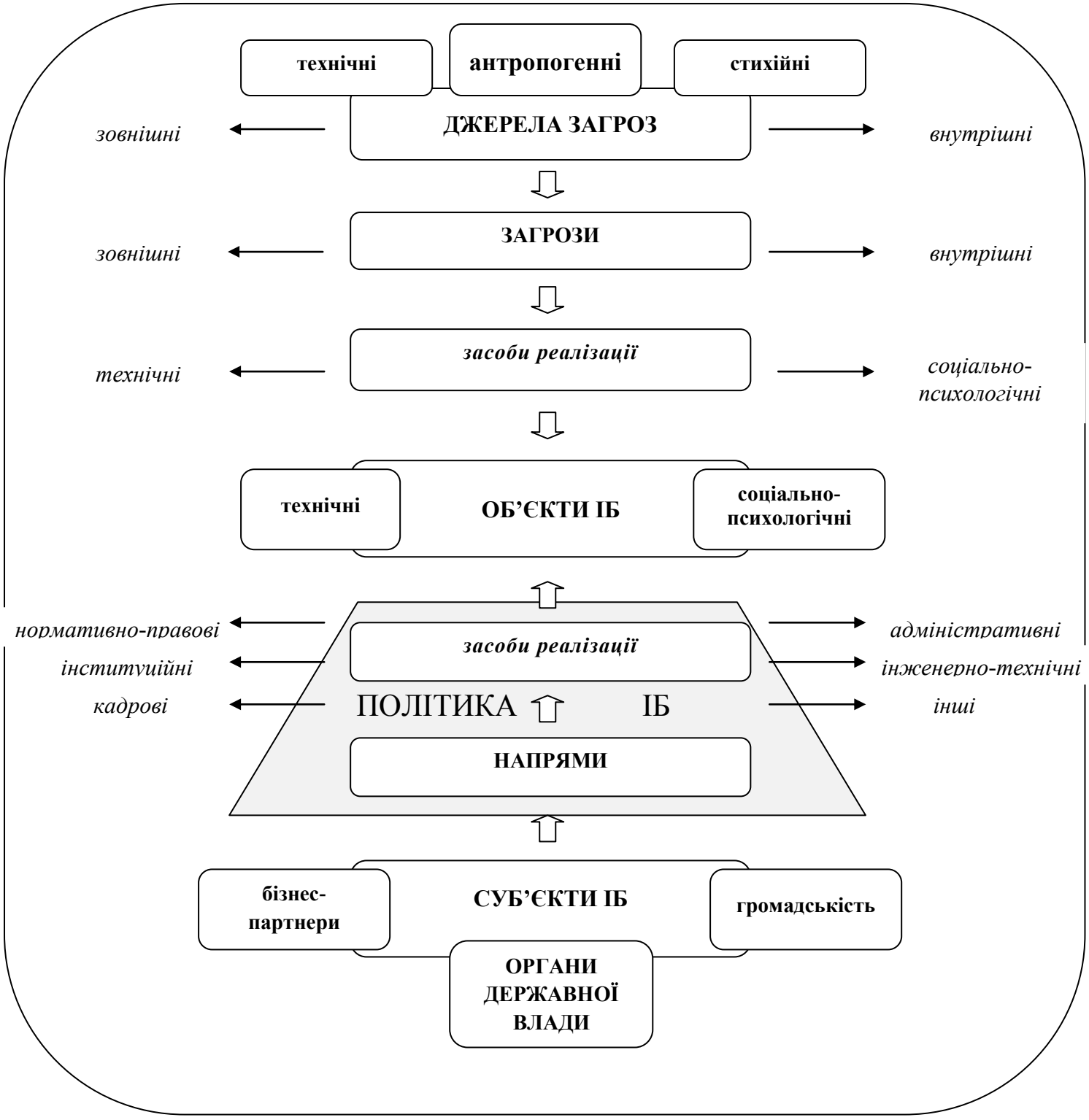

Рис.3. Модель інформаційної безпеки держави.

1.3. Етапи розвитку інформаційної безпеки.

Об'єктивно категорія «інформаційна безпека» виникла з появою засобів комунікації між людьми, а також з усвідомленням людиною наявності у людей і їх співтовариств інтересів, яким може бути завданий збитку шляхом дії на інформаційні та комунікаційні засоби, наявність і розвиток яких забезпечує інформаційний обмін в соціумі.

Враховуючи вплив на трансформацію ідей інформаційної безпеки, в розвитку інформаційно-комунікаційних засобів виділяють сім етапів.

Етап	**Розвиток засобів обробки та передачі інформації**	**Розвиток засобів інформаційної безпеки**
I етап до 1816 р.	використання природно виникаючих інформаційно-комунікаційних засобів	методи захисту інформації, розроблені на першому етапі її розвитку: підписи, особисті печатки, ручна і механічна шифрація, приховування факту передачі інформації
II етап з 1816 р.	початок використання штучно створюваних технічних засобів електро- і радіозв'язку	шифрування, білий шум
III етап з 1935 р.	поява засобів радіолокації і гідроакустики	поєднання організаційних і технічних заходів, направлених на підвищення захищеності засобів радіолокацій від дії на їх приймальні пристрої маскуючих і імітуючих радіоелектронних перешкод
IV етап з 1946 р.	винайдення і впровадження комп'ютерів	методи і способи обмеження фізичного доступу до устаткування засобів добування, переробки і передачі інформації
V етап з 1965 р.	створення і розвиток локальних інформаційно-комунікаційних мереж	методи і способи фізичного захисту засобів добування, переробки і передачі інформації, об'єднаних в локальну мережу шляхом адміністрування і управління доступом до мережевих ресурсів

VI етап з 1973 р.	використання надмобільних комунікаційних пристроїв з широким спектром завдань	розробка нових критеріїв безпеки, боротьба з хакерством, проблеми інформаційної безпеки виходять на рівень держави формування інформаційного права, основних рекомендацій щодо захисту інформації та безпечної роботи на ПК поява програмних рішень
VII етап з 1985 р.	створення і розвиток глобальних інформаційно-комунікаційних мереж з використанням космічних засобів забезпечення	створення систем захисту для кінцевих користувачів, сегментів мережі і навіть самого Інтернету Необхідним є створення макросистеми інформаційної безпеки людства під егідою провідних міжнародних форумів

Розглянемо кожний етап детальніше.

І етап – до 1816 року – характеризується використанням природно виникаючих інформаційно-комунікаційних засобів. У цей період основне завдання інформаційної безпеки полягало в захисті відомостей про події, факти, майно, місцезнаходження і інші дані, що мають для людини особисто або співтовариства, до якого вона належала, життєве значення.

Серед методів захисту інформації, розроблених на першому етапі її розвитку, варто згадати: підписи, особисті печатки, ручна і механічна шифрація, приховування факту передачі інформації. Незважаючи на простоту багатьох методів шифрації тих часів, вони виконували своє головне завдання - ворог не міг отримати інформацію в короткий термін, навіть перехопивши саме повідомлення. Час, необхідний на розшифровку закодованого повідомлення, майже завжди робив інформацію неактуальною.

Основою будь-якого шифру в усі часи був ключ шифрації: пронумеровані листочки, з прорізаними «віконцями», які треба було накладати на повідомлення і читати отримувані слова в віконцях, знамениті «танцюючі чоловічки» з розповідей Конан Дойля, які мають під собою цілком реальну основу.

Ще варто згадати таку методику шифрації повідомлень, як «лист у листі», популярну і в наш час. Сенс цієї методики полягав у тому, що всередині листа на пересічну тему за певним принципом (підстановка слів, ключові фрази) містилася інформація про важливі речі, наприклад про час і місце таємної зустрічі або донесення розвідки про пересування сил ворога.

Першим відомим засобом захисту інформації вважається давньогрецька скитала, опис якої було дано в 120 році до н.е. Вона працювала за таким принципом: у відправника і адресата були палки однакової товщини. Відправник намотував на палицю тонку смужку папірусу, і писав по

горизонталі букви. Після розгортання папірусу виходила безладна послідовність літер, прочитати яку можна було лише за допомогою палиці такої ж товщини. Найуразливішим місцем цього етапу стає людський фактор, у вигляді ненадійних посланників і потенційних зрадників з тих, хто знає секрет коду.

II етап – починаючи з 1816 року – пов'язаний з початком використання штучно створених технічних засобів електро- і радіозв'язку. Для забезпечення скритності і перешкодостійкості радіозв'язку необхідно було використовувати досвід першого періоду інформаційної безпеки на вищому технологічному рівні, а саме застосування перешкодостійкого кодування повідомлення (сигналу) з подальшим декодуванням прийнятого повідомлення (сигналу).

Цей часовий етап ознаменувався появою в широкому вжитку телеграфів і подібних пристроїв. До класичних проблем захисту інформації додалася ще одна - зацікавлена в інформації людина могла «підключитися» до лінії передачі інформації, і слухати всю інформацію, яка передавалася. А з урахуванням єдиної прийнятої в світі мови телеграфів - азбуки Морзе, для прослуховування переданої інформації не було ніяких перешкод. Ще на шляху тих, хто хотів зберегти свою інформацію в цілості встала проблема технічного характеру - інформація деколи могла дійти не вся або дійти з певними помилками. Як результат, звичайний телеграфний апарат військового зразка містив в собі автоматичний механічний модуль, який шифрував інформацію за певним зразком, а також генератор «білого шуму» - набору перешкод, які забивали лінії передач весь час, поки не відбувалося передачі інформації. Як результат, потенційний ворог не міг дізнатися, коли починається і закінчується справжня передача. Так само стало простіше підробляти листи, передані за допомогою телеграфу, адже тепер в них не використовувався почерк і друк, а текст повідомлень значно скоротився, адже кожна буква коштувала грошей. Найуразливішим місцем на цьому етапі продовжує залишатися людський фактор: вплив людей, пов'язаних з «програмуванням» шифрувальних засобів.

III етап – починаючи з 1935 року – пов'язаний з появою засобів радіолокації (визначення положення об'єкта за допомогою відбитих від нього радіохвиль) і гідроакустики (розділ акустики, що вивчає випромінювання, прийом і поширення звукових хвиль в реальному водному середовищі: океанах, морях, озерах тощо - для цілей підводної локації, зв'язку). Основним способом забезпечення інформаційної безпеки в цей період було поєднання організаційних і технічних заходів, направлених на підвищення захищеності засобів радіолокації від дії на їх приймальні пристрої активних маскуючих і пасивних імітуючих радіоелектронних перешкод.

На третьому часовому етапі створено нову технологію для передачі інформації - радіо. Довгі й короткі хвилі не залежать від проводів, і покривають чималі відстані, але будь-який налаштований приймач в зоні мовлення може отримати і відтворити передану інформацію. Для захисту інформації використовувалися майже ті ж самі технології, що й у часи телеграфів, але

складніші в технологічному плані. У більшості місць білий шум був замінений на безперервну трансляцію будь-якої або статистичної інформації, при перериванні якої точка мовлення повинна була вийти на зв'язок і підтвердити, що це те ж саме джерело. Інший варіант передбачав збереження повної тиші в ефірі, а під час сеансів зв'язку, що відбувалися в заздалегідь визначений час, сигнал, який надсилався, модулювався білим шумом, і для стороннього слухача від шуму не відрізнявся.

Варто відзначити, що підробка радіопередачі є набагато складнішою від підробки телеграфного повідомлення, адже через радіоканал передається голос, та й довжина, час передачі не так обмежені. До загального набору уразливих місць додалася можливість перехоплення устаткування, вивчення якого могло дати ворогові ключ до всіх попередніх передач.

IV етап – починаючи з 1946 року – пов'язаний з винаходом і впровадженням в практичну діяльність електронно-обчислювальних машин (комп'ютерів). Завдання інформаційної безпеки вирішувалися, в основному, методами і способами обмеження фізичного доступу до устаткування засобів добування, переробки і передачі інформації.

Четвертий етап поставив крапку на шифрах, заснованих на підміні символів. Великі, громіздкі комп'ютери, які могли робити по кілька сотень математичних операцій в секунду, розкривали такі шифри у дуже короткі терміни. Набагато складніше комп'ютерам було впоратися з радіограмами, адже вся інформація для комп'ютера складається з одиниць і нулів, перевести в які звук не так просто. Через розміри самих комп'ютерів для генерації шифрів вони не використовувалися. У порівнянні з третім етапом, в самій методиці шифрації та захисту інформації нічого не змінилося, так само не змінилися вразливі місця систем.

V етап – починаючи з 1965 року – обумовлений створенням і розвитком локальних інформаційно-комунікаційних мереж. Завдання інформаційної безпеки також вирішувалися, в основному, методами і способами фізичного захисту засобів добування, переробки і передачі інформації, об'єднаних в локальну мережу шляхом адміністрування і управління доступом до мережевих ресурсів.

П'ятий етап розпочався з прориву в галузі комунікацій – створення мереж. Комп'ютери об'єднуються в локальні мережі, фахівці фантазують про мережі, якими буде обплутаний весь світ, і користувача ПК з Англії буде відокремлювати від користувача ПК з Америки чи Китаю лише пара натискань клавіш.

Поки ж лише всередині великих університетів, а так само в ряді військових установ введені локальні комп'ютерні мережі, але вже тоді починають розроблятися системи протидії потенційним викрадачам інформації, адже сама логіка роботи локальної мережі має на увазі доступність загальної інформації з будь-якої точки. У цей же час вперше, стосовно комп'ютерів, використовується термін «парольного захисту» - певного коду, за допомогою якого користувач

може отримати доступ до даних і до комп'ютера взагалі. Саме тоді закладені основи інформаційної безпеки в її сучасному вигляді. Основною вразливістю знову стає людський фактор - неуважний або ненадійний співробітник може вчинити помилку, яка дасть потенційному зловмиснику доступ до інформації.

VI етап – починаючи з 1973 року – пов'язаний з використанням надмобільних комунікаційних пристроїв з широким спектром завдань. Загрози інформаційній безпеці стали набагато серйознішими. Для забезпечення інформаційної безпеки в комп'ютерних системах з безпровідними мережами передачі даних потрібно було розробити нові критерії безпеки. Утворилися співтовариства хакерів, що ставлять собі за мету нанесення збитку інформаційній безпеці окремих користувачів, організацій і цілих країн. Інформаційний ресурс став найважливішим ресурсом держави, а забезпечення його безпеки – найважливішою і обов'язковою складовою національної безпеки. Формується інформаційне право – нова галузь міжнародної правової системи.

Отже, цей етап ознаменувався появою хакерів, а також мобільних робочих станцій. Однак, якщо бути точними, термін «хакер» з'явився приблизно в 1960 році, в Массачусетському технологічному інституті, де використовувався для позначення будь-якого програміста, котрий придумав якесь дуже незвичайне і хитре рішення, або дуже грубе, але ефективне. Дуже швидко цей термін почав означати будь-якого комп'ютерного фахівця.

Що стосується інформаційного права та безпеки інформації держави, то це стосується лише дуже малого числа країн, а так само не слід забувати про те, що багато важливих інформаційних структур залишаються ізольованими від зовнішнього доступу. В цей же час якраз формуються основні рекомендації щодо захисту інформації та безпечної роботи на персональних комп'ютерах.

Персонал, якому довіряють персональні комп'ютери для роботи на них вдома, обов'язково повинен був пройти атестацію на вміння працювати на ПК, а також зобов'язувався не залишати не заблокований комп'ютер, не використовувати простих паролів і не давати фізичного доступу до ПК.

Водночас компанія IBM виходить на ринок з революційним рішенням – створення відкритої архітектури. До цього моменту всі комп'ютери були моноблочними - вони поставлялися як готовий виріб, і не передбачали будь-яких змін у своїй структурі. IBM запропонували випускати окремі компоненти, щоб кожен бажаючий зміг зібрати такий комп'ютер, який йому подобається і підходить для його цілей.

Кілька років пізніше з'являються модулі для апаратного захисту даних - окремі плати, при використанні яких фізично на жорсткому диску інформація зберігається в зашифрованому вигляді, і без знання пароля не може бути зчитана. При цьому система повністю прозора для користувача, адже будь-які зроблені зміни вже записуються на диск як зашифрована інформація.

Другим варіантом криптозахисту є програмні рішення, які вимагають для початку роботи з даними розшифрувати їх, а після роботи зашифрувати. У випадку з програмним захистом, може бути чимало варіантів, за яких кінцева

шифрація не буде виконана і інформація буде легко доступна. Основним слабким місцем залишається людський фактор - багато людей вважають зайвим використовувати паролі або залишають їх занадто простими. З'являються вразливості, пов'язані з помилками в програмному забезпеченні, за яких некоректна робота програми може привести до потенційної втрати даних.

VII етап – починаючи з 1985 року – пов'язаний зі створенням і розвитком глобальних інформаційно-комунікаційних мереж з використанням космічних засобів забезпечення. Черговий етап розвитку інформаційної безпеки, очевидно, буде пов'язаний з широким використанням надмобільних комунікаційних пристроїв з широким спектром завдань і глобальним охопленням у просторі та часі, що забезпечуватиметься космічними інформаційно-комунікаційними системами. Для вирішення завдань інформаційної безпеки на цьому етапі необхідним є створення макросистеми інформаційної безпеки людства під егідою провідних міжнародних форумів.

На сьомому етапі створено кібермережі сучасного зразка, найбільшою з яких є Інтернет. Безліч людей щодня використовують мережу, не замислюючись про особисту безпеку. Приголомшлива кількість комп'ютерів, без відома їх власників об'єднуються в єдиний логічний простір, щоб влаштовувати атаки на сайти, розсилати небажану пошту або захоплювати інші сегменти мережі. Такими комп'ютерами, як правило, маніпулює одна людина, яка написала складний вірус. Навіть найменші організації не уявляють собі роботи без кількох персональних комп'ютерів, об'єднаних в окрему мережу.

Величезні ресурси, в тому числі обсяги людської праці, служать для створення систем захисту для кінцевих користувачів, сегментів мережі і власне Інтернету. Різко змінюється цінність інформації - значна кількість особистої, конфіденційної переписки кожен день пересилається через незахищені мережі, використання слабких паролів дає зловмисникам можливість отримувати доступ до інформації, а методики навчання людей роботі на ПК навіть не передбачають набуття мінімальних навичок захисту в інформаційному середовищі.

Таким чином, упродовж століть формувалося і видозмінювалося поняття інформаційної безпеки. Паралельно із розвитком засобів оброблення та передачі інформації вдосконалювалися підходи до забезпечення інформаційної безпеки. Чим складніше ставала техніка, чим більше довіряли їй інформації, тим сильніше була необхідність зберігати її в цілості й схоронності. З часом з’явилася потреба у захисті не тільки інформації, але й самої інформаційно-комунікаційної інфраструктури.

Питання для самоконтролю

1. Які підходи до розуміння поняття «інформація» ви знаєте?
2. Якими є основні ознаки і властивості інформації?
3. Які види інформації ви можете назвати?

4. Що таке інформаційна безпека держави? Наведіть приклади різних підходів до визначення цього поняття.

5. Які об’єкти і суб’єкти інформаційної безпеки держави ви можете назвати?

6. Яка різниця між поняттями «інформаційна безпека держави» і «забезпечення інформаційної безпеки держави»?

7. Як співвідносяться поняття «інформаційна безпека держави» і «національна безпека держави»?

8. Яке співвідношення між поняттями «інформаційна безпека» та «безпека інформації»?

9. Які етапи розвитку інформаційної безпеки ви знаєте? Назвіть їхні основні характеристики.

ТЕМА 2. Інформація як об’єкт інформаційної безпеки. Види інформації з обмеженим доступом.

2.1. Види інформації з обмеженим доступом відповідно до законодавства України.

Закон України «Про інформацію» від 02.10.1992 р. № 2657-XII поділяє інформацію за порядком доступу на відкриту інформацію та інформацію з обмеженим доступом.

Закони України «Про інформацію» та «Про доступ до публічної інформації» від 13.01.2011 р. № 2939-VI виділяють такі види інформації з обмеженим доступом: *конфіденційна, таємна та службова*.

Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом. Розпорядники інформації, які володіють конфіденційною інформацією, можуть поширювати її лише за згодою осіб, які обмежили доступ до інформації, а за відсутності такої згоди - лише в інтересах національної безпеки, економічного добробуту та прав людини.

Таємна інформація - інформація, доступ до якої обмежується відповідно до зазначених вище вимог (в інтересах національної безпеки, з метою запобігання злочинам, для захисту прав інших людей тощо), розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю. Порядок доступу до таємної інформації регулюється законодавством.

Визначення поняття «*службова інформація*» не надано у вітчизняному законодавстві, натомість встановлено, що до службової відносять інформацію:

– що міститься в документах суб'єктів владних повноважень, які становлять внутрішньо-відомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

– зібрану в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Обмеження доступу до інформації здійснюється відповідно до закону при дотриманні сукупності таких вимог: виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою

запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя; розголошення інформації може завдати істотної шкоди цим інтересам; шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

Інформація з обмеженим доступом має надаватися розпорядником інформації, якщо він правомірно оприлюднив її раніше, або якщо немає законних підстав для обмеження у доступі до такої інформації, які існували раніше.

Згідно із зазначеним законом до інформації з обмеженим доступом не можуть бути віднесені відомості про стан довкілля, якість харчових продуктів і предметів побуту; аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей; стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення; факти порушення прав і свобод людини і громадянина; незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб; інші відомості, доступ до яких не може бути обмежено відповідно до законів та міжнародних договорів України.

Не може бути обмежено доступ до інформації про розпорядження бюджетними коштами, володіння, користування чи розпорядження державним, комунальним майном, у тому числі до копій відповідних документів, умови отримання цих коштів чи майна, прізвища, імена, по батькові фізичних осіб та найменування юридичних осіб, які отримали ці кошти або майно. При дотриманні вимог, передбачених заонодавством, зазначене положення не поширюється на випадки, коли оприлюднення або надання такої інформації може завдати шкоди інтересам національної безпеки, оборони, розслідуванню чи запобіганню злочину.

Також до інформації з обмеженим доступом не належать відомості, зазначені у декларації про майно, доходи, витрати і зобов’язання фінансового характеру, оформленої за формою і в порядку, що встановлені Законом України «Про засади запобігання і протидії корупції».

Встановлено, що обмеженню доступу підлягає інформація, а не документ. Якщо документ містить інформацію з обмеженим доступом, для ознайомлення надається інформація, доступ до якої необмежений.

Закон забороняє поширення інформації з обмеженим доступом за винятком випадків, коли така інформація є предметом суспільного інтересу, і право громадськості знати цю інформацію переважає потенційну шкоду від її поширення. Предметом суспільного інтересу вважається інформація, яка свідчить про загрозу державному суверенітету, територіальній цілісності

України; забезпечує реалізацію конституційних прав, свобод і обов'язків; свідчить про можливість порушення прав людини, введення громадськості в оману, шкідливі екологічні та інші негативні наслідки діяльності (бездіяльності) фізичних або юридичних осіб тощо.

2.2. Службова інформація. Державна таємниця.

Службова інформація. Як відзначалося вище, українське законодавство не дає визначення терміну «службова інформація», встановлюючи, що до службової відносять інформацію:

– що міститься в документах суб'єктів владних повноважень, які становлять внутрішньо-відомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

– зібрану в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Документам, що містять інформацію, яка становить службову інформацію, присвоюється гриф «Для службового користування». Доступ до таких документів надається відповідно до законодавства.

Категорії відомостей, які становлять службову інформацію, визначаються органами державної влади, органами місцевого самоврядування, іншими суб'єктами владних повноважень, у тому числі на виконання делегованих повноважень, у переліках відомостей, що становлять службову інформацію, які не можуть бути обмеженими у доступі.

Законодавством встановлено вимоги до оприлюднення інформації розпорядниками. Відповідно до Закону України «Про доступ до публічної інформації» розпорядники інформації зобов'язані оприлюднювати:

1) інформацію про організаційну структуру, місію, функції, повноваження, основні завдання, напрями діяльності та фінансові ресурси (структуру та обсяг бюджетних коштів, порядок та механізм їх витрачання тощо);

2) нормативно-правові акти, акти індивідуальної дії (крім внутрішньоорганізаційних), прийняті розпорядником, проекти рішень, що підлягають обговоренню, інформацію про нормативно-правові засади діяльності;

3) перелік та умови отримання послуг, що надаються цими органами, форми і зразки документів, правила їх заповнення;

4) порядок складання, подання запиту на інформацію, оскарження рішень розпорядників інформації, дій чи бездіяльності;

5) інформацію про систему обліку, види інформації, яку зберігає розпорядник;

5-1) перелік наборів даних, що оприлюднюються у формі відкритих даних;

6) інформацію про механізми чи процедури, за допомогою яких громадськість може представляти свої інтереси або в інший спосіб впливати на реалізацію повноважень розпорядника інформації;

7) плани проведення та порядок денний своїх відкритих засідань;

8) розташування місць, де надаються необхідні запитувачам форми і бланки установи;

9) загальні правила роботи установи, правила внутрішнього трудового розпорядку;

10) звіти, в тому числі щодо задоволення запитів на інформацію;

11) інформацію про діяльність суб'єктів владних повноважень, а саме про:

їхні місцезнаходження, поштову адресу, номери засобів зв'язку, адреси офіційного веб-сайту та електронної пошти;

прізвище, ім'я та по батькові, службові номери засобів зв'язку, адреси електронної пошти керівника органу та його заступників, а також керівників структурних та регіональних підрозділів, основні функції структурних та регіональних підрозділів, крім випадків, коли ці відомості належать до інформації з обмеженим доступом;

розклад роботи та графік прийому громадян;

вакансії, порядок та умови проходження конкурсу на заміщення вакантних посад;

перелік та умови надання послуг, форми і зразки документів, необхідних для надання послуг, правила їх оформлення;

перелік і службові номери засобів зв'язку підприємств, установ та організацій, що належать до сфери їх управління, та їх керівників, крім підприємств, установ та організацій, створених з метою конспірації, оперативно-розшукової або контррозвідувальної діяльності;

порядок складання, подання запиту на інформацію, оскарження рішень суб'єктів владних повноважень, їх дій чи бездіяльності;

систему обліку, види інформації, якою володіє суб'єкт владних повноважень;

12) іншу інформацію про діяльність суб'єктів владних повноважень, порядок обов'язкового оприлюднення якої встановлений законом.

Державна таємниця. Відповідно до Закону України «Про державну таємницю» від 21.01.1994 р. № 3855-XII державна таємниця (також - секретна інформація) - це вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому законодавством, державною таємницею і підлягають охороні державою;

До державної таємниці у порядку, встановленому цим Законом, відноситься інформація:

1) у сфері оборони:

– про зміст стратегічних і оперативних планів та інших документів бойового управління, підготовку та проведення військових операцій, стратегічне та мобілізаційне розгортання військ, а також про інші найважливіші показники, які характеризують організацію, чисельність, дислокацію, бойову і мобілізаційну готовність, бойову та іншу військову підготовку, озброєння та матеріально-технічне забезпечення Збройних Сил України та інших військових формувань;

– про напрями розвитку окремих видів озброєння, військової і спеціальної техніки, їх кількість, тактико-технічні характеристики, організацію і технологію виробництва, наукові, науково-дослідні та дослідно-конструкторські роботи, пов'язані з розробленням нових зразків озброєння, військової і спеціальної техніки або їх модернізацією, а також про інші роботи, що плануються або здійснюються в інтересах оборони країни;

– про дислокацію, характеристики пунктів управління, зміст заходів загальнодержавного та регіонального, у разі необхідності міського і районного рівня, щодо приведення у готовність єдиної державної системи цивільного захисту населення і територій до виконання завдань в особливий період та про організацію системи зв'язку (оповіщення) в особливий період, можливості населених пунктів, регіонів і окремих об'єктів щодо евакуації, розосередження населення і забезпечення його життєдіяльності; забезпечення виробничої діяльності об'єктів національної економіки у воєнний час;

– про геодезичні, гравіметричні, картографічні та гідрометеорологічні дані і характеристики, які мають значення для оборони країни;

2) у сфері економіки, науки і техніки:

– про зміст мобілізаційних планів державних органів та органів місцевого самоврядування, мобілізаційні потужності, заходи мобілізаційної підготовки і мобілізації та обсяги їх фінансування, запаси та обсяги постачання стратегічних видів сировини і матеріалів, а також зведені відомості про номенклатуру та рівні накопичення, загальні обсяги поставок, відпуску, закладення, освіження, розміщення і фактичні запаси державного матеріального резерву;

– про використання транспорту, зв'язку, потужностей інших галузей та об'єктів інфраструктури держави в інтересах забезпечення її безпеки;

– про плани, зміст, обсяг, фінансування та виконання державного оборонного замовлення;

– про плани, обсяги та інші найважливіші характеристики добування, виробництва та реалізації окремих стратегічних видів сировини і продукції;

– про державні запаси дорогоцінних металів монетарної групи, коштовного каміння, валюти та інших цінностей, операції, пов'язані з виготовленням грошових знаків і цінних паперів, їх зберіганням, охороною і захистом від підроблення, обігом, обміном або вилученням з обігу, а також про інші особливі заходи фінансової діяльності держави;

– про наукові, науково-дослідні, дослідно-конструкторські та проектні роботи, на базі яких можуть бути створені прогресивні технології, нові види виробництва, продукції та технологічних процесів, що мають важливе оборонне чи економічне значення або суттєво впливають на зовнішньоекономічну діяльність та національну безпеку України;

3) у сфері зовнішніх відносин:

– про директиви, плани, вказівки делегаціям і посадовим особам з питань зовнішньополітичної і зовнішньоекономічної діяльності України, спрямовані на забезпечення її національних інтересів і безпеки;

– про військове, науково-технічне та інше співробітництво України з іноземними державами, якщо розголошення відомостей про це завдаватиме шкоди національній безпеці України;

– про експорт та імпорт озброєння, військової і спеціальної техніки, окремих стратегічних видів сировини і продукції;

4) у сфері державної безпеки та охорони правопорядку:

– про особовий склад органів, що здійснюють оперативно-розшукову діяльність або розвідувальну чи контррозвідувальну;

– про засоби, зміст, плани, організацію, фінансування та матеріально-технічне забезпечення, форми, методи і результати оперативно-розшукової, розвідувальної і контррозвідувальної діяльності; про осіб, які співпрацюють або раніше співпрацювали на конфіденційній основі з органами, що проводять таку діяльність;

– про склад і конкретних осіб, що є негласними штатними працівниками органів, які здійснюють оперативно-розшукову, розвідувальну і контррозвідувальну діяльність;

– про організацію та порядок здійснення охорони адміністративних будинків та інших державних об'єктів, посадових та інших осіб, охорона яких здійснюється відповідно до Закону України «Про державну охорону органів державної влади України та посадових осіб»;

– про систему урядового та спеціального зв'язку;

– про організацію, зміст, стан і плани розвитку криптографічного захисту секретної інформації, зміст і результати наукових досліджень у сфері криптографії;

– про системи та засоби криптографічного захисту секретної інформації, їх розроблення, виробництво, технологію виготовлення та використання;

– про державні шифри, їх розроблення, виробництво, технологію виготовлення та використання;

– про організацію режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, державні програми, плани та інші заходи у сфері охорони державної таємниці;

– про організацію, зміст, стан і плани розвитку технічного захисту секретної інформації;

– про результати перевірок, здійснюваних згідно з законом прокурором у порядку відповідного нагляду за додержанням законів, та про зміст матеріалів оперативно-розшукової діяльності, досудового розслідування та судочинства з питань, зазначених у цій статті сфер;

– про інші засоби, форми і методи охорони державної таємниці.

Конкретні відомості можуть бути віднесені до державної таємниці за ступенями секретності «особливої важливості», «цілком таємно» та «таємно» лише за умови, що вони належать до категорій, зазначених у законодавстві, і їх розголошення завдаватиме шкоди інтересам національної безпеки України.

Забороняється віднесення до державної таємниці будь-яких відомостей, якщо цим будуть звужуватися зміст і обсяг конституційних прав та свобод людини і громадянина, завдаватиметься шкода здоров'ю та безпеці населення.

Не відноситься до державної таємниці інформація:

– про стан довкілля, про якість харчових продуктів і предметів побуту, про вплив товару (роботи, послуги) на життя та здоров’я людини;

– про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися і загрожують безпеці громадян;

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

– про факти порушень прав і свобод людини і громадянина;

– про незаконні дії державних органів, органів місцевого самоврядування та їх посадових і службових осіб;

– інша інформація, доступ до якої відповідно до законів та міжнародних договорів, не може бути обмежено.

2.3. Комерційна таємниця. Банківська таємниця. Професійна таємниця. Види професійних таємниць згідно із вітчизняним законодавством.

Комерційна таємниця. Цивільний Кодекс України від 16.01.2003 р. № 435-IV визначає комерційну таємницю як інформацію, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці.

Комерційна таємниця є одним з об'єктів інтелектуальної власності. Відповідно майнові права інтелектуальної власності на комерційну таємницю належать особі, яка правомірно визнала інформацію комерційною таємницею, якщо інше не встановлено договором.

Постанова Кабінету Міністрів України від 09.08.1993 р. № 611 встановлено перелік відомостей, що не становлять комерційної таємниці. Серед них:

– установчі документи, документи, що дозволяють займатися підприємницькою чи господарською діяльністю та її окремими видами;

– інформація за всіма встановленими формами державної звітності;

– дані, необхідні для перевірки обчислення і сплати податків та інших обов'язкових платежів;

– відомості про чисельність і склад працюючих, їхню заробітну плату в цілому та за професіями й посадами, а також наявність вільних робочих місць;

– документи про сплату податків і обов'язкових платежів;

– інформація про забруднення навколишнього природного середовища, недотримання безпечних умов праці, реалізацію продукції, що завдає шкоди здоров'ю, а також інші порушення законодавства України та розміри заподіяних при цьому збитків;

– документи про платоспроможність;

– відомості про участь посадових осіб підприємства в кооперативах, малих підприємствах, спілках, об'єднаннях та інших організаціях, які займаються підприємницькою діяльністю;

– відомості, що відповідно до чинного законодавства підлягають оголошенню.

Підприємства зобов'язані подавати перелічені у цій постанові відомості органам державної виконавчої влади, контролюючим і правоохоронним органам, іншим юридичним особам відповідно до чинного законодавства, за їх вимогою.

До комерційної таємниці може належати:

1) технологічна інформація; відомості про управління підприємством; відомості про фінанси підприємства (відомості про систему оплати праці;

2) відомості, що розкривають показники фінансового плану;

3) майнове становище, кількість і вартість товарних запасів;

4) відомості про баланс підприємства; відомості про стан банківських рахунків підприємства, відомості про рівень доходів підприємства);

5) відомості про плани підприємства (плани закупівель, продажу та інвестицій), а також інші відомості, зокрема, такі:

а) собівартість продукції;

б) розмір торговельної націнки;

в) обсяги виробництва продукції;

г) поточні і перспективні плати виробництва; стратегія підприємства;

д) відомості про постачальників, продавців та покупців продукції підприємства;

е) відомості про виробниче обладнання;

є) відомості про способи придбання і реалізації продукції підприємства;

ж) зміст та характер договорів та контрактів, однією із сторін в яких виступає підприємство;

з) відомості щодо обладнання приміщень підприємства охоронною сигналізацією та місця її встановлення.

Банківська таємниця. Відповідно до Закону України «Про банки і банківську діяльність» від 07.12.2000 р. № 2121-III банківською таємницею є інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку і розголошення якої може завдати матеріальної чи моральної шкоди клієнту.

Відзначено, що банківською таємницею, зокрема, є:

1) відомості про стан рахунків клієнтів, у тому числі стан кореспондентських рахунків банків у Національному банку України;

2) операції, які були проведені на користь чи за дорученням клієнта, здійснені ним угоди;

3) фінансово-економічний стан клієнтів;

4) системи охорони банку та клієнтів;

5) інформація про організаційно-правову структуру юридичної особи - клієнта, її керівників, напрями діяльності;

6) відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація;

7) інформація щодо звітності по окремому банку, за винятком тієї, що підлягає опублікуванню;

8) коди, що використовуються банками для захисту інформації.

Інформація про банки чи клієнтів, що збирається під час проведення банківського нагляду, становить банківську таємницю.

Банки зобов'язані забезпечувати збереження банківської таємниці і здійснюють вони це шляхом обмеження кола осіб, що мають доступ до інформації, яка становить банківську таємницю; організації спеціального діловодства з документами, що містять банківську таємницю; застосування технічних засобів для запобігання несанкціонованому доступу до електронних та інших носіїв інформації.

Професійна таємниця. Професійна таємниця – це матеріали, документи, інші відомості, якими користується особа в процесі та у зв’язку з виконанням своїх професійних обов’язків, які забороняється розголошувати у будь-якій формі.

У правовій науці виділені такі критерії, за якими інформація може бути віднесена до професійної таємниці:

по-перше, така інформація довірена або стала відомою особі виключно через виконання нею своїх професійних обов’язків;

по-друге, особа, якій довірено інформацію, не перебуває на державній або муніципальній службі;

по-третє, заборону на поширення довіреної або такої, що стала відомою, інформації, яка може зашкодити правам або законним інтересам довірителя, встановлено законом;

по-четверте, інформація не належить до відомостей, що становлять державну або комерційну таємницю.

Виходячи з наведених вище ознак та із змісту чинного законодавства, можна відзначити, що до професійної таємниці належать такі види інформації з обмеженим доступом: професійна таємниця суддів, адвокатська таємниця, таємниця вчинення нотаріальних дій (нотаріальна таємниця), аудиторська таємниця, лікарська таємниця, таємниця усиновлення та сповіді. До категорії професійної таємниці відносять також і журналістську таємницю.

Професійна таємниця суддів. Резолюція ООН «Основні принципи незалежності судових органів» від 13.12.1985 р. регулюючи питання професійної таємниці та імунітету суддів, гласить, що судді зобов'язані зберігати професійну таємницю щодо своєї роботи та конфіденційної інформації, отриманої в ході виконання ними своїх обов'язків, за винятком відкритих судових розглядів, і їх не можна примушувати давати свідчення з таких питань.

Адвокатська таємниця. У статті 9. Закону України «Про адвокатуру» від 19.12.1992 р. відзначено, що адвокат зобов'язаний зберігати адвокатську таємницю, предметом якої є питання, з яких громадянин або юридична особа зверталися до адвоката, суть консультацій, порад, роз'яснень та інших відомостей, одержаних адвокатом при здійсненні своїх професійних обов'язків.

Нотаріальна таємниця. Відповідно до Закону України «Про нотаріат» від 02.09.1993 р. нотаріус зобов'язаний зберігати в таємниці відомості, одержані ним у зв'язку з вчиненням нотаріальних дій. Обов'язок додержання таємниці вчинюваних нотаріальних дій поширюється також на інших осіб, яким про вчинені нотаріальні дії стало відомо у зв'язку з виконанням ними службових обов'язків.

Аудиторська таємниця. Закон України «Про аудит фінансової звітності та аудиторську діяльність» від 21.12.2017 визначає професійну таємницю аудитора як інформацію (матеріали, документи, інше), що стала відома аудитору в процесі надання аудиторських послуг та відповідає таким ознакам: є невідомою або не є загальнодоступною для широкого кола осіб; розголошення якої може завдати шкоди інтересам особи, яка звернулася до аудитора, суб’єкта аудиторської діяльності.

Лікарська таємниця. Згідно із Основами законодавства України про охорону здоров'я (Закон України від 19.11.1992 р.) медичні працівники та інші особи, яким у зв'язку з виконанням професійних або службових обов'язків стало

відомо про хворобу, медичне обстеження, огляд та їх результати, інтимну і сімейну сторони життя громадянина, не мають права розголошувати ці відомості, крім передбачених законодавчими актами випадків.

При використанні інформації, що становить лікарську таємницю, в навчальному процесі, науково-дослідній роботі, в тому числі у випадках її публікації у спеціальній літературі, повинна бути забезпечена анонімність пацієнта.

Крім того, обов'язок щодо збереження лікарської таємниці передбачено і Клятвою лікаря, затвердженою Указом Президента України від 15.06.1992 р.

Таємниця усиновлення. Сімейний кодекс України від 10.01.2002 р. встановлює права на таємницю усиновлення та приховання факту усиновлення від дитини, яка усиновлена.

Так, особа має право на таємницю перебування на обліку тих, хто бажає усиновити дитину, пошуку дитини для усиновлення, подання заяви про усиновлення та її розгляду, рішення суду про усиновлення. Дитина, яка усиновлена, має право на таємницю, в тому числі і від неї самої, факту її усиновлення. Особа, яка була усиновлена, має право після досягнення нею чотирнадцяти років на одержання інформації щодо свого усиновлення.

Відповідно до Сімейного кодексу усиновлювач має право приховувати факт усиновлення від дитини, яка ним усиновлена, і вимагати нерозголошення цієї інформації особами, яким стало відомо про неї як до, так і після досягнення дитиною повноліття. Також усиновлювач має право приховувати від дитини факт її усиновлення, якщо розкриття таємниці усиновлення може завдати шкоди її інтересам.

Якщо усиновлюється дитина, яка не досягла семи років, службові особи при виявленні її згоди на усиновлення зобов'язані вживати заходів щодо забезпечення таємниці усиновлення від самої дитини.

З метою забезпечення таємниці усиновлення особи, яким у зв'язку з виконанням службових обов'язків доступна інформація щодо усиновлення (перебування осіб, які бажають усиновити дитину, на обліку, пошук ними дитини для усиновлення, подання заяви про усиновлення, розгляд справи про усиновлення, здійснення нагляду за дотриманням прав усиновленої дитини тощо), а також інші особи, яким став відомий факт усиновлення, зобов'язані не розголошувати її, зокрема і тоді, коли усиновлення для самої дитини не є таємним.

Відомості про усиновлення видаються судом лише за згодою усиновлювача, крім випадків, коли такі відомості потрібні правоохоронним органам, суду у зв'язку з цивільною справою чи кримінальним провадженням.

Особи, які розголосили таємницю усиновлення, несуть відповідальність, встановлену законом.

Таємниця сповіді. Закон України «Про свободу совісті та релігійні організації» від 23.04.1991 р. встановлює таємницю сповіді. Відповідно до

статті 3 цього закону ніхто не має права вимагати від священнослужителів відомостей, одержаних ними при сповіді віруючих.

Журналістська таємниця

Закон України «Про інформацію» (стаття 25) гарантує журналістам право не розкривати джерело інформації або інформацію, яка дозволяє встановити джерела інформації, крім випадків, коли їх зобов'язано до цього рішенням суду на основі закону. Ідентична норма міститься і у статті 26 Закону України «Про пресу».

2.4. Персональні дані. Об'єкти захисту. Вимоги до обробки персональних даних.

Закон України «Про захист персональних даних» від 01.06.2010 р. № 2297-VI під персональними даними розуміє відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Персональні дані є об’єктами захисту.

Персональні дані можуть бути віднесені до конфіденційної інформації про особу законом або відповідною особою. Не є конфіденційною інформацією персональні дані, що стосуються здійснення особою, яка займає посаду, пов’язану з виконанням функцій держави або органів місцевого самоврядування, посадових або службових повноважень.

Персональні дані, зазначені у декларації про майно, доходи, витрати і зобов’язання фінансового характеру, оформленій за формою і в порядку, встановленими Законом України «Про засади запобігання і протидії корупції», не належать до інформації з обмеженим доступом, крім відомостей, визначених Законом України «Про засади запобігання і протидії корупції».

Не належить до інформації з обмеженим доступом інформація про отримання у будь-якій формі фізичною особою бюджетних коштів, державного чи комунального майна, крім випадків, передбачених статтею 6 Закону України «Про доступ до публічної інформації».

Законом може бути заборонено віднесення інших відомостей, що є персональними даними, до інформації з обмеженим доступом.

Відповідно до закону не допускається обробка даних про фізичну особу, які є конфіденційною інформацією, без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Закон визначає особливі вимоги до обробки персональних даних. Зокрема, забороняється обробка персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров’я, статевого життя, біометричних або генетичних даних.

Зазначене правило не діє, якщо обробка персональних даних:

1) здійснюється за умови надання суб'єктом персональних даних однозначної згоди на обробку таких даних;

2) необхідна для здійснення прав та виконання обов'язків володільця у сфері трудових правовідносин відповідно до закону із забезпеченням відповідного захисту;

3) необхідна для захисту життєво важливих інтересів суб'єкта персональних даних або іншої особи у разі недієздатності або обмеження цивільної дієздатності суб'єкта персональних даних;

4) здійснюється із забезпеченням відповідного захисту релігійною організацією, громадською організацією світоглядної спрямованості, політичною партією або професійною спілкою, що створені відповідно до закону, за умови, що обробка стосується виключно персональних даних членів цих об'єднань або осіб, які підтримують постійні контакти з ними у зв'язку з характером їх діяльності, та персональні дані не передаються третій особі без згоди суб'єктів персональних даних;

5) необхідна для обґрунтування, задоволення або захисту правової вимоги;

6) необхідна в цілях охорони здоров’я, встановлення медичного діагнозу, для забезпечення піклування чи лікування або надання медичних послуг за умови, що такі дані обробляються медичним працівником або іншою особою закладу охорони здоров’я, на якого покладено обов’язки щодо забезпечення захисту персональних даних та на якого поширюється законодавство про лікарську таємницю;

7) стосується вироків суду, виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом та здійснюється державним органом в межах його повноважень, визначених законом;

8) стосується даних, які були явно оприлюднені суб'єктом персональних даних.

Наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 р. затверджено Типовий порядок обробки персональних даних, Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних та Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб’єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу.

Відповідно до встановлених змін, відмінюється реєстрація баз персональних даних, а в свою чергу затверджено процедуру та форму повідомлення Уповноваженого про обробку персональних даних, яка становить особливий ризик для прав і свобод суб’єктів персональних даних, про зміну відомостей, що підлягають повідомленню, та про структурний підрозділ або відповідальну особу, що організовує роботу, пов’язану із захистом персональних даних при їх обробці.

До таких даних відносяться дані про:

– расове, етнічне та національне походження,

– політичні, релігійні або світоглядні переконання, членство в політичних партіях та/або організаціях, професійних спілках, релігійних організаціях чи в громадських організаціях світоглядної спрямованості,

– стан здоров'я, статеве життя, біометричні дані, генетичні дані,

– притягнення до адміністративної чи кримінальної відповідальності, застосування щодо особи заходів в рамках досудового розслідування, вжиття щодо особи заходів, передбачених Законом України «Про оперативно-розшукову діяльність»,

– вчинення щодо особи тих чи інших видів насильства,

– місцеперебування та/або шляхи пересування особи.

Питання для самоконтролю

1. Які види інформації з обмеженим доступом визначено у законодавстві України? Дайте визначення конфіденційної, таємної та службової інформації.

2. Який гриф присвоюють документам, які містять службову інформацію?

3. Які категорії інформації і в яких галузях можуть належати до державної таємниці? Назвіть види інформації, які не можуть бути віднесені до державної таємниці.

4. Яка інформація не може бути віднесена до комерційної таємниці?

5. Що таке банківська таємниця? Назвіть види інформації, які становлять банківську таємницю.

6. Які види професійних таємниць згідно із вітчизняним законодавством ви знаєте? Поясніть їх сутність.

7. Що таке персональні дані? Зазначте вимоги до обробки персональних даних.

8. Які особливі вимоги до обробки персональних даних визначені у законодавстві України?

ТЕМА 3. Національні інтереси в інформаційній сфері. Загрози інформаційній безпеці держави, суспільства, особи. Джерела загроз.

3.1. Національні інтереси в інформаційній сфері.

Категорія «національні інтереси» є багатокомпонентною. Через це постає необхідність у класифікації національних інтересів, виокремленні фундаментальних (базових), життєво важливих та інших груп національних інтересів. При цьому класифікація національних інтересів має розглядатися крізь призму необхідності виокремлення тих з них, завдання шкоди яким свідчить про національну небезпеку.

Життєво важливі інтереси можна визначати і як усвідомлені на рівні вищих органів державної влади *потреби* народу у збереженні й розвитку національних цінностей, національного багатства, вдосконалення економічного й політичного устрою суспільства.

Під *національними потребами* розуміють такий стан нації, який виражає необхідність у чомусь, обумовлений її незадоволеністю умовами життєдіяльності та спрямований на усунення цієї незадоволеності. Національні потреби реалізується у самому процесі їх задоволення. У разі ж незадоволення потреби нації це призводить до зміни нормальної життєдіяльності або ж до неможливості її подальшого існування.

Відповідно до Закону України «Про національну безпеку» від 21.06.2018 національні інтереси України - життєво важливі інтереси людини, суспільства і держави, реалізація яких забезпечує державний суверенітет України, її прогресивний демократичний розвиток, а також безпечні умови життєдіяльності і добробут її громадян.

Зазначений Закон України встановлює такі фундаментальні національні інтереси України:

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

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

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

Водночас варто також серед пріоритетних виділити такі національні інтереси України:

- гарантування конституційних прав і свобод людини і громадянина;
- розвиток громадянського суспільства, його демократичних інститутів;
- зміцнення політичної і соціальної стабільності в суспільстві;

– забезпечення розвитку і функціонування української мови як державної в усіх сферах суспільного життя на всій території України, гарантування вільного розвитку, використання і захисту російської, інших мов національних меншин України;

– збереження та зміцнення науково-технологічного потенціалу, утвердження інноваційної моделі розвитку;

– забезпечення екологічно та техногенно безпечних умов життєдіяльності громадян і суспільства, збереження навколишнього природного середовища та раціональне використання природних ресурсів;

– розвиток духовності, моральних засад, інтелектуального потенціалу Українського народу, зміцнення фізичного здоров'я нації, створення умов для розширеного відтворення населення.

На думку фахівців, в інформаційній сфері народ України має дві категорії життєво важливих інтересів: інтереси особи та інтереси суспільства і держави.

До життєво важливих інтересів особи відносять забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; забезпечення конституційних прав людини на захист приватного життя; захищеність від руйнівних інформаційно-психологічних впливів;

Життєво важливі інтереси суспільства і держави включають:

– захист українського суспільства від агресивного впливу деструктивної пропаганди з боку інших держав;

– всебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності у доступі до достовірної та об'єктивної інформації;

– забезпечення вільного обігу інформації, крім випадків, передбачених законом;

– розвиток та захист національної інформаційної інфраструктури;

– збереження і примноження духовних, культурних і моральних цінностей Українського народу;

– забезпечення всебічного розвитку і функціонування української мови в усіх сферах суспільного життя на всій території України;

– вільний розвиток, використання і захист мов національних меншин та сприяння вивченню мов міжнародного спілкування;

– зміцнення інформаційних зв'язків з українською діаспорою, сприяння збереженню її етнокультурної ідентичності;

– розвиток медіа-культури суспільства та соціально відповідального медіа-середовища;

– формування ефективної правової системи захисту особи, суспільства та держави від деструктивних пропагандистських впливів;

– створення з урахуванням норм міжнародного права системи і механізмів захисту від негативних зовнішніх інформаційно-психологічних впливів, передусім пропаганди;

– розвиток інформаційного суспільства, зокрема його технологічної інфраструктури;

– безпечне функціонування і розвиток національного інформаційного простору та його інтеграція у європейський і світовий інформаційний простір;

– розвиток системи стратегічних комунікацій України;

– ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації державної політики в інформаційній сфері;

– забезпечення розвитку інформаційно-комунікаційних технологій та інформаційних ресурсів України;

– захищеність державної таємниці та іншої інформації, вимоги щодо захисту якої встановлені законом;

– формування позитивного іміджу України у світі, донесення оперативної, достовірної і об'єктивної інформації про події в Україні до міжнародної спільноти;

– розбудова системи іномовлення України та забезпечення наявності іншомовного українського каналу в кабельних мережах та у супутниковому мовленні за межами України.

3.2. Сутність поняття «загроза» та наукові підходи до класифікації загроз інформаційній безпеці.

У науковій думці загрозу визначають як крайню ступінь небезпеки (безпосередню небезпеку); будь-який потенційно можливий несприятливий вплив, стадію крайнього загострення протиріч, безпосередньо передконфліктний стан тощо.

На думку фахівців з національної безпеки, загроза - це стадія крайнього загострення протиріч, безпосередньо передконфліктний стан, коли в наявності готовність одного із суб'єктів політики застосувати силу стосовно іншого конкретного об'єкта для досягнення своїх політичних та інших цілей. Небезпеку ж розуміють як стадію зародження і насичення протиріч, коли один із суб'єктів політики потенційно може, але ще не готовий застосувати силу або загрозу сили в своїх інтересах.

Загроза повинна містити в собі два компоненти: наміри і можливість нанесення збитку інтересам безпеки, а небезпека обмежується наявністю тільки однієї з цих компонент.

Загроза має персоніфікований, конкретно-адресний характер, що припускає наявність очевидних суб'єкта (джерела) загрози і об'єкта, на який спрямована її дію. На відміну від загрози небезпека носить гіпотетичний, часто безадресний характер, її суб'єкт і об'єкт явно не виражені.

Небезпека містить у собі потенційну загрозу заподіяння шкоди тим чи іншим інтересам, для реалізації якої необхідне створення відповідних умов (накопичення можливостей і формування намірів), загроза ж є безпосередня

можливість нанесення збитку, від початку здійснення якої її відділяє лише часовий інтервал, необхідний для прийняття рішення про реалізацію загрози.

Незважаючи на наявність різних підходів до визначення поняття «загроза», більшість учених сходяться на думці, що загрози:

– мають динамічний, змінний характер і включають події, зміни або дії;

– спричиняють шкоду або порушення нормального функціонування об’єкта (держави), і як наслідок є причиною збитків та втрат;

– виникають під дією певних чинників (зовнішніх та внутрішніх), і тому потребують комплексу заходів з боку держави для їх нейтралізації та усунення.

Загроза інформаційній безпеці - явище, дії негативних чинників або процес, через які: соціальні об’єкти інформаційної безпеки частково або повністю втрачають можливість реалізувати свої інтереси в інформаційній сфері; а також, порушується нормальне функціонування, здійснюється руйнація або стримується розвиток технічних об’єктів інформаційної безпеки.

Як бачимо з наведеного визначення загрози інформаційній безпеці поділяють на два види: соціальні (обмеження чи неспроможність особи та суспільства загалом реалізувати ключові інтереси в інформаційній сфері) та технічні (порушення функціонування та виведення з ладу інформаційної інфраструктури та інформаційних ресурсів зокрема).

Фахівці пропонують декілька підходів до класифікації загроз інформаційній безпеці. Так, на думку авторів термінологічного навчального довідника з інформаційної безпеки, всі загрози інформаційній безпеці особи можна поділити на такі основні групи:

– загрози шкідливого впливу відповідної інформації (недостовірної, шкідливої, дезінформації) на особистість;

– загрози несанкціонованого чи неправомірного впливу сторонніх осіб на інформацію й інформаційні ресурси фізичної особи;

– загрози обмеженню інформаційних прав особистості, механізмам їх реалізації.

Відповідно до іншого підходу виділяють декілька типів інформаційних загроз, серед яких політичні, економічні, суспільні, військові та науково-технічні. Так, у політичній сфері - загрози системі інформаційно-аналітичного забезпечення державних органів, загрози правам особи, суспільства на отримання інформації про діяльність органів державної влади та участь у прийнятті державно-управлінських рішень; в економічній - загрози, пов’язані з використанням е-комерції, банківських послуг, промислове шпигунство тощо; у суспільній - загрози для забезпечення основних прав і свобод людини, негативний вплив на системи інформування через ЗМІ та формування громадської думки; у військовій – загрози системі оборони держави (виведення з ладу критичної військової інформаційної інфраструктури, негативний вплив на керівництво та особовий склад збройних сил); в науково-технічній – загрози об’єктам інтелектуальної власності та конфіденційним даним.

Інші підходи до класифікації загроз інформаційній безпеці представлено нижче.

За джерелами походження

природного походження	небезпечні геологічні, метеорологічні, гідрологічні явища, деградація ґрунтів чи надр, природні пожежі, масове руйнування (через природні катаклізми) каналів зв'язку тощо
техногенного походження	транспортні аварії (катастрофи), пожежі, неспровоковані вибухи чи їх загроза, раптове руйнування каналів зв'язку, аварії на інженерних мережах і спорудах життєзабезпечення, аварії серверів та автоматизованих систем управління критичних об’єктів тощо
антропогенного походження	вчинення людиною різноманітних дій з руйнування інформаційних систем, ресурсів, програмного забезпечення тощо. До цієї групи за змістом дій належать: ненавмисні, викликані помилковими чи ненавмисними діями людини; навмисні (інспіровані), результат навмисних дій людей

За повторюваністю вчинення

повторювані	загрози, які мали місце раніше
продовжувані	неодноразове здійснення загроз, що складається з ряду тотожних загроз, які мають спільну мету

За сферами походження

екзогенні	джерело дестабілізації системи лежить поза її межами
ендогенні	джерело дестабілізації системи перебуває у самій системі

За ймовірністю реалізації

вірогідні	загрози, які за наявності певного комплексу умов обов'язково настануть
неможливі	загрози, які навіть за виконання певного комплексу умов ніколи не настануть. Такі загрози зазвичай мають більш декларативний, часто залякувальний характер
випадкові	загрози, які за виконання певного комплексу умов кожного разу реалізуються по-різному

За рівнем визначеності

закономірні	загрози, які носять стійкий, повторюваний характер, що зумовлені об'єктивними умовами існування та розвитку системи. Так, наприклад, за умови відсутності системи інформаційної безпеки будь-який суб'єкт закономірно піддаватиметься інформаційним атакам

випадкові загрози, які можуть або трапитися або не трапитися за певних умов

За значенням

допустимі загрози, які не можуть призвести до виведення з ладу системи

неприпустимі загрози, які: у разі їх реалізації можуть призвести до колапсу і системної дестабілізації системи або до змін, не сумісних із подальшим існуванням системи

За структурою впливу

системні загрози, що впливають одразу на усі складові елементи системи

структурні загрози, що впливають на окремі структури системи

елементні загрози, що впливають на окремі елементи структури системи. Такі загрози мають постійний характер і можуть бути небезпечними лише за умови неефективності або непроведення їх моніторингу

За характером реалізації

реальні активізація алгоритмів дестабілізації є неминучою і не обмежена часовим інтервалом і просторовою дією

потенційні активізація алгоритмів дестабілізації можлива за певних умов функціонування системи

здійснені загрози, які втілені у життя

уявні псевдореалізація механізмів дестабілізації, або ж активізація таких механізмів, що за деякими ознаками схожі з алгоритмами дестабілізації, але не є такими

За ставленням до них

об'єктивні загрози, які підтверджуються сукупністю обставин і фактів, що об'єктивно характеризують навколишнє середовище. При цьому ставлення до них суб'єкта управління не відіграє вирішальної ролі через те, що об'єктивні загрози існують незалежно від волі та свідомості суб'єкта

суб'єктивні така сукупність чинників об'єктивної дійсності, яка вважається загрозою суб'єктом управління. У такому випадку визначальну роль у ідентифікації загрози відіграє воля суб'єкта управління, який і приймає безпосереднє рішення про надання статусу або ідентифікації тих чи інших подій в якості загроз безпеці

Розглядаючи загрози інформаційній безпеці держави, слід виокремити

серед них загрози інтересам *особи, суспільства* та власне *держави* в інформаційній сфері.

Вартим уваги є підхід, відповідно до якого загрози інформаційній безпеці групують за сферами діяльності держави:

1) у зовнішньополітичній сфері:

– поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України;

– прояви комп'ютерної злочинності, комп'ютерного тероризму, що загрожують сталому та безпечному функціонуванню національних інформаційно-телекомунікаційних систем;

– зовнішні негативні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також мережу Інтернет;

2) у сфері державної безпеки:

– негативні інформаційні впливи, спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності і недоторканності кордонів України;

– використання засобів масової інформації, а також мережі Інтернет для пропаганди сепаратизму за етнічною, мовною, релігійною та іншими ознаками;

– несанкціонований доступ до інформаційних ресурсів органів державної влади;

– розголошення інформації, яка становить державну та іншу передбачену законодавством таємницю, а також конфіденційної інформації, що є власністю держави;

3) у воєнній сфері:

– порушення встановленого регламенту збирання, обробки, зберігання і передачі інформації з обмеженим доступом в органах військового управління та на підприємствах оборонно-промислового комплексу України;

– несанкціонований доступ до інформаційних ресурсів, незаконне збирання та використання інформації з питань оборони;

– реалізація програмно-математичних заходів з метою порушення функціонування інформаційних систем у сфері оборони України;

– перехоплення інформації в телекомунікаційних мережах, радіоелектронне глушіння засобів зв'язку та управління;

– інформаційно-психологічний вплив на населення України, у тому числі на особовий склад військових формувань, з метою послаблення їх готовності до оборони держави та погіршення іміджу військової служби;

4) у внутрішньополітичній сфері:

– недостатня розвиненість інститутів громадянського суспільства, недосконаліть партійно-політичної системи, непрозорість політичної та громадської діяльності, що створює передумови для обмеження свободи слова, маніпулювання суспільною свідомістю;

– негативні інформаційні впливи, в тому числі із застосуванням спеціальних засобів, на індивідуальну та суспільну свідомість;

– поширення суб'єктами інформаційної діяльності викривленої, недостовірної та упередженої інформації;

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

5) в економічній сфері:

– відставання вітчизняних наукоємних і високотехнологічних виробництв, особливо у сфері телекомунікаційних засобів і технологій;

– недостатній рівень інформатизації економічної сфери, зокрема кредитно-фінансової системи, промисловості, сільського господарства, сфери державних закупівель;

– несанкціонований доступ, порушення встановленого порядку роботи з інформаційними ресурсами в галузях національної економіки, викривлення інформації в таких ресурсах;

– використання неліцензованого і несертифікованого програмного забезпечення, засобів і комплексів обробки інформації;

– недостатній рівень розвитку національної інформаційної інфраструктури;

6) у соціальній та гуманітарній сферах:

– відставання України від розвинутих держав за рівнем інформатизації соціальної та гуманітарної сфер, насамперед освіти, охорони здоров'я, соціального забезпечення, культури;

– недодержання прав людини і громадянина на одержання інформації, необхідної для захисту їх соціально-економічних прав;

– поширення в засобах масової інформації невластивих українській культурній традиції цінностей і способу життя, культу насильства, жорстокості, порнографії, зневажливого ставлення до людської і національної гідності;

– тенденція до витіснення з інформаційного простору та молодіжної культури українських мистецьких творів, народних традицій і форм дозвілля;

– послаблення суспільно-політичної, міжетнічної та міжконфесійної єдності суспільства;

– відставання рівня розвитку українського кінематографу, книговидання, книгорозповсюдження та бібліотечної справи від рівня розвинутих держав;

7) у науково-технологічній сфері:

– зниження наукового потенціалу в галузі інформатизації та зв'язку;

– низька конкурентоспроможність вітчизняної інформаційної продукції на світовому ринку;

– відтік за кордон наукових кадрів та суб'єктів права інтелектуальної власності;

– недостатній захист від несанкціонованого доступу до інформації внаслідок використання іноземних інформаційних технологій та техніки;

– неконтрольована експансія сучасних інформаційних технологій, що створює передумови технологічної залежності України;

– комп'ютерна злочинність та комп'ютерний тероризм;

8) в екологічній сфері:

– приховування, несвоєчасне надання інформації або надання недостовірної інформації населенню про надзвичайні екологічні ситуації чи надзвичайні ситуації техногенного та природного характеру;

– недостатня надійність інформаційно-телекомунікаційних систем збирання, обробки та передачі інформації в умовах надзвичайних ситуацій;

– низький рівень інформатизації органів державної влади, що унеможливлює здійснення оперативного контролю та аналізу стану потенційно небезпечних об'єктів і територій, завчасного прогнозування та реагування на надзвичайні ситуації.

У Стратегії національної безпеки України, затвердженій Указом Президента України від 26.05.2015 р. № 287/2015 виділено дві групи загроз в інформаційній сфері:

– *загрози інформаційній безпеці*. До цієї групи загроз віднесено ведення інформаційної війни проти України; відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства;

– *загрози кібербезпеці і безпеці інформаційних ресурсів*, серед яких уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом.

3.3. Джерела загроз інформаційній безпеці держави.

Носіями загроз безпеці інформації є *джерела загроз*.

Джерелами загроз можуть виступати як суб'єкти (особистість, група, організація, держава), так і об'єктивні прояви. Причому, джерела загроз можуть бути і всередині держави - внутрішні джерела, і за її межами - зовнішні джерела.

Усі джерела загроз інформаційній безпеці подялюють на три основні групи: антропогенні джерела загроз (джерелом є суб’єкт); техногенні джерела загрози (джерелом є технічні засоби) стихійні джерела (джерелом загрози є природні явища).

Антропогенними джерелами загроз інформаційній безпеці виступають суб'єкти, дії яких можуть нанести шкоду інформаційній безпеці держави, суспільства, особистості.

Суб'єкти (джерела), дії яких можуть призвести до нанесення шкоди інформаційній безпеці можуть бути як зовнішні, і внутрішні. Вони можуть бути випадковими чи навмисними, володіти різним рівнем кваліфікації.

До зовнішніх джерел загроз інформаційній безпеці держави належать:

– іноземні політичні, економічні, військові, розвідувальні та інформаційні структури, діяльність яких спрямована проти інтересів держави в інформаційній сфері;

– іноземні держави;

– міжнародні, державні та приватні гравці, які беруть участь у міжнародній конкуренції за володіння та створення конкурентоспроможних інформаційних технологій та ресурсів;

– міжнародні терористичні організації, кримінальні структури;

– потенційні злочинці і хакери.

Внутрішніми джерелами загроз інформаційній безпеці держави можуть бути:

– високопосадовці органів державної влади, політики, представники силових структур (з огляду на те, що вони володіють найбільшою кількістю конфіденційної інформації відповідно до займаного ними положення в державно-управлінській ієрархії);

– представники політичних партій, громадських організацій, ЗМІ;

– лідери громадської думки, наукова, культурна та мистецька еліта;

– представники релігійних організацій;

– потенційні злочинці і хакери.

Техногенні джерела загроз включають джерела загроз, зумовлені технократичною діяльністю людини й розвитком цивілізації. Однак, наслідки, викликані такою діяльністю вийшли з під контролю людини і розвиваються у власний спосіб. Ці джерела загроз менш прогнозовані, безпосередньо залежать від властивостей техніки і тому вимагають особливої уваги.

Джерелами потенційних загроз інформаційній безпеці є такі технічні засоби як: засоби зв'язку; мережі інженерних комунікацій (водопостачання, каналізації); неякісні технічні засоби обробки інформації; неякісні програмні засоби обробки інформації; допоміжні засоби (охорони, сигналізації, телефонії) тощо.

Третя група джерел - *стихійні джерела загроз* - об'єднує обставини, які становлять нездоланну силу, тобто такі обставини, які мають об'єктивний, і абсолютний характер, поширюються на усіх. До непереборної сили у законодавстві і договірній практиці відносять стихійні лиха чи інші обставини, які неможливо передбачити чи запобігти /або можливо передбачити, але неможливо запобігти при рівні людського знання і набутих можливостей. До стихійних джерел потенційних загроз інформаційній безпеці відносять передусім природні катаклізми, пожежі; землетруси; повені; урагани; різні непередбачувані обставини; незрозумілі явища; інші форс-мажорні обставини.

Відповідно до іншого підходу виділяють такі джерела загроз інформаційній безпеці держави, суспільства, особистості.

Зовнішні джерела:

– діяльність іноземних політичних, економічних, військових, розвідувальних та інформаційних структур, спрямована проти інтересів держави в інформаційній сфері;

– прагнення ряду країн до домінування і утискання інтересів держави в світовому інформаційному просторі, витіснення її з зовнішнього і внутрішнього інформаційних ринків;

– загострення міжнародної конкуренції за володіння інформаційними технологіями та ресурсами;

– діяльність міжнародних терористичних організацій;

– збільшення технологічного відриву провідних держав світу і нарощування їх можливостей з протидії створенню конкурентоспроможних інформаційних технологій;

– діяльність космічних, повітряних, морських і наземних технічних та інших засобів (видів) розвідки іноземних держав;

– розробка низкою держав концепцій інформаційних війн, які передбачають створення засобів небезпечного впливу на інформаційні сфери інших країн світу, порушення нормального функціонування інформаційних і телекомунікаційних систем, збереження інформаційних ресурсів, отримання несанкціонованого доступу до них;

– культурна експансія з боку інших держав.

Внутрішні джерела:

– критичний стан вітчизняних галузей промисловості;

– несприятлива криміногенна обстановка, що супроводжується тенденціями зрощування державних і кримінальних структур в інформаційній сфері, отримання кримінальними структурами доступу до конфіденційної інформації, посилення впливу організованої злочинності на життя суспільства, зниження ступеня захищеності законних інтересів громадян, суспільства і держави в інформаційній сфері;

– недостатня координація діяльності державних органів державної влади, регіональних органів державної влади з формування та реалізації єдиної державної політики в галузі забезпечення інформаційної безпеки;

– недостатня розробленість нормативної правової бази, що регулює відносини в інформаційній сфері, а також недостатня правозастосовна практика;

– нерозвиненість інститутів громадянського суспільства і недостатній державний контроль за розвитком інформаційного ринку;

– недостатнє фінансування заходів щодо забезпечення інформаційної безпеки;

– недостатня економічна міць держави;

– зниження ефективності системи освіти і виховання, недостатня кількість кваліфікованих кадрів в галузі забезпечення інформаційної безпеки;

– недостатня активність органів державної влади в інформуванні суспільства про свою діяльність, в роз'ясненні прийнятих рішень, у формуванні відкритих державних ресурсів і розвитку системи доступу до них громадян;

– відставання від провідних країн світу за рівнем інформатизації органів державної влади і органів місцевого самоврядування, кредитно-фінансової сфери, промисловості, сільського господарства, освіти, охорони здоров'я, сфери послуг та побуту;

– відсутність історичного, політичного та соціального досвіду життя у правовій державі, що торкається процесу практичної реалізації конституційних прав та свобод громадян, в тому числі в інформаційній сфері;

– посилення організованої злочинності та збільшення кількості комп'ютерних злочинів;

– постійне вдосконалення інформаційних систем та мереж зв’язку загалом, критичних інфраструктур зокрема;

– можливість концентрації ЗМІ в руках невеликої кількості власників і як наслідок формування ними інформаційного простору;

– зростання можливостей маніпулювання свідомістю широких мас населення за рахунок різноманітних технологій, формування віртуального простору;

– використання персональних даних особи на шкоду її інтересам, розширення прихованих можливостей збирання приватної інформації.

Питання для самоконтролю

1. Що таке національні інтереси?
2. Які життєво важливі інтереси в інформаційній сфері визначає Доктрина інформаційної безпеки України?
3. Що таке загроза? Поясність сутність поняття «загроза інформаційній безпеці держави».
4. Які підходи до класифікації загроз інформаційній безпеці ви знаєте?
5. Які групи загроз в інформаційній сфері виділено у Стратегії національної безпеки України (2015)?
6. Що таке джерело загрози?
7. Які види джерел загроз інформаційній безпеці ви знаєте? Назвіть приклади зовнішніх та внутрішніх джерел загроз інформаційній безпеці держави.

ТЕМА 4. Інформаційний суверенітет держави. Інформаційний та електронний суверенітет. Основні завдання щодо забезпечення інформаційного суверенітету України.

4.1. Сутність поняття «суверенітет». Інформаційний суверенітет держави.

Розглянемо сутність поняття «суверенітет». Суверенітет (від франц. «Souverainete» - найвища влада) - верховенство, повнота і зовнішня незалежність державної влади, які виявляються у відповідних формах будови та внутрішньої і зовнішньополітичної діяльності держави.

Відповідно до іншого визначення суверенітет - це політико-правова властивість держави, зміст якої полягає в її праві самостійно вирішувати внутрішні та зовнішні політичні питання без втручання інших держав, організацій, осіб.

Міжнародне право визначає зміст поняття суверенітету та його складові, такі як верховенство, самостійність, повноту і неподільність влади в межах її території та незалежність і рівноправність у зовнішніх зносинах.

Соціальною цінністю суверенітету є юридична самостійність держави, котра виявляється в непідкоренні іншій державі або групі держав, тобто незалежність від чужої волі. Однак ця незалежність не означає непідкорення міжнародному праву і не повинна бути теоретичним обґрунтуванням самоізоляції, відокремлення.

Інформаційний суверенітет є похідним від державного суверенітету, але не є рівнозначним останньому. До формування поняття «інформаційний суверенітет» доцільно підходити, виходячи з того, що суверенітет, як відзначалося вище, - це верховна влада у внутрішніх справах і незалежність у зовнішніх відносинах.

Розглядаючи підходи до розуміння інформаційного суверенітету у вітчизняному законодавстві та науковій думці, слід відзначити, що в них містяться різні за змістом положення.

Закон України «Про національну програму інформатизації» визначає інформаційний суверенітет держави як здатність держави контролювати й регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки. На думку фахівців, таке визначення є неповним і суперечить нормам інших законодавчих актів.

Відповідно до одного з наукових бачень, під інформаційним суверенітетом України розуміють невід'ємне право людини, суспільства, держави на самовизначення та участь у формуванні, розвитку та здійсненні національної інформаційної політики відповідно до Конституції, чинного законодавства України, міжнародного права в національному інформаційному просторі України.

На думку авторів даної концепції, інформаційний суверенітет України забезпечується:

– виключним правом власності України на інформаційні ресурси, що формуються за рахунок коштів державного бюджету;

– створенням національних систем інформації;

– встановленням режиму доступу інших держав до інформаційних ресурсів України;

– використанням інформаційних ресурсів на основі рівноправного співробітництва з іншими державами.

Інформаційний суверенітет України, крім цього, має забезпечуватися проведенням цілісної державної інформаційної політики відповідно до Конституції, чинного законодавства України і норм міжнародного права шляхом реалізації відповідних доктрин, стратегій, концепцій та програм в інформаційній сфері. Важливим елементом інформаційного суверенітету є належний стан інформаційної безпеки держави, суспільства та його громадян.

Інформаційний суверенітет у відносинах з іншими країнами передбачає рівноправність, взаємовигідність міждержавного інформаційного обміну та взаємну повагу до національних інтересів та прав суверенних і незалежних держав.

У рамках іншого підходу інформаційний суверенітет визначено як право держави на формування і здійснення національної інформаційної політики відповідно до Конституції і законодавства України, міжнародного права в національному інформаційному просторі України.

Аналізуючи сутність інформаційного суверенітету, слід зауважити, що в Україні та світі загалом тривають активні дискусії щодо визначення у правовому плані поняття «інформаційний суверенітет» та правових норм його забезпечення.

Деякі дослідники, розвиваючи ідею вільного потоку інформації, узагалі заперечують можливість існування такого виду суверенітету, а також відокремленого національного інформаційного простору, що, на їхню думку, спростовується розвитком інформаційних технологій та інформаційних відносин у процесі глобалізації та інформатизації. Відовідно до цього підходу моделювання окремого «інформаційного» виду суверенітету суперечить положенням цілого ряду міжнародно-правових актів, починаючи з Міжнародного пакту про громадянські й політичні права, якими встановлюється, що принципи свободи слова та інформації діють незалежно від державних кордонів, а, отже, може призвести до неправомірного обмеження права на інформацію.

Крім того прихильники такого підходу наполягають на тому, що сьогодні суверенітет уже не розглядається як абсолютна цінність і протиставляється правам людини, праву націй на самовизначення тощо, а також багато сучасних держав нездатні ефективно управляти в умовах глобалізації, що, на їх думку, викликає необхідність створення нових систем управління, наприклад

управління за мережевим принципом та побудову за таким принципом організацій, здатних розв'язувати глобальні проблеми.

Критики такого «нового світового порядку» та глобального управління називають вищеокреслену доктрину «новим інтервенціонізмом», обстоюють погляд на суверенітет як абсолютну цінність, а державу розглядають як невід'ємний елемент міжнародного порядку.

Більшість вітчизняних дослідників стоять на аналогічній позиції і підтримують ідеї нормативного закріплення інформаційного суверенітету, який не тільки не суперечить міжнародним стандартам щодо реалізації громадянами та іншими суб'єктами права на інформацію, а навпаки, створює стан захищеності для реалізації цього права. Крім того, вони зауважують, що розглядати інформаційний суверенітет у географічному, територіальному контексті недоцільно, оскільки сьогодні уявлення про інформаційний суверенітет у науковій спільноті характеризуються параметрами, відмінними від топографічних.

Так, згідно, наприклад, з однією з найбільш повних у вітчизняній науці дефініцій, запропонованою В. О. Олійником, О. В. Сосніним та Л. Є. Шиманським, *інформаційний суверенітет* розглядається як «виключне право України відповідно до Конституції і законодавства України та норм міжнародного права самостійно і незалежно, з додержанням балансу інтересів особи, суспільства і держави визначати й здійснювати внутрішні і геополітичні національні інтереси в інформаційній сфері, державну внутрішню і зовнішню інформаційну політику, розпоряджатися власними інформаційними ресурсами, формувати інфраструктуру національного інформаційного простору, створювати умови для його інтегрування у світовий інформаційний простір та гарантувати інформаційну безпеку держави».

Проаналізувавши основні підходи до визначення поняття «інформаційний суверенітет», необхідно звернути увагу, що з точки зору політико-правового навантаження воно має подвійний характер: з одного боку інформаційний суверенітет – це виключно право держави та її можливості, з іншого – це основні функціональні напрями (завдання) державної діяльності.

У контексті принципів права інформаційному суверенітету притаманні такі принципи: законності; принип суверенної рівності держав; невтручання у внутрішні справи держави в інформаційній сфері; адекватної поінформованості держав; формування системи інформаційного суверенітету, як частини загальної системи національної безпеки країни; відкритості інформації про діяльність суб'єктів забезпечення інформаційного суверенітету, що не становить державну таємницю.

Необхідним для належного забезпечення державою інформаційного суверенітету є такі чинники, як: наявність повноцінного права на інформацію у всіх суб'єктів інформаційних соціальних відносин; реалізація державою інформаційного суверенітету включає забезпечення її інформаційної безпеки; реалізація інформаційного суверенітету повинна ґрунтуватися на основі

інформаційної свободи та рівноправності суб'єктів інформаційних відносин; інформаційний суверенітет держави неможливий без захищеності інформаційної приватності особи в цій державі

4.2. Інформаційний та електронний суверенітет.

З огляду на зростання обсягів інформатизації усіх сфер життєдіяльності суспільства та масштабів виникнення нових загроз інформаційного характеру у науці та практиці відзначено наявність двох компонентів інформаційного суверенітету у сучасному світі – *технологічного* та *контентного (змістовного)*, кожен з яких має бути повноцінно забезпеченим реальними кроками держави.

Так, необхідним є забезпечення електронного (кібер) суверенітету, який формуватиме технологічну основу забезпеченості контентної (змістовної) складової інформаційного суверенітету. Особливої важливості такий підхід набуває сьогодні, коли інформаційне протиборство відіграє фактично основну роль у вирішенні геополітичних, внутрішньополітичних, економічних суперечок.

Відповідно до існуючої концепції цифровий (електронний) суверенітет передбачає право і можливість уряду держави самостійно і незалежно визначати і внутрішні і геополітичні національні інтереси в цифровій сфері; вести самостійну внутрішню і зовнішню інформаційну політику; розпоряджатися власними інформаційними ресурсами, формувати інфраструктуру національного інформаційного простору; гарантувати електронну безпеку держави.

Електронний суверенітет має гарантувати стійкість держави до кібервійни, а саме: захищеність від вірусів, атак, зломів, витоків, закладок, крадіжки даних, спаму, вимикання інфраструктури та програмного забезпечення; стійкість до електронних атак (моніторинг, виявлення, попередження, блокування, контратаки). Водночас у межах забезпечення змістовного напряму інформаційного суверенітету забезпечується стійкість в інформаційній війні, зокрема самостійне управління інформацією (фільтрація, вимикання, розповсюдження) та стійкість до інформаційних атак (виявлення, попередження, блокування, контратака).

У контексті даного підходу виділено такі складові цифрового суверенітету:

– е*лектронний щит*, який передбачає наявність власних або контрольованих апаратної та програмної (інформаційні та телекомунікаційні системи), а також мобільної платформ;

– *інформаційний щит (*власні Інтернет-інфраструктура, медійна структура ЗМІ, телебачення та Інтернету, система й засоби пропаганди та ведення інформаційних війн, розвинена ідеологія, нормативна база, ринок ідеологічних послуг).

Як зазначено, обов'язковим елементом системи електронного суверенітету держави є власна медійна інфраструктура, яка має поєднувати пошукові сервіси, довідкові ресурси; соціальні мережі, месенджери; блоги, форуми, служби розсилки; Інтернет-ЗМІ, традиційні ЗМІ та телебачення; контентні ресурси

(рейтинги / аналітика, історія, наука, інформація за групами інтересів, дозвілля); програми для соціальних мереж і мобільних пристроїв; дитячий Інтернет.

Для забезпечення реального електронного суверенітету держава має володіти широким переліком засобів контролю, зокрема здійснювати моніторинг інформаційного простору, мати законодавство щодо відповідальності за контент різних категорій надавачів інформаційних послуг, в тому числі ЗМІ), фільтрації інформації та публічного правозастосування. Прийнятним розглядається можливість використовувати фільтрування інформації на всіх рівнях (школи, університети, мережі), принаймні у виняткових випадках загрози інформаційній (кібер) безпеці держави.

Поряд із засобами контролю державі необхідно мати потужні засоби впливу. Так, розвиток власного ринку ідеологічних послуг і технологій, формування й підтримання державної (національної) ідеології, функціонування системи впливу і ведення інформаційних війн, в тому числі наявність кваліфікованих кадрів і власних інструментів, інформаційна інфраструктура, що забезпечує поширення контенту, є основою для забезпечення електронногосуверенітету держави.

4.3. Основні завдання щодо забезпечення інформаційного суверенітету України.

Забезпечення інформаційного суверенітету України - сукупність організаційних, нормативно-правових, воєнних та зовнішньополітичних заходів, що спрямовані на забезпечення цілісності національного інформаційного простору, національної інформаційної інфраструктури та технологічної безпеки України, що здійснюється в інтересах забезпечення прав та свобод громадян України, суспільства та держави.

У сучасних умовах завдання щодо забезпечення інформаційного суверенітету держави розділяють на два напрями: технологічний та змістовний.

Завдання із забезпечення інформаційного суверенітету держави за технологічним напрямом включають, зокрема:

– забезпечення реального інноваційного потенціалу країни та її здатності до самостійного творення (від ідеї до реалізації) новітніх технологій;

– створення (або стимулювання) національних ІТ-ТНК;

– збільшення військового кіберпотенціалу держави;

– розвиток власного контенту та технологічної інфраструктури;

– створення кіберозброєнь, проведення інформаційних спеціальних операцій та інформаційних війн;

– запобігання, виявлення і нейтралізація внутрішніх та зовнішніх інформаційних загроз;

– підтримка національного інформаційного продукту, ІТ;

– впровадження цифрового мовлення та супутникового мовлення;

– ефективне використання національних інформаційних ресурсів, розвиток та захист інформаційної інфраструктури;

– протидія комп'ютерній злочинності, комп'ютерному тероризму;

– захист від несанкціонованого проникнення в масиви інформації, що становлять державну та іншу передбачену законом таємницю, інтелектуальну власність соціальних структур, окремих членів суспільства.

Для забезпечення інформаційного суверенітету України за змістовним напрямом основними завданнями є:

– наповнення національного інформаційного простору якісною інформацією, розвиток національного книговидання;

– виготовлення національної теле- та аудіопродукції, в тому числі для дітей та юнацтва;

– наповнення вітчизняного сегмента Інтернету і впорядкування його діяльності;

– достатній рівень інформаційного забезпечення прийняття рішень державними органами, підприємствами і громадянами;

– реалізація конституційних прав і свобод громадян, суспільства і держави на інформацію;

– визначення норм, засад і меж діяльності зарубіжних та міжнародних суб'єктів у національному інформаційному просторі України;

– формування та захист інтересів України у світовому інформаційному просторі й міжнародних інформаційних відносинах;

– участь у заходах, що сприяють сталому розвиткові національного інформаційного простору України та зміцненню її суверенітету;

– створення потужних інформаційних потоків, що підтримуватимуть національну систему символів, установок, переконань та стереотипів, а також забезпечуватимуть їхню експансію у навколишній світ (за принципом «дія-протидія»);

– жорсткий контроль за дотриманням вітчизняними, так і зарубіжними ЗМІ законодавства України і встановлення суворої відповідальності за його порушення;

– розвиток іномовлення.

Питання для самоконтролю

1. Що таке суверенітет?
2. Якими є характеристики інформаційного суверенітету держави?
3. У чому суть дискусії, яка триває навколо трактування змісту інформаційного суверенітету держави у світовій та вітчизняній науковій думці?
4. Що таке електронний суверенітет держави?
5. Які відмінності та взаємозв'язок між інформаційним та електронним суверенітетом держави?
6. Якими є основні завдання щодо забезпечення інформаційного суверенітету України за технологічним та змістовним напрямом?

ТЕМА 5. Система забезпечення інформаційної безпеки України. Державна інформаційна політика та державна політика інформаційної безпеки.

У відповідності до системного підходу виділяють такі складові забезпечення інформаційної безпеки держави:

– нормативно-правова база;

– інституційне забезпечення (структура і завдання органів з інформаційної безпеки);

– державна політика інформаційної безпеки як інструмент забезпечення інформаційної безпеки;

– ресурсне забезпечення (організаційне, інформаційно-аналітичне, програмно-технічне і режимне, фінансове, матеріально-технічне, кадрове тощо).

5.1. Нормативно-правове забезпечення інформаційної безпеки України.

До найвищого рівня нормативно-правового забезпечення у галузі інформаційної безпеки відносяться міжнародні документи, серед яких документи Організації Об'єднаних Націй, її профільних установ, фондів, програм, зокрема, ООН з питань освіти, науки і культури (ЮНЕСКО), Програми розвитку ООН (ПРООН), Міжнародного Союзу Електрозв'язку (МСЕ, International Telecommunication Union, ITU), Всесвітньої організації інтелектуальної власності (ВОІВ) та інших.

Розглядаючи нормативний доробок ООН, насамперед варто згадати такі ключові документи як Декларація прав людини 1948 року, в якій право на вираження своєї думки визнане однією з основних демократичних цінностей, та Міжнародний Пакт про громадянські та політичні права 1966 року. За підсумками діяльності Генеральної Асамблеї ООН прийнято низку резолюцій з питань розвитку інформаційного суспільства та інформаційної безпеки, серед яких «Необхідність встановлення нового, більш справедливого та більш ефективного міжнародного порядку в галузі інформації та зв'язку» (1978 р.), «Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки» (починаючи з 1998 року майже щорічно), «Використання інформаційно-комунікаційних технологій в цілях розвитку» (2002 р.), «Створення глобальної культури кібербезпеки і захист найважливіших інформаційних структур», (2002, 2003, 2009 р.р.), «Боротьба зі злочинним використанням інформаційної технології» (2002 р.) та багато інших.

Окрему увагу варто звернути на підсумкові документи міжнародних форумів, зокрема Окінавську хартію глобального інформаційного суспільства 2000 року, Декларацію принципів «Побудова інформаційного суспільства – глобальне завдання в новому тисячолітті» і План дій, прийнятих на Всесвітньому

саміті з інформаційного суспільства (ВСІС, World Summit on Information Society, WSIS) 2003 року.

У Додатку до Програми для інформаційного суспільства, що була прийнята за результатами другого етапу ВСІС у 2005 році, передбачаються основні напрями використання ІКТ як інструмента інформаційного суспільства, за які відповідають міжнародні організації і програми в системі ООН:

– електронний уряд (ПРООН / МСЕ);

– електронний бізнес (Всесвітня торгівельна організація (ВТО) / Конференція ООН з торгівлі і розвитку (ЮНКТАД) / МСЕ / Всесвітній поштовий союз (ВПС);

– електронне навчання (ЮНЕСКО / МСЕ / ООН з промислового розвитку (ЮНІДО);

– електронна охорона здоров'я (Всесвітня організація охорони здоровя (ВООЗ / МСЕ);

– електронна зайнятість (Міжнародна організація праці (МОП), МСЕ);

– електронна охорона довкілля (ВООЗ / Всесвітня метеорологічна організація (ВМО) / Програма ООН з навколишнього середовища (ЮНЕП) / Програма ООН з населених пунктів (ООН – Габітат) / МСЕ / Міжнародна організація цивільної авіації (ІКАО)

Значну роботу у сфері розвитку інформаційного суспільства та інформаційної безпеки за напрямами своєї діяльності здійснює ЮНЕСКО, яка розробила Декларацію про основні принципи, що стосуються вкладу ЗМІ у зміцнення миру та міжнародного взаєморозуміння, у розвиток прав людини і у боротьбу проти расизму і апартеїду та підбурення до війни (1978 р.), програму «Інформаційне суспільство для всіх» (1996 р.), Загальну декларацію ЮНЕСКО про культурне різноманіття (2001 р.), Рекомендацію про розвиток та використання багатомовності та загальний доступ до кіберпростору (2003 р.), Хартію про збереження цифрового надбання (2003 р.) та інші.

Особливою є роль у міжнародній нормотворчій діяльності Міжнародного союзу електрозв'язку, який бере участь у розробці міжнародних стандартів у сфері ІТ та інформаційної безпеки, формує стратегічні документи з цих питань, зокрема у 2007 році представив Глобальну програму кібербезпеки, яка визначила цілі, принципи і стратегії розробки моделей законодавства в сфері боротьби з комп'ютерною злочинністю, прийняв низку резолюцій, спрямованих на зміцнення довіри та безпеки при використанні інформаційно-комунікаційних технологій і боротьбі із комп'ютерними злочинами.

Активна нормативно-правова діяльність провадиться на європейському рівні, зокрема Рада Європи прийняла Конвенцію про кіберзлочинність (2001р.), яка набула загальносвітового значення і була підписана близько 50 країнами світу, Конвенцію про захист осіб стосовно автоматизованої обробки персональних даних (1981 р.), низку резолюцій та рекомендацій Кабінету міністрів з ключових питань розвитку інформаційного суспільства тощо.

Міжнародні стандарти у сфері інформаційної безпеки представлені багатьма стандартами, серед яких насамперед варто згадати такі: ISO/IEC 27000 - серія міжнародних стандартів, яка містить стандарти з інформаційної безпеки, опубліковані спільно Міжнародною організації зі стандартизації (ISO) і Міжнародною електротехнічною комісією (IEC). Серія включає кращі практики і рекомендації в галузі інформаційної безпеки для створення, розвитку і підтримання системи менеджменту інформаційної безпеки; CoBiT (англ. Control Objectives for Information and Related Technology («Завдання інформаційних і суміжних технологій») - відкритий IT-стандарт, який в свою чергу містить ряд документів зі стандартами щодо оптимізації управління IT: аудитом IT та IT-безпекою.

На думку фахівців, нормативно-правова база інформаційної безпеки має виконувати в першу чергу три основні функції:

– регулювати взаємовідносини між суб'єктами інформаційної безпеки, визначати їх права, обов'язки та відповідальність;

– нормативно забезпечувати дії суб'єктів інформаційної безпеки на всіх рівнях, а саме - людини, суспільства, держави;

– встановлювати порядок застосування різних сил і засобів забезпечення інформаційної безпеки.

За роки незалежності в Україні закладено законодавчі основи системи забезпечення інформаційної безпеки, зокрема було напрацьовано великий масив нормативно-правових актів.

Розглянемо структуру вітчизняного законодавства у сфері інформаційної безпеки. На вершині «піраміди» знаходиться основний закон - Конституція України, прийнята 28 червня 1996 року, яка закладає основи системи забезпечення інформаційної безпеки. Конституція встановлює, що забезпечення інформаційної безпеки України є однією з найважливіших функцій держави, гарантує кожному громадянину права в інформаційній сфері: свободу думки й слова, свободу вираження поглядів і переконань, право вільно збирати, зберігати, використовувати й поширювати інформацію, захист інтелектуальної власності, їхніх авторських прав тощо.

Законодавчі акти Верховної Ради України, розпорядчі документи Президента та Кабінету Міністрів України з питань інформаційної безпеки України, які становлять каркас нормативно-правової бази, за сферою регулювання можна поділити на такі тематичні групи:

1) концептуальні засади інформаційної безпеки як складової національної безпеки

– Закон України «Про національну безпеку України» (2018)

– Указ Президента «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» (2017)

– Указ Президента України «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» (2015)

– Указ Президента України від 15 березня 2016 року №96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» (2016).

2) використання, розповсюдження інформації

– Закон України «Про інформацію» (1992);

– Закон України «Про друковані засоби масової інформації (пресу) в Україні» (1992);

– Закон України «Про телебачення і радіомовлення» (1993);

– Закон України «Про доступ до публічної інформації» (2011);

– Закон України «Про Суспільне телебачення і радіомовлення України» (2014).

3) використання інформації з обмеженим доступом

– Закон України «Про державну таємницю» (1994);

– Постанова КМУ від 19 жовтня 2016 р. № 736 «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію» (2016);

– Закон України «Про Національну систему конфіденційного зв'язку» (2002);

– Закон України «Про захист персональних даних» (2010).

4) розвиток інформаційного суспільства, інформатизація

– Закон України «Про Національну програму інформатизації» (1998);

– Закон України «Про Концепцію Національної програми інформатизації» (1998);

– Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» (2007)

– Розпорядження Кабінету Міністрів України «Про схвалення Стратегії розвитку інформаційного суспільства в Україні» (2013).

5) зв'язок, ІКС, технічний захист інформації

– Закон України «Про зв'язок» (1995);

– Закон України «Про радіочастотний ресурс» (2000);

– Закон України «Про телекомунікації» (2005);

– Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» (2005);

– Закон України «Про державну підтримку розвитку індустрії програмної продукції» (2012);

– Постанова Кабінету Міністрів України «Про затвердження Концепції технічного захисту інформації в Україні» (1997)

6) електронні системи інформації

– Закон України «Про електронні документи та електронний документообіг» (2003);

– Закон України «Про електронний цифровий підпис» (2003);

– Постанова Кабінету Міністрів України «Про заходи щодо створення електронної інформаційної системи «Електронний Уряд» (2003).

– Розпорядження КМУ від 20.09.2017 № 649 «Про схвалення Концепції розвитку електронного урядування в Україні»

Нормативні акти міністерств, відомств, Національного банку України, інших органів влади, органів місцевого самоврядування регулюють питання інформаційної безпеки у межах своєї компетенції.

Загальна схема нормативно-правового забезпечення інформаційної безпеки в Україні представлена на рис. 4.

Рис. 4. Нормативно-правове забезпечення інформаційної безпеки в Україні.

5.2. Інституційне забезпечення інформаційної безпеки України.

На сьогодні в Україні діє достатньо розгалужена система органів державної влади, які виконують функції із забезпечення інформаційної безпеки у різних аспектах.

Систему суб'єктів забезпечення інформаційної безпеки можна визначити як організовану державою сукупність суб'єктів – органів законодавчої, виконавчої, судової влади, громадських організацій, посадових осіб та окремих громадян, об'єднаних цілями та завданнями щодо захисту національних інтересів в інформаційній сфері, що здійснюють узгоджену діяльність у межах законодавства України.

Характеризуючи систему інституційного забезпечення інформаційної безпеки України, слід відзначити, що до її складу входять:

– законодавчий орган – Верховна Рада України, в якій питаннями інформаційної безпеки займаються два комітети: Комітет з питань свободи слова та інформаційної політики та Комітет з питань інформатизації та зв'язку. На Уповноваженого Верховної Ради України з прав людини покладено обов'язки щодо захисту персональних даних;

– Президент України як глава держави і Верховний головнокомандувач, координуючу функцію у сфері інформаційної безпеки виконує Рада національної безпеки та оборони (РНБО) України;

– Кабінет Міністрів України як вищий орган у системі органів виконавчої влади;

– 2 регуляторних органи виконавчої влади - Національна рада України з питань телебачення і радіомовлення та Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації;

– органи виконавчої влади - Державний комітет телебачення та радіомовлення України, Міністерство інформаційної політики України, Державне агентство з питань е-урядування України, Державна служба спеціального зв'язку та захисту інформації України, а також міністерства та відомства т.зв. «силового» напряму (Служба безпеки України, Міністерство внутрішніх справ України, Міністерство оборони України та Служба зовнішньої розвідки України). Окрім того, виконання тих чи інших завдань та програм в інформаційній сфері здійснюють понад 20 інших органів державної влади України: Міністерство юстиції України, Міністерство закордонних справ України, Міністерство освіти і науки України, Міністерство інфраструктури України, Державна архівна служба України, інші;

– місцеві органи виконавчої влади, органи місцевого самоврядування;

– органи судочинства (місцеві, апеляційні, спеціалізовані суди, Верховний Суд України).

– організації громадянського суспільства, громадяни.

Основні суб'єкти забезпечення інформаційної безпеки показані на рис. 5.

Рис. 5. Інституційне забезпечення інформаційної безпеки України.

Єдиним органом законодавчої влади в Україні є парламент - Верховна Рада України. До повноважень ВР України належать, зокрема: прийняття законів, визначення засад внутрішньої і зовнішньої політики держави, затвердження загальнодержавних програм, надання законом згоди на обов'язковість міжнародних договорів України та денонсація міжнародних договорів України, здійснення парламентського контролю тощо.

Верховна Рада України для здійснення законопроектної роботи, підготовки і попереднього розгляду питань у межах її повноважень, виконання контрольних функцій створює з числа народних депутатів України комітети Верховної Ради України.

Законодавчою діяльністю з питань інформаційної безпеки опікується два комітети Верховної Ради України:

Комітет ВР України з питань свободи слова та інформаційної політики;

Комітет ВР України з питань інформатизації та зв'язку.

Основна сфера діяльності Комітету ВР України з питань свободи слова та інформаційної політики - розроблення й удосконалення законодавчої бази держави, що регулює відносини в інформаційній сфері. Напрямами діяльності Комітету є:

- державна політика у сфері інформації та інформаційної безпеки;
- забезпечення свободи слова;
- права громадян на інформацію;
- друковані, електронні засоби масової інформації та Інтернет;
- висвітлення діяльності Верховної Ради України;
- засади здійснення рекламної діяльності.

У своїй діяльності Комітет співпрацює з Державним комітетом України з телебачення і радіомовлення, Національною радою України з питань телебачення і радіомовлення, Міністерством інформаційної політики та іншими органами державної влади.

Для підготовки законопроектів Комітет залучає провідних вітчизняних фахівців у сфері інформаційного законодавства, співпрацює з Громадською радою з питань свободи слова та інформації**.** Комітет регулярно ініціює та організовує парламентські слухання, присвячені проблемам інформаційних відносин та свободи слова в Україні, реагує на звернення громадян щодо порушення їх права на інформацію і свободу слова.

Сфера повноважень Комітету з питань інформатизації та зв'язку ВР України включає нормотворчу діяльність за такими напрямами:

- розвиток інформаційного суспільства та інформатизація;
- електронне урядування;
- електронний документообіг, електронний цифровий підпис;
- національна система електронних інформаційних ресурсів;
- телекомунікації, використання радіочастотного ресурсу, поштовий зв'язок;

– індустрія програмування;

– кібербезпека, технічний та криптографічний захист інформації;

Повноваження щодо контролю за додержанням законодавства про захист персональних даних покладено на *Уповноваженого Верховної Ради України з прав людини*.

Згідно із Законом України «Про захист персональних даних» у сфері захисту персональних даних Уповноважений має такі повноваження:

– отримувати пропозиції, скарги та інші звернення фізичних і юридичних осіб з питань захисту персональних даних та приймати рішення за результатами їх розгляду;

– проводити на підставі звернень або за власною ініціативою виїзні та безвиїзні, планові, позапланові перевірки володільців або розпорядників персональних даних;

– отримувати на свою вимогу та мати доступ до будь-якої інформації (документів) володільців або розпорядників персональних даних, які необхідні для здійснення контролю за забезпеченням захисту персональних даних;

– затверджувати нормативно-правові акти у сфері захисту персональних даних у випадках, передбачених закоодавством;

– за підсумками перевірки, розгляду звернення видавати обов'язкові для виконання вимоги (приписи) про запобігання або усунення порушень законодавства про захист персональних даних;

– надавати рекомендації щодо практичного застосування законодавства про захист персональних даних, роз'яснювати права і обов'язки відповідних осіб за зверненням суб'єктів персональних даних, володільців або розпорядників персональних даних, структурних підрозділів або відповідальних осіб з організації роботи із захисту персональних даних, інших осіб;

– взаємодіяти із структурними підрозділами або відповідальними особами, які організовують роботу, пов'язану із захистом персональних даних при їх обробці;

– складати протоколи про притягнення до адміністративної відповідальності та направляти їх до суду у випадках, передбачених законом;

– інформувати про законодавство з питань захисту персональних даних, проблеми його практичного застосування, права і обов'язки суб'єктів відносин, пов'язаних із персональними даними;

– здійснювати моніторинг нових практик, тенденцій та технологій захисту персональних даних;

– організовувати та забезпечувати взаємодію з іноземними суб'єктами відносин, брати участь у роботі міжнародних організацій з питань захисту персональних даних.

З метою забезпечення виконання Уповноваженим функцій контролю за виконанням законодавства в сфері захисту персональних даних в Секретаріаті

Уповноваженого Верхової Ради України з прав людини створено Департамент з питань захисту персональних даних.

Президент України є главою держави, гарантом державного суверенітету, територіальної цілісності України, додержання Конституції України, прав і свобод людини і громадянина.

Президент спільно з Верховною Радою визначає державну інформаційну політику, а також політику у галузі захисту інформації, державну політику на телебаченні та радіомовленні, законодавчі основи її реалізації, гарантування соціальної та правового захисту співробітників інформаційної сфери.

Крім того, Президент України:

– керує в межах своїх конституційних повноважень органами і силами з забезпечення інформаційної безпеки;

– санкціонує заходи, щодо забезпечення інформаційної безпеки;

– формує, реорганізує та ліквідує органи і сили з забезпечення інформаційної безпеки.

Координуючу функцію у сфері інформаційної безпеки виконує *Рада національної безпеки та оборони (РНБО) України*. Президент України у своїй діяльності спирається на апарат Ради національної безпеки та оборони.

Рада національної безпеки і оборони України подає пропозиції Президентові України щодо:

– визначення стратегічних національних інтересів України, концептуальних підходів та напрямів забезпечення інформаційної безпеки, заходів політичного, економічного, соціального, воєнного, науково-технологічного, екологічного, інформаційного та іншого характеру відповідно до масштабу потенційних та реальних загроз національним інтересам України;

– забезпечення і контролю надходження та опрацювання необхідної інформації, її збереження, конфіденційності та використання в інтересах національної безпеки України, аналізу на її основі стану і тенденції розвитку подій, що відбуваються в Україні і в світі,

– визначення потенційних та реальних загроз національним інтересам України.

Рада національної безпеки і оборони України проводить роботу, щодо виявлення і оцінки загроз інформаційній безпеці та готує проекти рішень Президента України щодо запобігання цим загрозам, розробляє пропозиції у галузі забезпечення інформаційної безпеки.

Рада національної безпеки і оборони України здійснює поточний контроль за діяльністю органів виконавчої влади у сфері інформаційної безпеки, подає Президентові України відповідні висновки та пропозиції.

Указом Президента України у 2002 р. при РНБО було створено Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки, яка є консультативно-дорадчим органом із зазначених питань.

У складі Адміністрації Президента України діє *Головний департамент інформаційної політики*.

Кабінет Міністрів України як вищий орган у системі органів виконавчої влади, відповідальний перед Президентом України та підконтрольний і підзвітний Верховній Раді України у межах, передбачених Конституцією України, відповідно до ст. 116 Конституції України:

– забезпечує інформаційний суверенітет України, здійснення внутрішньої і зовнішньої інформаційної політики держави, виконання Конституції і законів України, актів Президента України, що стосуються інформаційної безпеки;

– вживає заходів щодо забезпечення прав і свобод людини і громадянина в інформаційній сфері;

– забезпечує проведення державної політики інформаційної безпеки;

– спрямовує і координує роботу усієї системи органів державного управління з питань, що стосуються інформаційної безпеки.

Окрім цього Кабінет Міністрів України:

– визначає потреби в витратах на забезпечення інформаційної безпеки, забезпечує виконання затвердженого Верховною Радою України Державного бюджету України щодо фінансування заходів у сфері інформаційної безпеки у визначених обсягах;

– організовує розроблення і виконання державних програм з розвитку інформаційної інфраструктури органів державного управління;

– здійснює передбачені законодавством заходи щодо формування, розміщення, фінансування та виконання державного оборонного замовлення на поставку (закупівлю) продукції, виконання робіт, надання послуг для потреб органів, що забезпечують інформаційну безпеку;

– встановлює порядок надання суб'єктам забезпечення інформаційної безпеки у користування державного майна, засобів зв'язку і радіочастотного ресурсу, комунікацій, інших об'єктів інфраструктури держави, навігаційної, топогеодезичної, метеорологічної, гідрографічної та іншої інформації;

– здійснює загальнодержавні заходи щодо забезпечення живучості об'єктів інформаційної інфраструктури;

– забезпечує комплектування особовим складом сили забезпечення інформаційної безпеки;

– утворює, реорганізовує, ліквідовує науково-дослідні установи, навчальні заклади та окремі кафедри (відділення, факультети) суб'єктів забезпечення інформаційної безпеки;

– забезпечує реалізацію права на соціально-економічний захист відповідно до законодавства України, що регламентує діяльність окремих суб'єктів забезпечення інформаційної безпеки;

– здійснює у визначених законом випадках регулювання господарської діяльності у суб'єктах забезпечення інформаційної безпеки;

– встановлює відповідно до закону порядок реалізації та утилізації об'єктів інформаційної інфраструктури, інформаційних ресурсів тощо.

Національна рада України з питань телебачення і радіомовлення є постійно діючим колегіальним органом, метою діяльності якого є нагляд за

дотриманням законів України у сфері телерадіомовлення, а також здійснення регуляторних повноважень.

Національна рада складається з восьми осіб. З них чотири члени Національної ради призначаються Верховною Радою України і чотири - Президентом України. Голова Національної ради обирається Національною радою з числа членів Національної ради таємним голосуванням.

Національна рада здійснює:

– нагляд за дотриманням телерадіоорганізаціями та провайдерами програмної послуги вимог законодавства у галузі телерадіомовлення, в том числі реклами та спонсорства;

– нагляд за дотриманням ліцензіатами ліцензійних умов та умов ліцензій, стандартів та норм технічної якості телерадіопрограм, визначеного законодавством порядку мовлення під час проведення виборчих кампаній та референдумів;

– нагляд за дотриманням телерадіоорганізаціями законодавства України у сфері кінематографії, вимог щодо частки вітчизняного продукту у їх програмах (передачах) та вживання мов при здійсненні телерадіомовлення;

– нагляд за дотриманням телерадіоорганізаціями законодавства у сфері захисту суспільної моралі;

– нагляд за дотриманням телерадіоорганізаціями вимог законодавства щодо складу їх засновників (власників), а також частки іноземних інвестицій у їх статутному капіталі;

– застосування в межах своїх повноважень санкцій відповідно до закону (оголошення попередження, штраф, звернення до суду із заявою про анулювання ліцензії);

– офіційний моніторинг телерадіопрограм тощо.

Національна рада виконує такі регуляторні функції, передбачені законодавством України у сфері телерадіомовлення:

– ліцензування телерадіомовлення та провайдерів програмної послуги;

– участь у розробленні та погодження проекту Національної таблиці розподілу смуг радіочастот України і Плану використання радіочастотного ресурсу України у частині смуг радіочастот, виділених для потреб телерадіомовлення;

– розроблення умов використання та визначення користувачів радіочастотного ресурсу, виділеного для потреб телерадіомовлення;

– забезпечення і сприяння конкуренції у діяльності телерадіо-організацій усіх форм власності відповідно до вимог законодавства, створення умов щодо недопущення усунення, обмеження чи спотворення конкуренції в телерадіоінформаційному просторі;

– ведення Державного реєстру телерадіоорганізацій України.

Повноваженнями Національної ради щодо організації та перспектив розвитку телерадіомовлення є: участь у розробці і реалізації державної

політики у сфері телерадіомовлення; розробка і затвердження Плану розвитку національного телерадіоінформаційного простору та інші.

Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації (НКРЗІ), є державним колегіальним органом, підпорядкованим Президенту України, підзвітним Верховній Раді України.

НКРЗІ є органом державного регулювання у сфері телекомунікацій, інформатизації, користування радіочастотним ресурсом та надання послуг поштового зв'язку. У визначеній сфері НКРЗІ здійснює повноваження органу ліцензування, дозвільного органу, регуляторного органу та органу державного нагляду (контролю).

Основними завданнями НКРЗІ є:

– забезпечення проведення єдиної державної політики з питань державного регулювання у сфері телекомунікацій, інформатизації та розвитку інформаційного суспільства, користування радіочастотним ресурсом, надання послуг поштового зв'язку;

– здійснення державного регулювання (в т.ч. ліцензування та реєстрація) та нагляду у сфері телекомунікацій, інформатизації, користування радіочастотним ресурсом, надання послуг поштового зв'язку, використання інфраструктури з метою максимального задоволення попиту споживачів на послуги зв'язку та інформаційні послуги, створення сприятливих умов для залучення інвестицій, збільшення обсягів послуг та підвищення їх якості, розвитку та модернізації телекомунікаційних та інформаційно-телекомунікаційних мереж з урахуванням інтересів національної безпеки;

– забезпечення ефективного користування радіочастотним ресурсом і функціонування ринку телекомунікаційних, інформаційно-телекомунікаційних, інформаційних послуг та послуг поштового зв'язку на основі збалансування інтересів суспільства, суб'єктів господарювання та споживачів цих послуг;

– сприяння розвитку конкуренції та підприємництва, забезпечення рівних умов діяльності суб'єктів господарювання всіх форм власності, вдосконалення механізму регулювання ринкових відносин у сфері телекомунікацій, інформатизації, користування радіочастотним ресурсом та надання послуг поштового зв'язку;

– забезпечення системності, комплексності і узгодженості розвитку інформатизації та інформаційного суспільства в державі.

Рішення НКРЗІ приймаються на засіданнях, які проводяться у формі відкритих або закритих слухань. У разі розгляду питань, що мають важливе суспільне значення, засідання проводяться у формі відкритих слухань, у яких мають право брати участь суб'єкти ринку телекомунікацій, нформатизації, користування радіочастотним ресурсом та надання послуг поштового зв'язку і громадські організації.

Рішення НКРЗІ, прийняті в межах її повноважень, обов'язкові для виконання центральними та місцевими органами виконавчої влади, органами

місцевого самоврядування, учасниками ринку телекомунікаційних послуг, їх об'єднаннями.

Державний комітет телебачення і радіомовлення України (Держкомтелерадіо) є центральним органом виконавчої влади із спеціальним статусом, діяльність якого спрямовується і координується Кабінетом Міністрів України.

Держкомтелерадіо є головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сфері телебачення і радіомовлення, інформаційній та видавничій сфері.

Держкомтелерадіо відповідно до покладених на нього завдань:

– бере участь у законотворчій діяльності з питань, що належать до його компетенції;

– виконує разом з іншими державними органами завдання щодо забезпечення інформаційної безпеки, розробляє заходи щодо запобігання внутрішньому і зовнішньому інформаційному впливу, який загрожує інформаційній безпеці держави, суспільства, особи;

– визначає порядок функціонування та проводить моніторинг інформаційного наповнення веб-сайтів та стан роз'яснювальної роботи органів виконавчої влади з пріоритетних питань державної політики та надає пропозиції зазначеним органам;

– аналізує та прогнозує розвиток ринку у сфері телебачення і радіомовлення, інформаційній та видавничій сфері, поліграфії;

– сприяє розвитку вітчизняних засобів масової інформації, книговидавничої справи та книгорозповсюдження, підвищенню художньої якості вітчизняних телерадіопрограм, захисту суспільства від негативного впливу аудіо- і відеопродукції, яка становить загрозу суспільній моралі;

– забезпечує дотримання державної мовної політики у сфері телебачення і радіомовлення, інформаційній та видавничій сфері;

– сприяє створенню та діяльності Суспільного телебачення і радіомовлення, впровадженню ефірного наземного цифрового телерадіомовлення;

– здійснює методологічне забезпечення та координує діяльність державних телерадіоорганізацій, інформаційних агентств, видавництв, поліграфічних підприємств і підприємств книгорозповсюдження, установ та організацій;

– є замовником на виробництво і розповсюдження теле- та радіопрограм, випуск видавничої продукції, проведення наукових досліджень у сфері засобів масової інформації, книговидавничої справи та інформаційно-бібліографічної діяльності;

– забезпечує в межах повноважень міжнародне співробітництво, бере участь у розробленні проектів та укладенні міжнародних договорів України, забезпечує їх виконання.

Міністерство інформаційної політики України створене у 2014 році з метою забезпечення інформаційного суверенітету України, зокрема з питань поширення суспільно важливої інформації в Україні та за її межами, а також забезпечення функціонування державних інформаційних ресурсів; забезпечення здійснення реформ засобів масової інформації щодо поширення суспільно важливої інформації.

Міністерство інформаційної політики України відповідно до покладених на нього завдань:

– бере участь у законотворчій діяльності з питань, що належать до його компетенції, і формуванні державної інформаційної політики;

– здійснює нормативно-правове регулювання у сфері забезпечення інформаційного суверенітету України, зокрема з питань поширення суспільно важливої інформації в Україні та за її межами, а також забезпечення функціонування державних інформаційних ресурсів;

– здійснює в межах повноважень, передбачених законом, координацію діяльності ОВВ та взаємодію з органами місцевого самоврядування з питань, віднесених до його компетенції;

– надає методичну та практичну допомогу прес-службам органів виконавчої влади, державним та комунальним ЗМІ в процесі їх реформування;

– розробляє плани заходів щодо сприяння незалежності ЗМІ, захисту прав журналістів та споживачів інформаційної продукції;

– організовує проведення досліджень впливу результатів діяльності ЗМІ на суспільну свідомість;

– організовує розроблення та впровадження навчальних курсів з інформаційної політики і розробляє навчально-методичне забезпечення для навчальних закладів усіх рівнів акредитації;

– бере участь у підготовці ЦОВВ планів і програм навчання фахівців у сфері інформаційної політики, їх професійній підготовці, перепідготовці та підвищенні кваліфікації;

– розробляє разом з МЗС, Мінкультури та МОН плани заходів та програмні документи щодо позиціонування України в світі;

– розробляє та вносить на розгляд Кабінету Міністрів України програмні документи у сфері захисту інформаційного простору України від зовнішнього інформаційного впливу;

– сприяє дотриманню в Україні свободи слова;

– вживає разом з іншими ЦОВВ заходів до популяризації вітчизняної телепродукції за кордоном;

– вносить на розгляд КМУ пропозиції щодо визначення механізму державної підтримки діяльності з виготовлення та популяризації вітчизняної аудіовізуальної продукції;

– забезпечує проведення фестивалів, виставок тощо;

– проводить моніторинг інформації у вітчизняних та іноземних ЗМІ та інформує КМУ;

– організовує та забезпечує діяльність державних телерадіоорганізацій в частині закордонного мовлення з метою поширення інформації про Україну у світі;

– здійснює міжнародне співробітництво, забезпечує виконання зобов'язань, узятих за міжнародними договорами України, з питань, що належать до його компетенції.

Міністерство цифрової трансформації України (з 2014 року до вересня 2019 року - Державне агентство з питань електронного урядування України) є центральним органом виконавчої влади, діяльність якого спрямовується і координується Кабінетом Міністрів України.

Міністерство є головним органом у системі центральних органів виконавчої влади, що забезпечує:

– формування та реалізацію державної політики у сфері цифровізації, цифрової економіки, цифрових інновацій, електронного урядування та електронної демократії, розвитку інформаційного суспільства;

– формування та реалізацію державної політики у сфері розвитку цифрових навичок та цифрових прав громадян;

– формування та реалізацію державної політики у сфері відкритих даних, розвитку національних електронних інформаційних ресурсів та інтероперабельності, розвитку інфраструктури широкосмугового доступу до Інтернету та телекомунікацій, електронної комерції та бізнесу;

– формування та реалізацію державної політики у сфері надання електронних та адміністративних послуг;

– формування та реалізацію державної політики у сфері електронних довірчих послуг;

– формування та реалізацію державної політики у сфері розвитку IT-індустрії;

– виконання функцій центрального засвідчувального органу шляхом забезпечення створення умов для функціонування суб'єктів правових відносин у сфері електронних довірчих послуг.

Державна служба спеціального зв'язку та захисту інформації України створена на виконання прийнятого 23 лютого 2006 року Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» на базі ліквідованого Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України.

Державна служба спеціального зв'язку та захисту інформації України є державним органом, який призначений для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, захисту державних інформаційних ресурсів в

інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації.

Основними завданнями Державної служби спеціального зв'язку та захисту інформації України є:

– участь у формуванні та реалізація державної політики у сфері захисту державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації;

– забезпечення в установленому порядку урядовим зв'язком Президента України, Голови Верховної Ради України, Прем'єр-міністра України, інших посадових осіб органів державної влади, органів місцевого самоврядування, органів військового управління, керівників підприємств, установ і організацій у мирний час, в умовах надзвичайного та воєнного стану, а також у разі виникнення надзвичайної ситуації;

– забезпечення функціонування, безпеки та розвитку державної системи урядового зв'язку і Національної системи конфіденційного зв'язку;

– визначення вимог і порядку створення та розвитку систем технічного та криптографічного захисту інформації,яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

– здійснення державного контролю за станом криптографічного та технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, а також за додержанням вимог законодавства у сфері надання послуг електронного цифрового підпису;

– охорона об'єктів, приміщень, систем, мереж, комплексів, засобів урядового і спеціального зв'язку, ключових документів до засобів криптографічного захисту інформації Державної служби спеціального зв'язку та захисту інформації України.

Служба безпеки України є державним правоохоронним органом спеціального призначення, який забезпечує державну безпеку України.

Вона також є спеціально уповноваженим органом державної влади у сфері контррозвідувальної діяльності, охорони державної таємниці та головним органом у сфері боротьби з тероризмом.

Служба безпеки України підпорядкована Президентові України.

На Службу безпеки України покладається у межах визначеної законодавством компетенції захист державного суверенітету, конституційного ладу, територіальної цілісності, економічного, науково-технічного і оборонного потенціалу України, законних інтересів держави та прав громадян від розвідувально-підривної діяльності іноземних спеціальних служб, посягань з боку окремих організацій, груп та осіб, а також забезпечення охорони державної таємниці.

До завдань Служби безпеки України також входить попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, тероризму, корупції та організованої злочинної діяльності у сфері управління і економіки та інших протиправних дій, які безпосередньо створюють загрозу життєво важливим інтересам України.

У межах своєї компетенції Служба безпеки України:

– вносить Президенту України пропозиції про видання актів з питань збереження державної таємниці, обов'язкових для виконання органами державного управління, підприємствами, установами, організаціями і громадянами;

– здійснює інформаційно-аналітичну роботу в інтересах ефективного проведення органами державної влади та управління України внутрішньої і зовнішньої діяльності, вирішення проблем оборони, соціально-економічного будівництва, науково-технічного прогресу, екології та інших питань, пов'язаних з національною безпекою України;

– забезпечує захист державного суверенітету, конституційного ладу і територіальної цілісності України від протиправних посягань з боку окремих осіб та їх об'єднань;

– здійснює контррозвідувальне забезпечення оборонного комплексу, Збройних Сил України, інших військових формувань, дислокованих на території України, енергетики, транспорту, зв'язку, а також важливих об'єктів інших галузей господарства;

– бере участь у розробці і здійсненні відповідно до Закону України «Про державну таємницю» та інших актів законодавства заходів щодо забезпечення охорони державної таємниці та конфіденційної інформації, що є власністю держави, сприяти у порядку, передбаченому законодавством, підприємствам, установам, організаціям та підприємцям у збереженні комерційної таємниці, розголошення якої може завдати шкоди життєво важливим інтересам України;

– подає органам державної влади, органам місцевого самоврядування, підприємствам, установам, організаціям усіх форм власності обов'язкові для розгляду пропозиції з питань національної безпеки, у тому числі із забезпечення охорони державної таємниці.

У складі Центрального управління Служби безпеки України діють, зокрема, такі підрозділи, які виконують завдання у сфері інформаційної безпеки держави: *Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки* і *Департамент охорони державної таємниці та ліцензування.*

Міністерство внутрішніх справ України – центральний орган виконавчої влади України, діяльність якого спрямовується і координується Кабінетом Міністрів України.

МВС України є головним (провідним) органом у системі центральних органів виконавчої влади з питань формування і реалізації державної політики у сфері забезпечення охорони прав і свобод людини, інтересів суспільства і

держави, протидії злочинності, підтримання публічної безпеки і порядку, а також надання поліцейських послуг; захисту державного кордону, цивільного захисту, захисту населення і територій від надзвичайних ситуацій та запобігання їх виникненню; міграції та протидії нелегальній міграції, громадянства тощо.

У 2015 році у складі Національної поліції, діяльність якої спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ , створено *Департамент кіберполіції*. Кіберполіція є міжрегіональним територіальним органом Національної поліції України, входить до структури кримінальної поліції Національної поліції та відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність.

Основні завдання Департаменту кіберполіції Національної поліції України:

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

– сприяння у порядку, передбаченому чинним законодавством, іншим підрозділам Національної поліції у попередженні, виявленні та припиненні кримінальних правопорушень.

Міністерство оборони України забезпечує виконання вимог законодавства України, здійснює реалізацію концепцій, програм у сфері інформаційної безпеки.

Департамент охорони державної таємниці – структурний підрозділ Міністерства оборони, який забезпечує та здійснює контроль за дотримання вимог щодо охорони державної таємниці у структурі Міністерства оборони та підпорядкованих йому організацій.

Головне управління розвідки Міністерства оборони України згідно із Законом України «Про розвідувальні органи України» здійснює розвідувальну діяльність у воєнній, воєнно-політичній, воєнно-технічній, воєнно-економічній, інформаційній, екологічній сферах.

На розвідувальний орган Міністерства оборони України покладаються такі завдання:

– добування, аналітична обробка та надання органам державної влади розвідувальної інформації;

– здійснення спеціальних заходів, спрямованих на підтримку національних інтересів і державної політики України в економічній, політичній, воєнній, військово-технічній, екологічній та інформаційній сферах, зміцнення обороноздатності, економічного і науково-технічного розвитку, захисту та охорони державного кордону;

– участь у боротьбі з тероризмом, міжнародною організованою злочинністю, незаконним обігом наркотичних засобів, незаконною торгівлею зброєю і технологією її виготовлення, незаконною міграцією у порядку, визначеному законом;

– вжиття заходів протидії зовнішнім загрозам національній безпеці України, життю, здоров'ю її громадян та об'єктам державної власності за межами України.

Генеральний штаб Збройних Сил України - головний військовий орган з планування оборони держави, управління застосуванням Збройних сил України, координації та контролю за виконанням завдань у сфері оборони іншими утвореними відповідно до законів України військовими формуваннями, органами виконавчої влади, органами місцевого самоврядування, правоохоронними органами, Державною спеціальною службою транспорту і Державною службою спеціального зв'язку та захисту інформації України.

Головне управління зв'язку та інформаційних систем Генерального штабу Збройних Сил України є структурним підрозділом Генерального штабу Збройних Сил України і призначене для проведення єдиної державної технічної політики в сфері зв'язку та інформатизації, захисту інформаційних ресурсів в інформаційно-телекомунікаційних системах Збройних Сил України та організації зв'язку.

Служба зовнішньої розвідки (СЗР) України є державним органом, який здійснює розвідувальну діяльність у політичній, економічній, військово-технічній, науково-технічній, інформаційній та екологічній сферах.

На Службу зовнішньої розвідки України покладаються такі основні завдання:

– добування, аналітичне опрацювання та надання визначеним законодавством України керівникам вищих органів державної влади розвідувальної інформації;

– сприяння спеціальними заходами здійсненню державної політики України в економічній, політичній, військово-технічній, екологічній та інформаційній сферах, зміцненню обороноздатності, економічного і науково-технічного розвитку країни;

– участь у забезпеченні безпечного функціонування установ України за кордоном, безпеки співробітників цих установ та членів їхніх сімей у країні перебування, а також відряджених за кордон громадян України, які обізнані з відомостями, що становлять державну таємницю;

– участь у боротьбі з міжнародною організованою злочинністю, тероризмом, незаконним обігом наркотичних засобів, незаконною торгівлею зброєю і технологією її виготовлення, незаконною міграцією;

– вжиття заходів протидії зовнішнім загрозам національній безпеці України, життю, здоров'ю її громадян та об'єктам державної власності за межами України.

За усталеною світовою практикою функціональна структура розвідки охоплює процеси добування шляхом проведення агентурної та технічної розвідки актуальної інформації, її аналізу та підготовки аналітичних матеріалів, прогнозів і сценаріїв розвитку ситуації у сфері національної та міжнародної безпеки.

Окрім того, виконання завдань та програм в інформаційній сфері здійснюють понад 20 інших *центральних органів виконавчої влади*: Міністерство юстиції України, Міністерство закордонних справ України, Міністерство освіти і науки України, Міністерство інфраструктури України, Державна архівна служба України тощо.

На рівні адміністративно-територіальних одиниць України повноваження з питань інформаційної політики та забезпечення інформаційної безпеки виконують *місцеві органи виконавчої влади та органи місцевого самоврядування*.

Органи судочинства. Судочинство в Україні здійснюється виключно судами на засадах верховенства права, забезпечення кожному права на справедливий суд та повагу до інших прав і свобод, які гарантують Конституція та закони України, а також міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.

Суди відповідно до ст. 6 Конституції є самостійною гілкою влади і діють незалежно від законодавчої і виконавчої влади. Юрисдикція судів поширюється на всі правовідносини, що виникають у державі.

Система правосуддя має на меті постійно і надійно захищати громадян, підприємства, організації від протиправних посягань, зловживань влади, гарантувати їм дієве поновлення порушених законних прав і свобод.

Відповідно до закону діють апеляційні та місцеві суди. Вищими судовими органами спеціалізованих судів є відповідні вищі суди. Найвищим судовим органом у системі судів загальної юрисдикції є Верховний Суд України.

Судова влада виступає в ролі арбітра, що вирішує спори: між громадянами, громадянами і підприємствами, громадянами і державними чи громадськими організаціями, між громадянами і державою в цілому тощо.

Суди зобов'язані своєчасно й дієво захищати права та свободи громадян, підприємств, організацій шляхом розгляду цивільних, господарських, адміністративних, кримінальних справ і справ про адміністративні правопорушення. Суд не може відмовити у правосудді, якщо суб’єкт вважає, що його права і свободи порушені або створюються перешкоди для їх реалізації чи мають місце інші порушення прав і свобод.

Конституція України встановлює, що носієм суверенітету і єдиним джерелом влади в Україні є народ, а громадяни мають право брати участь в управлінні державними справами.

Громадяни та організації громадянського суспільства можуть залучатися до процесу державного управління через такі механізми громадської участі як інформування (висвітлення діяльності органів влади на сайтах, у друкованих та

Інтернет-виданнях тощо), консультації (інтерактивні методи обговорення на всіх етепах прийняття управлінських рішень, вивчення громадської думки) та механізми прийняття рішень (облік та використання пропозицій громадськості при прийнятті управлінських рішень).

Одним з найбільш поширених та дієвих механізмів активної участі громадськості в державному управлінні є діяльність *громадських рад* при органах державної влади, органах місцевого самоврядування, які представляють та захищають інтереси громадян у процесі підготовки, обговорення та прийняття державно-управлінських рішень з найважливіших питань життя суспільства і держави, а також є суб'єктами здійснення громадського контролю за діяльністю органів виконавчої влади, органів місцевого самоврядування.

Громадська рада відповідно до покладених на неї завдань:

– готує та подає органу влади пропозиції щодо орієнтовного плану проведення консультацій з громадськістю, організації консультацій та питань, які обговорюватимуться;

– проводить відповідно до законодавства громадську експертизу діяльності органу та громадську антикорупційну експертизу нормативно-правових актів та проектів нормативно-правових актів, які розробляє орган;

– здійснює громадський контроль за врахуванням органом пропозицій та зауважень громадськості, забезпечення ним прозорості та відкритості своєї діяльності, доступу до публічної інформації, яка знаходиться у його володінні, а також дотриманням ним нормативно-правових актів, спрямованих на запобігання та протидію корупції;

– інформує в обов'язковому порядку громадськість про свою діяльність, прийняті рішення та їх виконання;

– збирає, узагальнює та подає органу інформацію про пропозиції інститутів громадянського суспільства щодо вирішення питань, які мають важливе суспільне значення;

– організовує публічні заходи для обговорення актуальних питань.

Для прикладу можна навести *Громадську раду з питань свободи слова та інформації*, яка є постійно діючим незалежним громадським колегіальним експертним органом при Комітеті Верховної Ради України з питань свободи слова та інформації. Громадська рада здійснює координацію у сфері співпраці недержавних організацій та експертів з Комітетом. Основними цілями діяльності Громадської ради є забезпечення права на свободу слова та права на інформацію, реформування національного інформаційного законодавства.

При Державному агентстві України з питань кіно діє *Експертна комісія з питань розповсюдження і демонстрування фільмів*, яка здійснює експертизу фільмів щодо їх потенційної шкоди моральному і фізичному вихованню, культурному розвитку громадян, національній безпеці, правам і свободам людини, здоров'ю населення.

Варто звернути увагу, що до складу громадських рад при органах виконавчої влади можуть входити представники не тільки громадських об'єднань, але й релігійних, благодійних організацій, творчих спілок, професійних спілок та їх об'єднань, асоціацій, організацій роботодавців, органів самоорганізації населення, недержавних засобів масової інформації, інших непідприємницьких товариств та установ.

Відповідно до Постанови Кабінету Міністрів України від 03.11.2010 р. № 996 «Про забезпечення участі громадськості у формуванні та реалізації державної політики» громадські ради діють при всіх центральних та місцевих органах виконавчої влади.

5.3. Державна політика інформаційної безпеки як інструмент забезпечення інформаційної безпеки держави.

Розглядаючи сутність державної політики інформаційної безпеки, насамперед встановимо значення поняття «державна політика». У наукових дослідженнях з державного управління представлено декілька підходів до визначення державної політики.

На думку авторів словника-довідника «Державне управління», державна політика є засобом, що дозволяє державі досягнути певної мети в конкретній галузі, використовуючи правові, економічні, адміністративні методи впливу, спираючись на ресурси, які є в її розпорядженні.

Відповідно до іншого підходу державна політика включає визначення проблеми, цілей та інструментів розв'язання проблеми.

Натомість автори Енциклопедичного словника з державного управління вважають, що державна політика – це дії системи органів державної влади згідно з визначеними цілями, напрямами, принципами для розв'язування сукупності взаємопов'язаних проблем у певній сфері суспільної діяльності.

Таким чином державна політика включає як визначення системи напрямів, методів, завдань щодо досягнення певної мети (теоретична складова), так і комплекс дій, заходів для її втілення в життя (практична складова). Тобто можна говорити про вироблення державної політики як сукупності цілей, завдань, засобів і про реалізацію державної політики – комплексу дій, які практично здійснюються органами державної влади.

З'ясуємо сутність понять «державна інформаційна політика» та «державна політика інформаційної безпеки».

Відповідно до Закону України «Про інформацію» державна інформаційна політика – це сукупність основних напрямів і способів діяльності держави з одержання, використання, поширення та зберігання інформації.

Концепція національної інформаційної політики України визначає національну інформаційну політику як стратегію, напрями і завдання держави у сфері збирання, зберігання, використання та поширення інформації та інформаційних ресурсів у суспільстві.

До головних завдань державної інформаційної політики можна віднести:

– вдосконалення державного регулювання розвитку інформаційної сфери;

– гарантування інформаційного суверенітету України;

– забезпечення прав і свобод громадян в інформаційній сфері, зокрема прав на доступ, використання, розповсюдження інформації, свобода слова, захист приватної інформації тощо;

– розвиток національного інформаційного простору, в тому числі його наповнення достовірною та якісною інформацією, інформування про діяльність органів влади, запобігання негативним інформаційно-психологічним впливам на суспільство, забезпечення інформаційної та духовної, культурної ідентифікації України, а також сприяння розвитку незалежних вітчизняних ЗМІ, інших суб'єктів національного інформаційного простору, протидія його монополізації, упорядкування інформаційних відносин;

– розвиток національної інформаційної інфраструктури, в тому числі створення національних систем і мереж інформації, розробка та впровадження інформаційних і телекомунікаційних технологій;

– ефективне формування і використання системи національних інформаційних ресурсів, в тому числі захист інформаційних ресурсів обмеженого доступу;

– забезпечення присутності у світовому інформаційному просторі, формування позитивного іміджу України;

– сприяння міжнародному співробітництву в інформаційній сфері.

На думку вітчизняних фахівців, на сучасному етапі інформаційна політика держави реалізується за чотирма основними напрямами:

– розвиток національного інформаційного простору (питання пов’язані з діяльністю засобів масової інформації та комунікації, інформаційних агентств, телекомунікацій, бібліотек, архівів тощо);

– розвиток інформаційного суспільства (вироблення та використання новітніх ІКТ та упровадження заснованих на них формах діяльності: Е-уряд, Е-банкінг, електронний документообіг тощо);

– розвиток офіційної комунікації (інформування громадськості, формування позитивного іміджу держави тощо);

– забезпечення інформаційної безпеки держави (захист інформаційного суверенітету, забезпечення інформаційних прав та свобод громадян, визначення режимів функціонування інформації тощо).

Проаналізувавши представлені вище визначення та напрями державної інформаційної політики, можна дійти висновку, що державна політика інформаційної безпеки є її важливою складовою, а також важливим аспектом кожної з інших складових. З іншого боку державна політика інформаційної безпеки є складовою політики національної безпеки України.

Отже, державна політика інформаційної безпеки (забезпечення інформаційної безпеки) - сукупність основних напрямів і способів діяльності держави щодо забезпечення:

– інформаційного суверенітету держави,

– захищеності життєво важливих інтересів особистості, суспільства й держави від негативних інформаційних впливів у всіх сферах життєдіяльності,

– розвитку й захисту всіх елементів національного інформаційного простору, в тому числі інфраструктури та ресурсів,

– захищеності громадян і суспільства загалом від маніпулювання інформацією та негативних інформаційно-психологічних впливів,

– здатності держави запобігати, нейтралізувати чи послаблювати дію внутрішніх і зовнішніх інформаційних загроз як технічного, так і соціально-психологічного характеру.

Забезпечення інформаційної безпеки України має здійснюватися за такими принципами:

– свобода збирання, зберігання, використання та поширення інформації;

– достовірність, повнота та неупередженість інформації;

– обмеження доступу до інформації виключно на підставі закону; гармонізація особистих, суспільних і державних інтересів;

– запобігання правопорушенням в інформаційній сфері;

– економічна доцільність;

– гармонізація українського законодавства в інформаційній сфері з міжнародним; пріоритетність національної інформаційної продукції.

Крім того необхідним є використання комплексного підходу до вирішення проблем забезпечення інформаційної безпеки.

Основними засобами досягнення цілей політики інформаційної безпеки України мають бути:

– створення законодавчої та нормативної баз;

– визначення компетенцій органів державної влади та управління;

– здійснення моніторингу інформаційної безпеки з метою аналізу та розробки заходів задля усунення недоліків та подальшого удосконалення системи забезпечення інформаційної безпеки;

– здійснення контролю за діяльністю юридичних та фізичних осіб у сфері забезпечення інформаційної безпеки;

– фінансова, наукова та матеріально-технічна підтримка юридичних та фізичних осіб, що беруть участь у створенні системи забезпечення інформаційної безпеки;

– стандартизація, сертифікація та ліцензування діяльності в сфері забезпечення інформаційної безпеки;

– удосконалення та розвиток державної інформаційної інфраструктури, в тому числі інформаційних ресурсів з урахуванням вимог інформаційної безпеки;

– удосконалення системи підготовки інтелектуальної еліти суспільства та створення умов для її творчої роботи;

– удосконалення системи освіти та наукової діяльності, а також виховання з урахуванням вимог інформаційної безпеки тощо.

У науці представлено багато бачень щодо напрямів, методів, засобів забезпечення інформаційної безпеки держави. Відомим є поділ усіх засобів та методів забезпечення інформаційної безпеки на нормативно-правові, організаційні та програмно-технічні. Деякі фахівці розглядають це питання детальніше і виділяють крім вище зазначених методи й засоби кадрового, інформаційно-аналітичного, матеріально-технічного, фінансового забезпечення. Відзначено також приналежність до засобів забезпечення інформаційної безпеки держави і зовнішньо-політичних та військових засобів.

Цікавою є схема напрямів та засобів забезпечення інформаційної безпеки держави із відзначенням взаємозв'язків між ними, представлена закордонними науковцями (Рис 6).

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

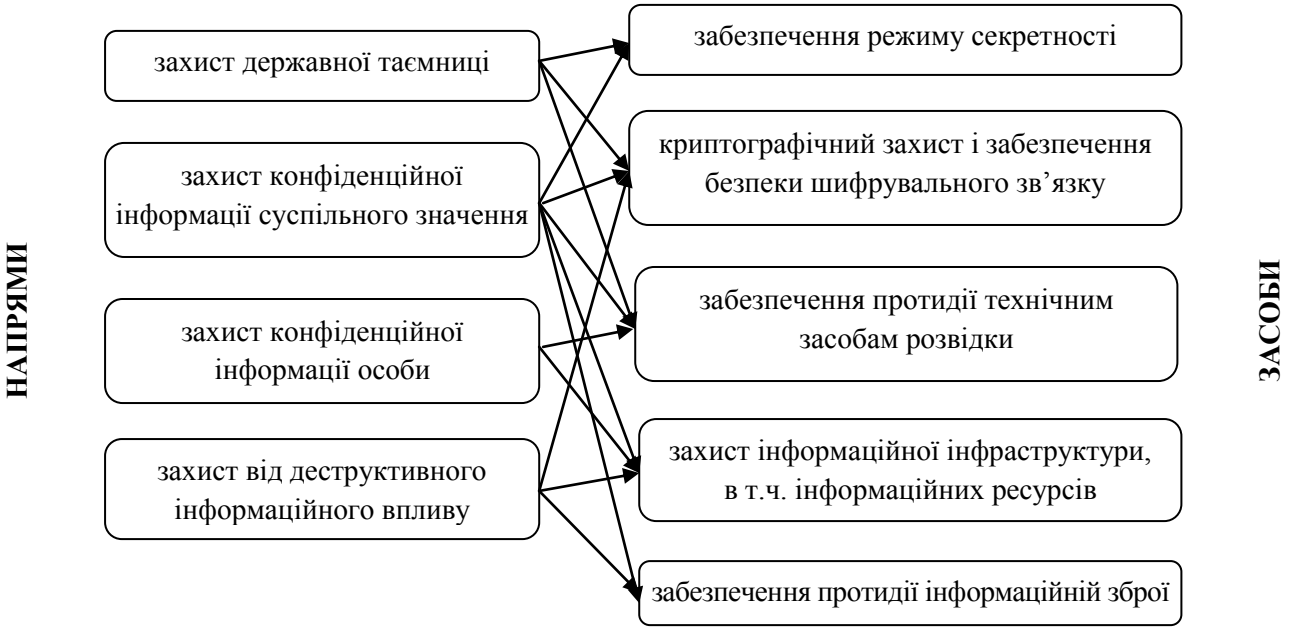

Рис. 6. Напрями та засоби забезпечення інформаційної безпеки дер:

Відповідно до іншого бачення, діяльність із забезпечення інформаційної безпеки держави можна поділити на три основні напрями: державно-управлінський, техніко-технологічний та соціально-змістовний. Детальний, але не вичерпний перелік видів діяльності представлено нижче.

Напрями забезпечення інформаційної безпеки держави

державно-управлінський

- Реалізація державної політики інформаційної безпеки та забезпечення інформаційного суверенітету України.
- Законодавче визначення стратегічних напрямів забезпечення інформаційної безпеки та їх реалізація.
- Удосконалення державного регулювання розвитку інформаційної сфери, протидія її монополізації.
- Належне інформаційне забезпечення прийняття державно-управлінських рішень.
- Постійна відкрита інформаційна взаємодія між державною владою і громадянським суспільством (е-уряд, е-демократія).
- Забезпечення урядового зв'язку і Національної системи конфіденційного зв'язку.
- Участь у міжнародному співробітництві у сфері інформаційної безпеки.
- Протидія поширенню інформації, що містить заклики до зміни конституційного ладу та кордонів держави, міжнаціо-нальної та міжконфесійної ворожнечі.
- Запобігання та протидія інформаційній експансії інших держав, інформаційному тероризму, використанню інформаційної зброї.
- Ведення активної розвідувальної, контррозвідувальної і оперативно-розшукової діяльності з метою забезпечення інформаційної безпеки.

техніко-технологічний

- Забезпечення інноваційного потенціалу країни через впровадження новітніх технологій в інформаційній сфері.
- Підтримка вітчизняних виробників засобів інформатизації та захисту інформації, створення передумов для підвищення їх конкурентоспроможності на світовому та національному ринках.
- Стандартизація, сертифікація і ліцензування засобів інформатизації та захисту інформації.
- Розвиток національного інформаційного простору, створення умов для його інтегрування у світовий інформаційний простір.
- Розвиток, ефективне використання та захист національної інформаційної інфраструктури.
- Розвиток, ефективне використання та захист інформаційних ресурсів, забезпечення вільного доступу до них, формування системи національних електронних ресурсів.
- Управління вітчизняним сегментом мережі Інтернет.
- Технічний та криптографічний захист інформації з обмеженим доступом (службової інформації та інших видів конфіденційної інформації, державної таємниці).
- Запобігання та протидія правопорушенням в інформаційній сфері, комп'ютерним злочинам.

соціально-змістовний

- Наповнення національного інформаційного простору якісним вітчизняним інформаційним продуктом, забезпечення потреб громадян у якісній, повній і достовірній інформації для їх життєдіяльності, освіти та розвитку.
- Поширення у світовому інформаційному просторі достовірної інформації про Україну, розвиток іномовлення.
- Забезпечення законності та незалежності функціонування ЗМІ, запобігання їх монополізації.
- Реалізація конституційних прав і свобод громадян на вільне збирання, зберігання, використання та поширення інформації, свободу думки й слова, вільне вираження своїх поглядів і переконань.
- Захист від маніпулювання інформацією та дезінформування, деструктивних впливів на свідомість, підсвідомість і психіку як індивіда, так і суспільства в цілому.
- Забезпечення приватності життя громадян, захист персональних даних.
- Захист суспільної моралі, духовної, культурної і мовної самобутності.
- Запобігання та протидія поширенню інформації, що пропагує агресію, насильство, наркоманію, алкоголізм та інші негативні суспільні явища.

Питання для самоконтролю

1. Які міжнародні організації займаються питаннями нормативного забезпечення інформаційної безпеки?
2. Які міжнародні стандарти у сфері інформаційної безпеки ви знаєте?
3. Якою є структура вітчизняної нормативно-правової бази у сфері інформаційної безпеки? Назвіть основні законодавчі акти з інформаційної безпеки України.
4. Якою є роль Верховної Ради України та її профільних комітетів у забезпеченні інформаційної безпеки держави? Зазначте повноваження Уповноваженого Верховної Ради України з прав людини у цій сфері.
5. Які повноваження у сфері інформаційної безпеки держави покладено на Раду національної безпеки та оборони України?
6. Охарактеризуйте систему органів виконавчої влади, які виконують завдання із забезпечення інформаційної безпеки держави.
7. Які регуляторні органи виконавчої влади з питань інформаційної безпеки держави ви знаєте? Зазначте їхні основні функції.
8. Якою є роль організацій громадянського суспільства, громадян у забезпеченні забезпеченні інформаційної безпеки держави?
9. Що таке державна інформаційна політика? Якими є її основні завдання?
10. Що таке «державна політика інформаційної безпеки»? Вкажіть відмінності між поняттями «державна інформаційна політика» та «державна політика інформаційної безпеки».

ТЕМА 6. Кібербезпека як складова інформаційної безпеки держави. Проблеми та перспективи забезпечення кібербезпеки в Україні.

6.1. Кібернетична безпека: категорійний апарат.

Насамперед з'ясуємо співвідношення понять «інформаційна безпека» та «кібернетична безпека». Як зазначено вище, зміст поняття «інформаційна безпека» можна розглядати у двох вимірах: перший – роблячи акцент на захищеності інтересів особи, суспільства та держави в інформаційній сфері, другий – через призму безпеки власне інформаційного простору (сфери) та всіх процесів, повязаних з інформацією.

Виходячи з того, що

інформаційний простір – це середовище, в якому здійснюється формування, збір, зберігання та розповсюдження інформації у будь-якій формі (вербальній/невербальній, безпосередній/опосередкованій різними засобами – механічними, технічними, електронними), а

кібернетичний простір – це віртуальний (або, згідно з іншим баченням, поєднання віртуального та реального) простір, сформований інформаційно-телекомунікаційними системами, в яких здійснюється створення, зберігання, обробка й обмін інформації в електронному вигляді,

кібернетична безпека – є частиною інформаційної безпеки і означає стан захищеності кіберпростору, окремих його об'єктів, процесів створення, зберігання, обробки й обміну інформації в електронному вигляді, а також пов'язаних з ними життєво важливих прав та інтересів людини, суспільства, держави.

Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. під кібербезпекою розуміє захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

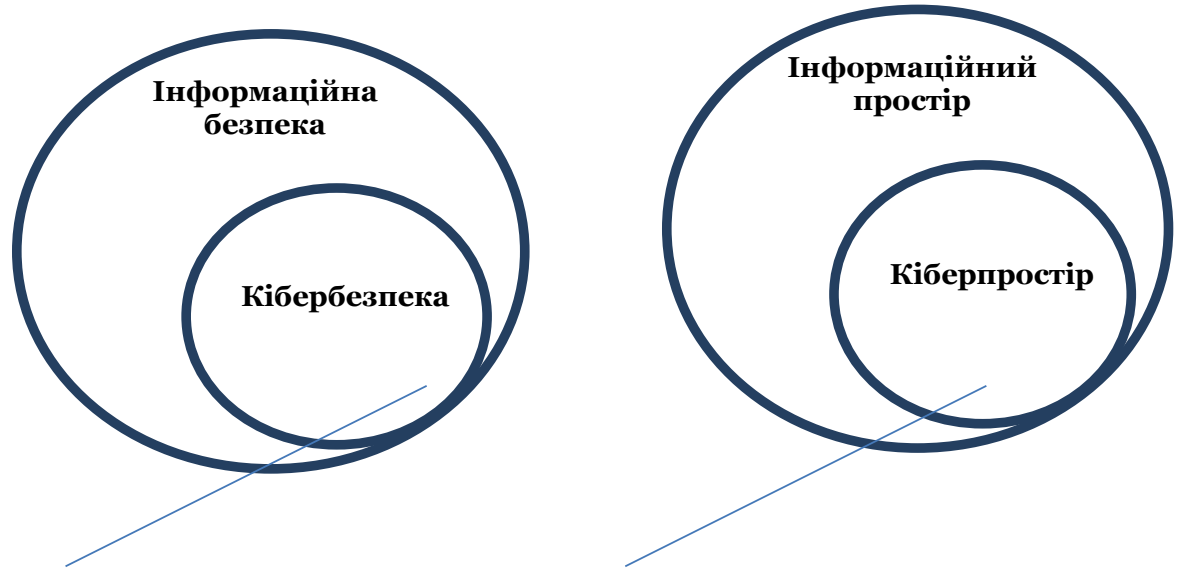

Рис.7. Співвідношення понять «інформаційна безпека» та «кібербезпека», «інформаційний простір» та «кібернетичний простір».

Розглянемо значення споріднених понять, які дадуть змогу в подальшому окреслити напрями забезпечення кібернетичної безпеки держави.

Відповідно до згаданого вище Закону України:

кібератака - спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту;

кіберзагроза - наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об’єктів;

кіберзахист - сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем;

кіберзлочин (комп'ютерний злочин) - суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;

кіберзлочинність - сукупність кіберзлочинів;

кібероборона - сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії;

кібертероризм - терористична діяльність, що здійснюється у кіберпросторі або з його використанням. Під терористичною діяльністю розуміємо свідомі та цілеспрямовані протиправні дії осіб або організованих груп, що спрямовані на порушення роботи критично важливих елементів інфраструктури держави; дестабілізацію суспільно-політичної обстановки в державі та/або ускладнення міжнародних відносин; створення небезпеки для життя і здоров'я людини або задля її залякування; завдання фінансово-майнових збитків, тобто приведення до суспільно-небезпечних і критичних для держави наслідків.

Як показано на Рис.8, повноваження щодо протидії та запобігання основним видам загроз кібербезпеці: кіберзлочинності, кіберагресії та кібертероризму покладаються відповідно на правоохоронну сферу, сферу оборони і оборонно-промислового комплексу держави, сферу державної безпеки.

Рис.8. Загрози кібербезпеці та органи, що забезпечують протидію.

6.2. Сучасний стан забезпечення кібербезпеки в Україні.

Характеризуючи сучасний стан забезпечення кібербезпеки в Україні, слід відзначити, що ще рік тому фахівці виділяли три основні проблеми, що ускладнюють боротьбу проти злочинів в кіберсфері: відсутність усталених визначень ключових термінів; несформованість (не реформованість) чинного нормативно-правового поля; відсутність єдиної загальнодержавної системи протидії кіберзлочинності із відповідним нормативним забезпеченням.

Однак із прийняттям Закону України «Про основні засади забезпечення кібербезпеки України» зроблено суттєві кроки щодо вирішення цих проблем.

Загалом згаданий Закон визначає правові й організаційні засади забезпечення захисту національних інтересів України в кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, також повноваження та обов'язки державних органів в цієй сфері, основні принципи координації їх діяльності щодо забезпечення кібербезпеки.

Слід зазначити, що дія даного Закону не поширюється, зокрема, на:

– відносини та послуги, пов'язані із змістом інформації, що обробляється (передається, зберігається) у комунікаційних та/або в технологічних системах;

– діяльність, пов'язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення;

– соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси), якщо такі інформаційні ресурси не містять інформації, необхідність захисту якої встановлено законом, відносини та послуги, пов'язані з функціонуванням таких мереж і ресурсів;

– комунікаційні системи, які не взаємодіють із публічними мережами електронних комунікацій (електронними мережами загального користування), не підключені до мережі Інтернет та/або інших глобальних мереж передачі даних (крім технологічних систем).

Закон визначає принципи забезпечення кібербезпеки в Україні, серед яких:

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

– забезпечення національних інтересів України;

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

– державно-приватної взаємодії, широкої співпраці з громадянським суспільством у сфері кібербезпеки та кіберзахисту;

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

– пріоритетності запобіжних заходів;

– невідворотності покарання за вчинення кіберзлочинів;

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

– міжнародного співробітництва, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в терористичних, воєнних, інших протиправних цілях;

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

Відповідно до Закону об'єктами кібербезпеки та кіберзахисту є: конституційні права і свободи людини і громадянина; суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища; держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність; національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави; об'єкти критичної інфраструктури.

Об'єктами кіберзахисту, натомість, є: комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону; об'єкти критичної інформаційної інфраструктури; комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

Важливим здобутком Закону України «Про основні засади забезпечення кібербезпеки України» є закріплення на законодавчому рівні базових понять у сфері кібербезпеки (основні з них наведено вище), а також визначення прав і обов'язків державних органів у цій сфері.

Відповідно до Закону Національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури.

Повноваження щодо забезпечення безпеки в кіберпросторі має Президент України через очолювану ним Раду національної безпеки і оборони (РНБО); Національний координаційний центр кібербезпеки як робочий орган РНБО; Кабінет Міністрів і міністерства.

Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів країни в кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (крім об'єктів критичної інфраструктури у банківській системі України).

Основними суб'єктами національної системи кібербезпеки є Держспецзв'язку та захисту інформації, Національна поліція, СБУ, Міноборони та Генеральний штаб ЗСУ, розвідувальні органи, Національний банк України. Суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є: міністерства та інші центральні органи виконавчої влади; місцеві державні адміністрації; органи місцевого самоврядування; правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; ЗСУ, інші військові формування, утворені відповідно до закону; НБУ; підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури; суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

Законом встановлено, що суб'єкти забезпечення кібербезпеки в межах своєї компетенції здійснюють низку різнопланових заходів:

– заходи щодо запобігання використання кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях;

– виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

– інформаційний обмін щодо реалізованих та потенційних кіберзагроз;

– розробку та реалізацію запобіжних, організаційних, освітніх та інших заходів у сфері кібербезпеки, кібероборони та кіберзахисту;

– забезпечення проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління;

– інші заходи із забезпечення розвитку та безпеки кіберпростору.

Відповідно до Закону запропоновано такий розподіл функцій і повноважень органів державної влади у сфері кіберзахисту:

Держспецзв'язку та захисту інформації здійснюватиме функції кіберзахисту об'єктів критичної інформаційної інфраструктури; координацію діяльності інших суб'єктів кібербезпеки; забезпечення створення та функціонування національної телекомунікаційної мережі; запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків; інформування про кіберзагрози і методи захисту від них; забезпечення аудиту інформаційної безпеки на об'єктах критичної інфраструктури, установлення вимог до аудиторів інформаційної безпеки, визначення порядку їх атестації та переатестації;

на Нацполіцію покладено відповідальність за попередження, виявлення, припинення й розкриття кіберзлочинів;

Міністерство оборони та Генеральний штаб ЗСУ мають забезпечувати кібероборону військових об'єктів, кіберзахист об'єктів критичної

інфраструктури під час війни і надзвичайного стану, а також відбивати військову агресію в кіберпросторі;

СБУ в межах своїх повноважень зобов'язана попереджати, виявляти, припиняти та розкривати злочини проти миру та безпеки людства в кіберпросторі, боротися з кібертероризмом і кібершпигунством, а також проводити таємні перевірки об'єктів критичної інфраструктури;

Національний банк є регулятором з кібербезпеки у банківській сфері і має право на встановлення власних стандартів в цій сфері і організацію перевірки їх дотримання. Завданням НБУ є також визначення порядку, вимог і заходів щодо забезпечення кіберзахисту та інформаційної безпеки в банківській системі, створення центру кіберзахисту та реєстру об'єктів критичної інформаційної інфраструктури в банківській системі.

Закон «Про основні засади забезпечення кібербезпеки України» закрив ще одну значну прогалину в нормативно-правовій базі – визначив об'єкти, які можуть бути віднесені до об'єктів критичної інфраструктури. Серед них виділено підприємства, установи та організації незалежно від форми власності, які:

1) провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах;

2) надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я;

3) є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню;

4) включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави;

5) є об'єктами потенційно небезпечних технологій і виробництв.

Законом передбачено державно-приватну взаємодію у сфері кібербезпеки. Так, система своєчасного виявлення, попередження та нейтралізації кіберзагроз може бути створена із залученням волонтерських організацій. Передбачено підвищення цифрової грамотності громадян і культури безпеки поведінки в кіберпросторі. Заплановано обмін інформацією про кіберзагрози і координацію команд реагування на комп'ютерні надзвичайні події. Для громадян, представників промисловості та бізнесу створять консультаційні пункти. Крім того, буде створено систему підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки.

Таким чином, закладено нормативно-правові основи для розбудови національної системи забезпечення кібербезпеки України, здійснено розподіл повноважень між органами державної влади, закріплено роль Національного координаційного центру кібербезпеки як суб'єкта, що здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують

кібербезпеку. Нагальним завданням є координація їх діяльності, процедур взаємодії та засобів комплексного реагування на загрози кібербезпеці держави, так і значної роботи із запобігання кіберзлочинам.

Водночас, в Україні відсутні системні нормативні документи, що описували б саме загрози Україні у кіберпросторі, давали їх визначення та формували основи для цілісної державної політики із кібербезпеки.

Також фахівці відзначають недостатнє кадрове забезпечення відомств фахівцями у сфері кібербезпеки, що є наслідком, з одного боку, низькою якістю підготовки, з іншого – швидким розвитком технологій та відставанням сфери освіти у їх освоєнні, складнощами у залученні до навчального процесу фахівців-практиків, а також небажанням молодих спеціалістів працювати у державних структурах, які не можуть гарантувати надання їм достатніх матеріальних і нематеріальних стимулів. Крім того, відсутні поліпрофільні науково-дослідні інститути, які б займались комплексними дослідженнями з інформаційної та кібербезпеки (як проблемами технологічного, так і соціально-гуманітарного характеру).

На думку деяких фахівців, Україна залишається технологічно вразливою (зокрема у телекомунікаційній сфері), не в останню чергу через надмірно широке впровадження західних програмних продуктів та використання матеріально-технічної бази іноземного виробництва. Пошук можливих «закладок» у цій продукції практично унеможливлений, а залежність української держави від згаданих продуктів становить загрозливий рівень для національної безпеки. Актуальною залишається проблема створення національної операційної системи (принаймні для використання в системі органів державної влади, хоча для такого переходу до програмного забезпечення з відкритим кодом є і суттєві зауваження з боку ключових вітчизняних безпекових організацій), відновлення вітчизняних потужностей із виробництва матеріально-технічної телекомунікаційної бази (особливо для потреб закритих відомчих інформаційних систем), стимулювання з боку держави створення національного антивірусу.

В українському суспільстві, як на рівні державних органів, установ, організацій, так і на рівні особи низькою є культура кібербезпеки, відсутнє усвідомлення необхідності дотримуватися вимог безпеки та наслідків, що можуть настати в результаті їх нехтування.

6.3. Завдання щодо побудови національної системи забезпечення кібербезпеки.

На основі вивчення стратегій кібербезпеки провідних держав світу, можна виділити основоположні завдання щодо побудови національної системи забезпечення кібербезпеки України:

– визначення концептуальних засад державної політики кібербезпеки (понятійно-категоріальний апарат, види загроз кібербезпеці, коротко- та

середньострокові цілі забезпечення кібербезпеки та методи їх досягнення, механізми прийняття рішень, розмежування повноважень та координації діяльності тощо);

– визначення механізму суспільно-державного партнерства, який дозволить приватним та державним зацікавленим сторонам поєднати зусислля щодо запобігання й подолання проблем кібербезпеки;

– визначення об’єктів критичної інформаційно-телекомунікаційної інфраструктури та впровадження національної системи їх захисту;

– розробка системного та інтегрованого підходу до оцінки та управління ризиками кібербепеки на рівні держави;

– формування національних систем моніторингу та реагування на загрози безпеці кіберпростору, системи заходів із нівелювання загроз і вразливостей кіберпростору, відновлення після інцидентів та розслідування кіберзлочинів;

– впровадження нової програми освіти з акцентом на навчання ІТ-фахівців та професіоналів в області кібербезпеки;

– створення системи профілактики кіберзлочинів та підвищення обізнаності населення про конкретні форми кіберзлочинів, способи захисту від них, формування кіберкультури громадян;

– розвиток міжнародної співпраці, участь у боротьбі з кіберзлочинністю на міжнародному рівні.

Як показав огляд Закону України «Про основні засади забезпечення кібербезпеки України» основна частина завдань щодо побудови державної системи забезпечення кібербезпеки нормативно закріплена, на часі впровадження їх у життя.

Питання для самоконтролю

1. Яка різниця між поняттями «інформаційна безпека» та «кібербезпека»?.
2. Яка різниця між поняттями «інформаційний простір» та «кібернетичний простір»?
3. Поясніть значення основних понять у сфері кібербезпеки: кіберзагроза, кіберзлочин, кібератака, кібертероризм.
4. Охарактеризуйте сучасний стан забезпечення кібербезпеки в Україні.
5. Які основні положення Закону України «Про основні засади забезпечення кібербезпеки України»?
6. Які об’єкти можуть бути віднесені до об’єктів критичної інфраструктури держави?
7. Назвіть суб’єктів системи забезпечення України та їх повноваження.
8. Якими є основні завдання щодо побудови національної системи забезпечення кібербезпеки України?

ТЕМА 7. Безпека інформаційних ресурсів та інфраструктури.

7.1. Інформаційні ресурси: сутність та види. Електронні ресурси.

Розглянемо сутність поняття «ресурси» загалом. Так, ресурси визначають як запаси, джерела чого-небудь. Ресурс – це те, що не потребує додаткового опрацювання для того, щоб ним скористатися.

Виникнення такого принципово нового поняття як інформаційні ресурси пов'язано із зростаючою залежністю від наявності інформації, рівня розвитку та ефективності використання засобів її обробки та передачі.

Говорячи про інформаційні ресурси, слід відзначити, що в умовах формування інформаційного суспільства вони набувають першорядної значимості і прирівнюються до капіталу. Сьогодні оволодіння інформаційними ресурсами розглядається як економічна категорія.

В науці представлено декілька підходів до розуміння сутності інформаційних ресурсів. Зокрема, під інформаційними ресурсами мають на увазі сукупність даних, організованих для отримання достовірної інформації в різних областях знань і практичної діяльності, або особливий вид ресурсів, що ґрунтуються на ідеях і знаннях, нагромаджених у результаті науково-технічної діяльності людей і подані у формі, придатній для збирання, реалізації та відтворення.

Також інформаційні ресурси розглядають як складову інфраструктури інформаційного простору, що поєднує в собі дані, їхнє місце (засіб) зберігання, взаємозв'язок між інформаційними елементами, відомості про процеси надходження, зберігання, обробки тощо.

Зміст інформаційного ресурсу ми пропонуємо розглядати у двох аспектах: як процес поступового розвитку інформаційної сфери, та як продукт, тобто об'єкт інтелектуальної праці людини. Інформаційним ресурсом є лише та інформація, що актуалізована в суспільстві: входить у систему людської діяльності й має практичне значення для людини як в її соціальному, так і особистому житті.

У вітчизняному законодавстві перше визначення дефініції «інформаційний ресурс» було наведено у Законі України «Про Концепцію Національної програми інформатизації»: «сукупність документів в інформаційних системах (бібліотеках, архівах, банках даних тощо)».

Визначення поняття інформаційних ресурсів наведено в перших статтях Законів «Про науково-технічну інформацію» (1993 р.) та «Про національну програму інформатизації» (1998 р.). Слід зазначити, що мова йде про інформаційні ресурси, які визначаються як документована інформація, що зберігається в різних інформаційних системах (комп'ютерних базах і банках даних, бібліотеках, архівах, інформаційних сховищах тощо). При цьому під документованою розуміється інформація, зафіксована на матеріальному носії з реквізитами, що дозволяють її ідентифікувати (друкована, теле- і радіопродукція державних і інших засобів масової інформації не є предметом

даного дослідження).

Інформаційний ресурс має низку характерних особливостей.

– на відміну від інших (матеріальних) ресурсів, він практично невичерпний;

– з використанням ІР не зникає, а зберігається і навіть збільшується;

– застосування нового інформаційного ресурсу замість застарілого потенційно може спричинити дії радикального характеру, багаторазово підвищити продуктивність праці, поліпшити використання інших ресурсів тощо;

– ІР не є самостійним і сам по собі має лише потенційне значення. Тільки поєднуючись з іншими ресурсами – досвідом, працею, кваліфікацією, технікою, енергією, сировиною – він є рушійною силою;

– ефективність застосування ІР пов’язана з ефектом повторного виробництва знань; інформаційна взаємодія дозволяє одержати нові знання ціною менших витрат, порівняно з витратами праці, енергії, часу на його пряме генерування;

– ІР виникають в результаті не просто розумової праці, а її творчої частини.

Сьогодні у наукових та нормативних джерелах представлена велика кількість підходів до класифікації інформаційних ресурсів.

Так, наприклад, інформаційні ресурси підрозділяються за класами інформації, що збирається. До первинної інформації, тобто тієї, яка відображає специфіку її джерела, області або сфери створення, виникнення, відноситься інформація, що утворюється самостійно в природних умовах (наприклад, кількість кілець на спилі дерева свідчить про його вік).

Інформація про кількісні та якісні характеристики різних соціальних процесів утворюють клас інформації, яка "знімається". Виділені за цією ознакою інформаційні ресурси можна класифікувати як природні, виробничі, соціально-економічні. Наприклад, інформація про зростання населення.

Інший клас інформаційного ресурсу утворюють відомості, дані, одержані штучно в процесі науково-дослідної діяльності, а також будь-якої творчої роботи. Вона базується на обробці вже наявної інформації зі спеціальним параметрами і моделями (математична обробка, логічна, семантична і т.д.). До цього ж класу відносяться і об'єкти, створені як авторські твори у галузі літератури, мистецтва. Важливим компонентом цих ресурсів є інформація, що отримується в результаті інтелектуальної діяльності людини.

Основні з них подані нижче.

Класифікації інформаційних ресурсів

Критерій	Види ІР
джерело виникнення	– первинні, – вторинні (виникають на основі переробки вже наявної інформації)
вид носія	– паперові, – на машинозчитуваних носіях (кіно-, аудіо-та відеозаписи, електронні), – на каналі зв'язку (ТБ, радіо).
спосіб організації зберігання та використання	– документи на традиційних носіях (книги, газети, журнали), – масив документів, – фонд документів, – архів, – автоматизовані форми.
цільове призначення	масова інформація, бізнес, переписка, особисті, корпоративні, ЗМІ, бізнес, освітні, політика, установи та організації, сервіси та послуги, дошки оголошень, освіта і культура, чати, спорт, відпочинок, зображення і фото, розважальні портали, інші.
зміст	тематична інформація, наукові публікації, рекламна інформація, довідкова інформація, новини, вторинна (бібліографічна) інформація.
сфера життєдіяльності, галузь (ЗУ «Про інформацію»)	– статистичні, – масові (поширювані публічно), – ІР про діяльність державних органів влади та органів місцевого самоврядування, – правові; – ІР про особу; – довідково-енциклопедичні, – соціологічні, – екологічні, – ІР про товар (роботу, послугу); – науково-технічні, – податкові.
обсяг (глобальність)	– глобальні, – загальнонаціональні, – регіональні, – на рівні місцевого самоврядування, соціальних організацій і окремих підрозділів.
джерело	– міжнародні, національні або закордонні,

інформації	– офіційні або неофіційні тощо.
форма власності	– загальнонаціональне надбання, – державна власність, – муніципальна власність, – приватна (особиста, корпоративна) власність.
правовий статус	публічні документи, об’єкти інтелектуальної власності, спам, таємні документи, тощо.
доступ	відкриті або з обмеженим доступом.
мова	англомовні, україномовні, російськомовні тощо.
географічне розташування	європейські, південно-азійські, українські.
важливість	– стратегічні, – тактичні, – операційні.
важливість (міжнародні критерії)	– життєво важливі (пов'язані з виживанням і безпекою нації), – важливі (такі, що здійснюють відчутний вплив на добробут нації та характер міжнародних відносин), – гуманітарні (такі, що безпосередньо не питань свободи, виживання, процвітання нації, але стратегічно й тактично вигідні державі для позитивного позиціонування себе як усередині країни, так і на міжнародній арені).
характер впливу на суспільні процеси	– формувальні (спрямовані на створення суспільних процесів), – стимулювальні (орієнтовані на підтримку та розвиток суспільних процесів), – стримувальні (визначають межі суспільних процесів), – деструктивні, (антиресурс) спрямовані на підрив і усунення визначених процесів).
готовність до використання	– актуальні, – потенційні, – критичні.

Деякі вчені акцентують на тому, що інформаційний ресурс є симбіозом знань та інформації.

Як відзначалося, інформація – це відомості про суб’єкти, об’єкти, явища і процеси. Знання – сукупність фактів, закономірностей, відносин, евристичних правил, що відбивають рівень знайомства з проблемами деяких предметних галузей.

За європейськими стандартами, знання – це комбінація даних (інформації у формі, придатній для автоматизованої обробки її засобами обчислювальної техніки) та інформації, до яких додається точка зору, навички та досвід

експерта, що дає вагомий результат, який може бути використано для прийняття рішень. Знання може бути вичерпним та/або вузьким, індивідуальним та/або колективним.

За іншим визначенням дані – це результат простого збору визначених фактів; інформацією вони стають лише при зв’язуванні у щось корисне, комбінацію хто, що, де і як. У свою чергу знання – це розуміння, як і чому щось відбувається. Українське законодавство взагалі не визначає поняття "знання".

В умовах розвитку інформаційного суспільства та інформатизації усіх сфер життєдіяльності суспільства особливого значення набувають електронні інформаційні ресурси.

Електронні інформаційні ресурси – інформаційні ресурси, які зберігають, обробляють, розповсюджують та представляють користувачеві за допомогою засобів обчислювальної техніки. Їм притаманні такі ознаки: подання інформації в цифровому вигляді (текст, звук, зображення статичне або те, що рухається у цифрових форматах), необхідність програмних та апаратних засобів для її сприйняття людиною (тобто, комп'ютерного обладнання та програмного забезпечення), необхідність телекомунікаційних засобів для отримання або розповсюдження інформації.

У Концепції формування системи національних електронних інформаційних ресурсів визначено, що національні електронні інформаційні ресурси – це «ресурси незалежно від їх змісту, форми, години та місця створення, форми власності, призначені для задоволення потреб громадянина, суспільства, держави. Національні ресурси включають державні, комунальні та приватні ресурси».

Відповідно до Закону України «Про забезпечення кібербезпеки» національні електронні інформаційні ресурси – це систематизовані електронні інформаційні ресурси, які містять інформацію незалежно від виду, змісту, форми, часу і місця її створення (включаючи публічну інформацію, державні інформаційні ресурси та іншу інформацію), призначену для задоволення життєво важливих суспільних потреб громадянина, особи, суспільства і держави. Під електронними інформаційними ресурсами розуміється будь-яка інформація, що створена, записана, оброблена або збережена у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів.

До електронних ресурсів відносять:

– електронні текстові аналоги друкованих видань, таких як книги, журнали тощо (при цьому передбачається, що текстова інформація, котра міститься в них, подана у формі, яка допускає посимвольну обробку);

– електронні образи друкованих видань, коли елементи останніх (наприклад, сторінки) подаються як цілісні графічні образи, до цього ж виду електронної інформації належать образи рукописних матеріалів - факсиміле;

– бази даних, які відповідають вимогам до електронної інформації, наприклад, бібліографічні, адресні, статистичні, лінгвістичні, до цього ж виду

належать і повнотекстові бази даних, якщо вони не відтворюють повною мірою друковані видання;

– нові форми публікацій, що не мають друкованих аналогів, такі як електронні оголошення, матеріали електронних конференцій та інші електронні повідомлення, доступні користувачам через телекомунікаційні мережі;

– електронні публікації аудіо- та відеоінформації;

– мультимедійні продукти;

– програмні продукти;

– комбіновані програмно-інформаційні продукти, наприклад, геоінформаційні системи;

– електронні ігри.

Види електронних інформаційних ресурсів.

1) Засоби масової інформації. До них відносяться різного роду новинні і семантичні сайти (або електронні версії ЗМІ). Їх відмінною рисою є високий рівень відвідуваності, швидка зміна інформації, наявність відеоряду на сайті.

2) Електронні бібліотеки. Електронна бібліотека - розподілена інформаційна система, що дозволяє надійно зберігати і ефективно використовувати різнорідні колекції електронних документів через глобальні мережі передачі даних в зручному для кінцевого користувача вигляді.

3) Електронні бази даних. У найзагальнішому сенсі база даних - це набір написів і файлів, організованих спеціальним чином. Один з типів баз даних - це документи , набрані за допомогою текстових редакторів і згруповані за темами. Інший тип - це файли з електронними таблицями, які об'єднані в групи за характером їх використання.

4) Сайти. Корпоративний сайт - це Інтернет-ресурс, присвячений якійсь організації, фірмі, підприємству. Як правило, він знайомить користувачів з фірмою, напрямами і видами її діяльності, відображає різні довідкові матеріали: прайс -листи, умови поставок і оплати; рекламну інформацію: наявність сертифікатів якості, участь у виставках, публікації в пресі тощо; контактну інформацію.

На відміну від корпоративного сайту виділяють персональний і аматорський сайт, домашню сторінку. Вони відрізняються повнотою інформації, що представляється і професіоналізмом виконання.

Як правило, на сайті можна познайомитися з інформацією вузькотематичної спрямованості. Глибина її розкриття може бути різною: від суто ознайомчої, поверхневої до високопрофесійної, що висвітлює всі сторони діяльності. Визначає інформативність сайту його власник. На сайтах може бути представлена велика кількість гіперпосилань, які допомагають орієнтуватися в ньому.

5) Сервіси - це група сайтів, на яких можна скористатися різноманітними сервісними послугами: електронною поштовою скринькою, блогом (а також познайомитися з правилами його ведення), пошуком, різними каталогами,

словниками, довідниками, прогнозом погоди, телепрограмою, курсами валют і т. д. Наприклад , Яндекс, Укрнет.

Інформаційний портал - це веб-сайт, організований як багаторівневе об'єднання різних ресурсів і сервісів, оновлення якого відбувається в реальному часі. Прикладом інформаційного порталу може служити АСУ портал.

7.2. Національні інформаційні ресурси. Система національних інформаційних ресурсів

Незважаючи на те, що в Україні накопичено велику кількість інформаційних джерел, створено ряд інформаційних центрів, функціонує мережа публічних, наукових й освітніх бібліотек, а обсяги інформації постійно збільшуються, питання формування та використання національних інформаційних ресурсів залишаються постійно актуальними і складними для вирішення.

Законом України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» передбачається, що серед основних напрямів розвитку інформаційного суспільства в Україні слід визначити створення загальнодоступних електронних інформаційних ресурсів на основі врахування національних, світоглядних, політичних, економічних, культурних та інших аспектів розвитку України.

При цьому при створенні загальнодоступних електронних інформаційних ресурсів слід забезпечити генерування національних інформаційних ресурсів в економічній, науково-технічній, соціальній, національно-культурній сферах, охороні довкілля тощо, відповідність електронних інформаційних ресурсів стандартам і технічним регламентам, загальнодержавним, галузевим і локальним класифікаторам і довідникам; створення системи центрів даних, що надають послуги з їхнього зберігання та захисту, збереження в електронному вигляді рідкісних даних, що зберігаються на носіях, які можуть зіпсуватися чи зруйнуватися, із визначенням умов їхнього збереження.

Побіжно Доктрина інформаційної безпеки визначає, що одним з напрямів державної політики у сфері інформаційної безпеки України є розбудова та інноваційне оновлення національних інформаційних ресурсів. При цьому держава з метою забезпечення інформаційної безпеки України має вживати в економічній сфері таких заходів як формування вітчизняної індустрії інформаційних послуг, підвищення ефективності використання державних, корпоративних і приватних інформаційних ресурсів.

Прийнято низку відповідних актів Кабінету Міністрів України, якими, зокрема, передбачається, що має здійснюватися управління та координація діяльності з питань, пов’язаних з формуванням, використанням і захистом національних ресурсів, включаючи ведення Національного реєстру електронних інформаційних ресурсів.

Національні інформаційні ресурси - вся належна Україні інформація, включаючи окремі документи і масиви документів, незалежно від змісту, форми, часу і місця їх створення, форми власності, а також кінцеві результати інтелектуальної, творчої діяльності, зафіксовані на будь-яких носіях інформації, доступні для використання особою, суспільством і державою через засоби масової інформації та телекомунікації, архіви, бібліотеки, музеї, фонди, банки даних, публічні виступи, художньо-виконавську діяльність тощо.

В іншому визначенні звернуто увагу на аспекти правовласності та вартості національних інформаційних ресурсів України, під якими розуміють окремі документи і масиви документів, результати інтелектуальної, творчої та інформаційної діяльності, бази й банки даних, всі види архівів, бібліотеки, музейні фонди та інші, що містять дані, відомості й знання, зафіксовані на відповідних носіях інформації, є об`єктами права власності всіх суб`єктів України і мають споживацьку вартість (політичну, економічну, соціокультурну, оборонну, історичну, ринкову, інформаційну тощо).

З розвитком технологій на передній план стали висуватися проблеми власності і володіння електронними інформаційними ресурсами, визначення прав доступу, формулювання вимог до інформаційного ресурсу як товару. Певні інформаційні ресурси в державі стали набувати статусу національних. Це, в першу чергу, інформаційні ресурси, які містять інформацію з різноманітних аспектів діяльності органів державної влади і місцевого самоврядування, а також юридичних осіб і громадян, що відповідають визначеним вимогам до структури й утримання, та зареєстровані відповідно з регламентованою процедурою. Наприклад, найбільш розвинутою в країні є сфера національних ресурсів науково-технічної інформації. Крім того, для України на даному етапі її розвитку, формування системи управління національними електронними інформаційними ресурсами є стратегічним напрямком і потребує від органів державної влади вирішення проблем, що виникають, з єдиних методологічних позицій.

Аналіз стану електронних інформаційних ресурсів країни визначає множину й інших проблем, які у своїй більшості є загальними для всієї сфери формування і використання інформаційних ресурсів. Серед чинників, що системно впливають на цей комплекс проблем, слід відзначити такі:

– переважно галузевий принцип інформатизації державних органів, що призводить до формування електронних інформаційних ресурсів, орієнтованих, як правило, на задоволення потреб обмеженого кола користувачів;

– відсутність у державних органах та організаціях орієнтації на інформаційне обслуговування громадян;

– неузгодженість і несумісність форматів даних, які зберігаються в різних інформаційних системах, несумісність регламентів і технологій їхнього відновлення, використання різних систем класифікацій і лінгвістичних засобів, що призводить до неоднозначності й суперечливості інформаційних ресурсів різних відомств, неможливості їхнього спільного використання і міжгалузевої

взаємодії;

– відсутність сталої системи зберігання та архівування державних електронних документів, документів електронної пошти та електронних копій паперових документів, а також прийнятих на державному рівні технологій довготривалого зберігання електронних інформаційних ресурсів;

– відсутність єдиних правових норм, які регулюють доступ до державних інформаційних ресурсів, регламентують порядок передачі та використання інформації про діяльність органів державної влади, підприємств і організацій у відкритих мережах і відповідають вимогам інформаційної безпеки.

Ці та інші проблеми в області формування і використання національних інформаційних ресурсів, аналіз їхніх причин свідчать про необхідність корінної зміни пріоритетів у державній політиці в цьому напрямку.

Система національних інформаційних ресурсів - організована за єдиною технологією сукупність національних ресурсів, необхідних для розв'язання завдань соціально-економічного, суспільно-політичного, культурного, духовного розвитку держави (суспільства) та внесених до Національного реєстру електронних інформаційних ресурсів.

Система національних інформаційних ресурсів має відомчі та міжвідомчі ознаки та охоплює інформаційні ресурси:

– органів державної влади і управління, місцевого і регіонального самоврядування;

– державної статистики (державний, обласний, районний рівні);

– архівного, бібліотечного та музейного фондів;

– податкової служби України, правоохоронних і силових структур;

– науково-технічної інформації (створюється у процесі виконання науково-дослідницьких і конструкторських робіт);

– матеріального виробництва, соціальної та фінансової сфер та державного майна і нерухомості.

Окремим видом інформаційних ресурсів, чинне законодавство визначає «інформацію про особу, яка вміщує персональні дані й таємницю особистого життя».

Відповідно до законодавства України прийнято рішення про створення національного реєстру електронних ресурсів - інформаційно-телекомунікаційної системи, призначеної для реєстрації, обліку, накопичення, оброблення і зберігання відомостей про склад, зміст, розміщення, умови доступу до електронних інформаційних ресурсів та задоволення потреб юридичних і фізичних осіб в інформаційних послугах.

До Національного реєстру не включають е-ресурси, які містять відомості, що становлять державну таємницю; інформацію з обмеженим доступом та інформацію, розповсюдження якої заборонене законодавством.

Наступним кроком має стати створення репозитарію електронних ресурсів – інформаційної системи, що забезпечує зосередження в одному місці сучасних електронних інформаційних ресурсів з можливістю надання доступу до них

через технічні засоби, у тому числі в інформаційних мережах (як локальних, так і глобальних).

Для забезпечення формування системи національних ресурсів України необхідно розв'язати такі основні завдання:

– забезпечення широкого доступу до ресурсів, у тому числі іноземних, через глобальні інформаційні мережі;

– правове врегулювання суспільних відносин, пов'язаних з формуванням, використанням та захистом національних ресурсів;

– вироблення рекомендацій щодо приведення національних ресурсів до єдиних стандартів на базі новітніх інформаційних технологій, міжнародних стандартів, уніфікованих систем класифікації і кодування інформації;

– створення ефективних національних пошукових, геоінформаційних (комп'ютерні системи, що забезпечують можливість використання, збереження, редагування, аналізу та відображення географічних даних) та навігаційних систем;

– забезпечення розвитку національної освіти, науки, культури через використання новітніх інформаційних технологій;

– залучення до формування системи національних ресурсів недержавних структур;

– створення умов для забезпечення захисту національних ресурсів незалежно від форми власності;

– сприяння наповненню інформаційного ринку національними ресурсами.

7.3. Інформаційна інфраструктура. Критична інформаційна інфраструктура держави.

Інформаційні ресурси є однією з основних складових інформаційної інфраструктури (інфраструктури інформаційного простору), яка є системою організаційних структур, що забезпечують функціонування й розвиток інформаційного простору та засобів інформаційної взаємодії.

На думку фахівців, інформаційна інфраструктура є сукупністю:

– інформаційних ресурсів, у т.ч. ЗМІ;

– інформаційних технологій як організованої сукупності систем, засобів, методів і способів, яка забезпечує процеси обробки, зберігання, розвитку, поширення, використання та захисту інформаційних ресурсів;

– інформаційно-телекомунікаційних структур – це комп`ютерні мережі, телекомунікаційні мережі й системи спеціального призначення і загального користування, мережі й канали передачі даних, засоби комутації та управління інформаційними потоками;

– відповідних інституційних складових (обчислювальні центри, інформаційні агенції, оператори та провайдери тощо);

– системи забезпечення, що включає засоби нормативно-правового,

економічного забезпечення, стандарти, інструктивні матеріали та документацію, кадрове забезпечення.

Особливий інтерес у контексті інформаційної безпеки держави викликає критична інформаційна інфраструктура, під якою розуміють частину інформаційної інфраструктури, сукупність інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, порушення функціонування яких може призвести до виникнення аварії та/або надзвичайної ситуації, неспроможності держави виконувати свої функції.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» критична інформаційна інфраструктура є сукупністю об'єктів критичної інформаційної інфраструктури, а критично важливими об'єктами інфраструктури (далі - об'єкти критичної інфраструктури) є підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей.

Під об'єктом критичної інформаційної інфраструктури даний закон розуміє комунікаційну або технологічну систему об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури, а до об'єктів критичної інфраструктури відносить підприємства, установи та організації незалежно від форми власності, які:

1) провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах;

2) надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я;

3) є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню;

4) включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави;

5) є об'єктами потенційно небезпечних технологій і виробництв.

Критерії та порядок віднесення об'єктів до об'єктів критичної інфраструктури, перелік таких об'єктів, загальні вимоги до їх кіберзахисту, у тому числі щодо застосування індикаторів кіберзагроз затверджуються Кабінетом Міністрів України, а в банківській системі України - Національним банком України.

Відповідно до Директиви Європейської Комісії серед критеріїв визначення елементів критичної інфраструктури ЄС відзначено:

1) масштаб (географічне охоплення території, для якої втрата елементу критичної інфраструктури завдає значної шкоди);

2) важкість можливих наслідків за такими показниками:

– вплив на населення (число постраждалих, загиблих, осіб, які отримали значні травми, а також чисельність евакуйованого населення);

– економічна шкода (вплив на ВВП, розмір економічних втрат, як прямих, так і непрямих);

– екологічна шкода (вплив на населення та навколишнє природне середовище);

– взаємозв'язок з іншими елементами критичної інфраструктури;

– політичний ефект (втрата впевненості в дієздатності влади);

– тривалість впливу (як саме і коли проявлятимуться наслідки, пов'язані зі втратою чи відмовою об'єктів критичної інфраструктури).

Питання для самоконтролю

1) Визначте сутність поняття «інформаційні ресурси».
2) Які підходи до класифікації інформаційних ресурсів ви знаєте?
3) Поясніть значення поняття «електронні інформаційні ресурси»
4) Назвіть види електронних інформаційних ресурсів.
5) Що таке національні інформаційні ресурси?
6) Які види інформаційних ресурсів охоплює система національних інформаційних ресурсів?
7) Визначте сутність поняття «інформаційна інфраструктура».
8) Поясніть, що таке критична інформаційна інфраструктура держави.
9) Якими є положення Закону України «Про основні засади забезпечення кібербезпеки України» щодо критичної інформаційної інфраструктури держави?

ТЕМА 8. Безпека інформаційного простору.

8.1. Інформаційний простір: основні підходи до визначення.

Сучасне значення поняття "інформаційний простір" склалося в результаті еволюції концептуальної схеми розрізнення в сукупному геополітичному просторі областей, що володіють властивостями, що дозволяють розглядати їх як самостійні простори зі своїми кордонами, структурою, ресурсами та особливостями взаємодії суб'єктів соціальних відносин. Геополітичний простір набуває нового виміру, включивши в себе простір інформаційний.

Геополітика (географічна політика) - наука про контроль над територією, про закономірності розподілу та перерозподілу сфер впливу (центрів сили) різних держав і міждержавних об'єднань.

Інформаційний простір, або інфосфера, являє собою дуже специфічне середовище. В ній помітно змінюється зміст таких процесів, як взаємодія в процесі спільної діяльності, конкуренція (через зміну змісту і характеру конкурентної боротьби між діючими в ньому суб'єктами). У плані силового протиборства змінюється збройна боротьба і перехресне з нею, але не повністю ідентичне інформаційне протиборство.

Особливо істотно в інформаційному просторі змінюється характер геополітичної конкуренції через боротьбу за досягнення інформаційної переваги, за володіння більш розвиненим інформаційним ресурсом, який відкриває кращі можливості контролю над інформаційним ресурсом противника.

В інформаціологічному аспекті розуміння терміна "інформаційний простір" базується на визначенні інформаційної сфери. В даний час існує безліч наукових підходів до трактування даного визначення. Нижче наведені деякі з них.

Інформаційна сфера - кінцевий обсяг осмисленого інформаційного простору.

Інформаційна сфера - сукупність інформації, інформаційної інфраструктури, суб'єктів, які здійснюють збір, формування, розповсюдження і використання інформації, а також системи регулювання виникаючих при цьому громадських відносин.

Інформаційна сфера (середовище) - сфера діяльності суб'єктів, пов'язана зі створенням, перетворенням і споживанням інформації.

Інформаційна сфера - сукупність інформаційних ресурсів, системи формування, поширення і використання інформації, інформаційної інфраструктури.

Інформаційна сфера - специфічна сфера діяльності суб'єктів суспільного життя, пов'язана зі створенням, зберіганням, розповсюдженням, передачею, обробкою і використанням інформації.

Інформаційна сфера - сукупність

суб'єктів інформаційної взаємодії або впливу;

власне інформації, призначеної для використання суб'єктами інформаційної сфери;

інформаційної інфраструктури, що забезпечує можливість здійснення обміну інформацією між суб'єктами;

суспільних відносин, що складаються у зв'язку з формуванням, передачею, розповсюдженням і збереженням інформації, обміном інформацією всередині суспільства.

Інформаційна сфера - сукупність відносин, що виникають при:

формуванні та використанні інформаційних ресурсів на основі створення, збору, обробки, накопичення, зберігання, пошуку, розповсюдження і надання споживачеві документованої інформації;

створенні та використанні інформаційних технологій та засобів їх забезпечення;

захисту інформації, прав суб'єктів, що беруть участь в інформаційних процесах та інформатизації.

На думку окремих фахівців, інформаційна сфера забезпечує:

1. реалізацію права на пошук, отримання, передачу та застосування інформації;

2. виробництво, передачу та розповсюдження вихідної і похідної інформації;

3. формування інформаційних ресурсів, підготовку інформаційних продуктів, надання інформаційних послуг;

4. створення та застосування інформаційних систем (АІС, БД, баз знань), інших інформаційно-телекомунікаційних технологій;

5. створення та застосування засобів і механізмів інформаційної безпеки, у тому числі засобів інформатики та обчислювальної техніки для безпеки систем і мереж, а також програмних і апаратних засобів захисту інформації, що в них обробляється.

Як сфера правового регулювання, інформаційна сфера являє собою сукупність суб'єктів права, які здійснюють інформаційну діяльність, об'єктів права, по відношенню до яких або в зв'язку з якими ця діяльність здійснюється, і соціальних відносин, регульованих правом або підлягають правовому регулюванню.

Окремо взяті інфосфери, занурені в глобальний інформаційний простір, можуть вступати у взаємодію як із самим інформаційним простором, так і з іншими інформаційними сферами. Дві і більше інфосфери можуть вступити в комунікацію між собою за умови наявності загального протоколу обміну інформацією, коду або мови, зрозумілої обом учасникам комунікативного акта.

Інформаційна політика розглядає переважно інформаційно-психологічну складову інформаційних процесів. Відповідно, для інформаційної політики найбільшу значимість має інформаційно-психологічна складова інформаційного простору - інформаційно-психологічна сфера.

Інформаційно-психологічна сфера являє собою частину інформаційної сфери, яка пов'язана з впливами інформації на психічну діяльність людини.

Вона утворюється сукупністю: людей; інформації, якою вони обмінюються і яку сприймають; суспільних відносин, що виникають у зв'язку з інформаційним обміном та інформаційними впливами на психіку людини.

Стосовно до соціальних систем під інформаційною сферою найчастіше розуміється саме інформаційно-психологічна сфера.

Важливою частиною цієї сфери є люди. Психічна діяльність людей становить основу розвитку всіх сфер суспільного життя, визначає інтелектуальний потенціал суспільства, його здатність до розвитку, гідного існування в світовому співтоваристві. На основі цієї діяльності формуються культура, суспільна свідомість, громадська думка з усіх соціально важливих подій. Психічна діяльність, що базується на зборі, обробці, зберіганні, передачі і поширенні інформації, визначає особистісну своєрідність людини, її духовні потреби, мотивацію поведінки, моральні цінності, світогляд, ставлення до оточуючих і суспільству загалом.

Інформаційна сфера є системоутворюючим фактором життя суспільства. Вона активно впливає на стан економічної, політичної, оборонної та інших складових національної безпеки.

Інформаційний простір - це середовище, де здійснюється формування, збір, зберігання та розповсюдження інформації, інформаційна взаємодія організацій та громадян і задоволення їхніх інформаційних потреб.

З позицій синергетики *інформаційний простір* - це відкрита система, що самоорганізується, включає в себе величезну різноманітність інформаційних потоків та інформаційних полів, що знаходяться у взаємодії.

На відміну від інших просторів, де *фізична географія* визначає владу, в інформаційному просторі структуру влади задають *інформація і знання*.

В інформаційному просторі немає звичних кордонів і території. Відстані, географія, кордони можуть бути віднесені до абстрактних штучних категорій, які майже не впливають на відносини між окремими людьми і цілими організаціями.

Значимість в інформаційному просторі для інформаційної політики мають ті його компоненти і процеси, вплив на які засобами і методами інформаційної політики дозволяє впливати на перспективи, впливати на осіб, що приймають рішення, контролювати системи збору, обробки, зберігання та передачі інформації, примножувати ресурси.

На думку американського дослідника Д. Елема, інформаційний простір становить вся сукупність об'єктів, що вступають один з одним в інформаційну взаємодію, а також самі технології цієї взаємодії.

Інформаційний простір в принципі дозволяє існування будь-якого типу інформації, в чому реалізуються його відмінності від простору фізичного плану.

Інформаційний простір є сферою діяльності окремих людей, професійних груп, суб'єктів державного управління, економічних і політичних відносин і т.п. - Тобто фактично будь-якого суб'єкта діяльності, що здійснює таку діяльність цілком або частково з використанням можливостей сучасних інформаційних технологій.

Рівень розвитку інформаційного простору вирішальним чином впливає на основні сфери суспільства - соціально-політичну, економічну. Від цього рівня сильно залежать поведінка людей, формування суспільно-політичних рухів, соціальна безпека. Зв'язавши і інтегрувавши (різною мірою) практично всі країни світу, які мають досить розвинену інфраструктуру систем зв'язку та телекомунікацій, інформаційний простір фактично стер кордони між країнами, що є одним з головних стимулів глобалізації і одночасно результатом цього процесу. З розвитком технічних каналів зв'язку та телекомунікацій інформаційний простір набуває в інформаційному суспільстві глобалізованого світу якість транскордонного (а можливо, і фактичної безмежності) в силу відсутності або неефективності в інформаційному просторі більшості традиційних обмежень, що накладаються рознесеністю різних суб'єктів цього простору в реальному просторі земної кулі і існуванням природних та інституційних перешкод (океанів, гір, державних кордонів тощо). В результаті інформаційний простір соціальних систем, включаючи і компоненти, безпосередньо не відображені в кіберпросторі, також стає транскордонним, що вводить в інформаційні процеси раніше щодо замкнутих систем нових суб'єктів, які можуть надавати через інформаційний простір вплив на "внутрішні" процеси цих систем, порівнянне з впливом традиційних "гравців".

Російський дослідник І.М.Дзялошинський виділяє три підходи до осмислення даного поняття (геополітичне, інформаційно-ноосферне і соціальне розуміння). Розгляд даних підходів дозволяє визначити комунікативний простір з урахуванням усього комплексу його специфічних особливостей.

Так, з *геополітичної* точки зору комунікативний простір можна визначити як «якусь віртуальну територію, яка належить державі, є специфічним державним ресурсом і повинна захищатися від можливих агресорів». Автор уточнює, що даний «простір має не тільки географічні, але й аудиторно-журналістські характеристики». Очевидною вадою цього підходу є те, що, позначаючи комунікативний простір як якусь територіальну одиницю, він не дозволяє відповісти на питання «Де? Де саме перебуває комунікативний простір? Де його межі? ». Але даний підхід має місце бути, тому що «у сфері інформаційних процесів будь-які кордони мають чисто символічний сенс». Таким чином, завдяки даному підходу можна зробити висновок, про те, що комунікативний простір - це деяка територія, що має вкрай невизначені кордони, який неможливо побачити, відчути і, як наслідок, точно виміряти.

Суть *інформаційно-ноосферного* розуміння полягає в тому, що комунікативний простір - це деякий простір (не метричний), який за визначенням не може нікому належати, і в якому розташовується «сукупність

інформаційних ресурсів, засобів забезпечення їх поповнення та обробки, а також механізмів доступу користувачів до цих, як вважають автори концепції, багатств».

Говорячи про *соціальне* розуміння комунікативного простору, слід зазначити, що в дане поняття включили весь спектр інформаційної взаємодії між індивідами. Тобто, всю «сукупність певних структур (індивідів, їх груп і організацій), з'єднаних інформаційними відносинами, тобто відносинами збору, виробництва, розповсюдження та споживання інформації».

З урахуванням наведених уявлень про комунікативний простір, актуальним залишається питання про те, де ж цей простір розташовується. Теоретично у нього можуть бути межі, але настільки розмиті, що чітких вимірів провести неможливо. Науковці також приходять до висновку що «існують феномени, для яких неможлива просторова локалізація. І, по всій видимості, інформація належить саме до таких феноменів». Незважаючи на неможливість просторової локалізації, варто враховувати той факт, що комунікативний простір ділиться на зони за ознакою концентрації інформації.

Таким чином, можна припустити, що комунікативний простір все ж може мати свою проекцію на географічній карті, але так як комунікація може в один момент часу і за певних умов мати місце в певній географічній точці, а в інший момент ні, то даний факт свідчить про те, що комунікативний простір постійно знаходиться в динаміці. На наш погляд, сучасні комунікаційні технології (технології передачі інформації) роблять питання про визначення географічної території комунікативного простору вельми складним, тому що потенційно комунікація може охоплювати всю поверхню земної кулі і навіть доступні куточки космосу (комунікація з астронавтами).

Враховуючи все вищевикладене, можна визначити комунікативний простір як всю «систему різноманітних комунікативних зв'язків, що виникають між різними агентами комунікації».

Відповідно до американської Доктрини інформаційних операцій інформаційний простір має три виміри: фізичний, інформаційний та когнітивний (Рис. 9, 10).

Фізичний розмір складається із систем управління і контролю, ключових осіб, які приймають рішення, та підтримуючої інфраструктури, які дозволяють окремим особам і організаціям створювати ефекти. Це є вимір, де знаходяться фізичні платформи і мережі зв'язку, які їх з'єднують. Фізичний вимір включає в себе людей, системи управління і контролю, газети, книги, мікрохвильові вежі, об’єкти комп'ютерної обробки, ноутбуки, смартфони, планшети, або будь-які інші об'єкти, які підлягають емпіричному вимірюванню. Однак, цей перелік не є вичерпним. Фізичний вимір не обмежується виключно корпоративними або навіть національними системами і процесами; це є єдина мережа, незважаючи на національні, економічні та географічні кордони.

Рис.9. Виміри інформаційного простору.

ВИМІРИ ІНФОРМАЦІЙНОГО ПРОСТОРУ

фізичний вимір	де інформаційний простір накладається з фізичним світом інформаційні системи і мережі *ключові характеристики*: комп'ютери і комунікаційні системи і підтримуюча інфраструктура
нформаційний вимір	де інформація збирається, обробляється, зберігається, оприлюднюється, поширюється і захищається власне інформація і засіб, носій повязує фізичний і когнітивний виміри *ключові характеристики*: зміст інформації, її рух (потоки), якість інформації де відбуваються *автоматизовані процеси прийняття рішень*
пізнавальний (когнітивний) вимір	де відбувається *прийняття рішень людьми* сприйняття інформації через свідомість людини: мораль, солідарність, громадська думка, інформованість *ключові характеристики*: свідоме сприйняття, емоції, обізнаність і розуміння

Рис.10. Виміри інформаційного простору та їх характеристики.

Інформаційній вимір охоплює, де і як інформація збирається, обробляється, зберігається, поширюється, і захищається. Це вимір, де функціонувють системи управління і контролю, передається намір субєкта інформаційного впливу. Дії в цьому вимірі впливають на зміст і рух інформації.

Когнітивний вимір охоплює думки, свідомість тих, хто передає, приймає, відповідає або діє на інформацію. Це стосується інформації, сприйняття, оцінки і прийняття рішень індивідами або групами. Ці елементи знаходяться під впливом багатьох чинників, серед яких індивідуальні та культурні переконання, норми, уразливості, мотивації, емоції, переживання, мораль, освіта, психічне здоров'я, ідентифікації та ідеології. Визначення цих факторів впливу в даному середовищі є критично важливими для розуміння того, як найкращим чином впливати на розум особи, яка приймає рішення, і створити бажані ефекти. Тому ідеологи американської доктрини інформаційних операцій вважають цей вимір найважливішим компонентом інформаційного простору.

8.2. Властивості, функції та структура інформаційного простору.

Основні властивості інформаційного простору.

1. Інформаційний простір *динамічний*. В ньому не буває завершеного стану. Фізичні об'єкти, як правило, мають строго певні фізичні межі. Звідси можливий такий наслідок: досить важко досягти постійного інформаційного домінування, хоча можливе досягнення тимчасової інформаційної переваги.
2. Інформаційний простір *структурований*. Він неоднорідний, в ньому є атрактори, що привертають увагу, і бар'єри, які відвертають увагу споживача від даної точки інформаційного простору.
3. Інформаційний простір завжди *захищений*, в ньому є місця, що свідомо захищаються від чужого входження. Захист одночасно передбачає наявність слабких місць, служить їх детектором.
4. Інформаційний простір *універсальний*: будь-яка область людської діяльності спирається на нього. Звідси і виникають унікальні можливості для впливу в будь-якій професійній області.
5. Інформаційний простір *не пов'язаний безпосередньо з реальним простором через його частково нематеріальну природу*, а також можливості використовувати цивільні інформаційні інфраструктури, які досягають будь-якої точки земної кулі, тоді як звичні військові методи вимагають своїх власних засобів.
6. Інформаційний простір *володіє національно-специфічними способами побудови*, обробки та розповсюдження інформації.
7. Інформаційний простір є базовим для понять інформаційної війни та інформаційної зброї. Інформаційну війну можна визначати як несанкціоновану діяльність у чужому інформаційному просторі.

Для інформаційного простору характерно чітке розрізнення таких понять, як "інформація" і "знання", які в повсякденній свідомості є, по суті,

синонімами. У практичній діяльності в інформаційному просторі інформація починає розглядатися як ресурс - якась "сировина" для "виробництва знань".

Інформаційному простору притаманний особливий тип знань, що забезпечує оформлення інформації в тих чи інших музичних конфігураціях. На відміну від класичної природничої парадигми знання в інформаційному просторі не розглядається як щось непорушне і постійне (яке залежить від мінливих ситуацій і що є істинним незалежно від діапазону можливих інтерпретацій). Основною ознакою такого знання є контекстуальність, тобто залежність від багатьох факторів, у тому числі тих, які не завжди осягаються раціонально. Це знання суб'єктне, тобто залежить від способу аналізу, типу мислення, рефлексії, а також індивідуальної інтуїції, досвіду і т.д. свого творця. Це знання також ситуативне - тобто спочатку і спеціально створюється (і є) тільки до певного спектру ситуацій. Тим самим творець знання в інформаційному просторі стає "конструктором" знань.

Якщо ж певний суб'єкт контролює значний сегмент інформаційного простору (принаймні, щодо інформаційних потоків в певній сфері професійної діяльності або регіоні / країні), то він може в своїх інтересах вже на рівні первинної інформації здійснювати інформаційне наповнення контрольованого сегмента інформаційного простору за допомогою цілеспрямованого відбору інформації та додавання спотвореної інформації (дезінформації).

Основні функції, які виконує інформаційний простір.

1. Інтегруюча. В рамках даної функції інформаційний простір об'єднує в єдину просторово-комунікативну та соціокультурну середу різні види людської діяльності і суб'єктів, які ними займаються, у тому числі як окремих людей, так і цілі держави, народи і міжнародні коаліції і транснаціональні корпорації.

2. Комунікативна. Інформаційний простір створює особливе середовище транскордонної, інтерактивною і мобільної комунікації різних суб'єктів діяльності, в рамках якої вони здійснюють інформаційний обмін.

3. Актуалізуюча. Саме в інформаційному просторі здійснюється актуалізація інтересів різних суб'єктів діяльності за допомогою реалізації ними інформаційної політики.

4. Соціальна. Інформаційний простір трансформує склад суспільства і змінює характер і зміст соціально-політичних (громадських) відносин у всіх сферах - політиці, культурі, науці, релігії та інших.

5. Геополітична. Інформаційний простір формує власні ресурси і змінює значимість традиційних ресурсів, створюючи нове середовище геополітичних відносин і конкуренції.

Структура інформаційного простору

Структура - це сукупність стійких відносин і зв'язків між елементами системи. В структуру входить загальна організація системи (предмета, процесу, явища), просторове і тимчасове розташування складових частин системи і т.д.

Основними структурними складовими інформаційного простору в його синергетичному поданні є *інформаційні поля та інформаційні потоки*.

Інформаційне поле - це сукупність всієї зосередженої в даному обсязі простору-часу інформації, безвідносно до її формі і стану, що знаходиться у відриві як від об'єкта відображення, так і від суб'єкта сприйняття. Інформаційне поле утворюється об'єктивною, генетичною та ідеалізованою інформацією. Рух інформації в інформаційному полі здійснюється за допомогою фізичного зв'язку між реципієнтом і джерелом інформації, матеріалізованого в інформаційному потоці.

Інформаційний потік являє собою в загальному випадку сукупність інформації, що переміщається в інформаційному просторі по каналу комунікації. Інформаційні потоки можуть протікати як усередині окремих інфосфер, так і між ними, в залежності від наявності каналів комунікації.

В організаційно-технічному аспекті *структуру інформаційного простору* становить сукупність баз і банків даних, технологій їх супроводу, використання, інформаційно-телекомунікаційних систем, мереж, додатків та організаційних структур, що функціонують на основі певних принципів і за встановленими правилами, що забезпечує інформаційну взаємодію користувачів, а також задоволення їх інформаційних потреб.

Інформаційна система являє собою організаційно впорядковану сукупність фахівців, інформаційних ресурсів (масивів документів) та інформаційних технологій, у тому числі з використанням засобів обчислювальної техніки і зв'язку, що реалізують інформаційні процеси - отримання вхідних даних; обробку цих даних та / або зміну власного внутрішнього стану (внутрішніх зв'язків / відношень), видачу результату або зміну свого зовнішнього стану (зовнішніх зв'язків / відношень).

До складу технологічних і організаційних компонентів інформаційного простору в узагальненому варіанті входять.

1. *Інформаційно-телекомунікаційна інфраструктура* - територіально розподілені в країні (країнах, світі) комп'ютери, пов'язані між собою в мережі засобами зв'язку і телекомунікації.

Інформаційна інфраструктура - це середовище, яке забезпечує можливість збору, передачі, зберігання, автоматизованої обробки і розповсюдження інформації в суспільстві.

Інформаційна інфраструктура суспільства утворюється сукупністю:

– інформаційно-телекомунікаційних систем і мереж зв'язку, індустрії засобів інформатизації, телекомунікації та зв'язку;

– систем формування та забезпечення збереження інформаційних ресурсів;

– системи забезпечення доступу до інформаційно-телекомунікаційних систем, мереж зв'язку та інформаційних ресурсів;

– індустрії інформаційних послуг та інформаційного ринку;

– систем підготовки і перепідготовки кадрів, проведення наукових досліджень.

2. *Інформаційні ресурси на машинних носіях, насамперед - спеціалізовані інформаційні масиви у вигляді автоматизованих баз даних (АБД), а також інформаційні ресурси, розподілені по WEB-сайтам в мережі Internet.* До інформаційних ресурсів відносяться окремі документи і окремі масиви документів, документи і масиви документів в інформаційних системах (бібліотеках, архівах, фондах, банках даних, базах знань, інших інформаційних системах). Інформаційні ресурси є об'єктами відносин фізичних, юридичних осіб, держави. Інформаційні ресурси можуть бути державними і недержавними і як елемент складу майна знаходитися у власності громадян, органів державної влади, органів місцевого самоврядування, організацій та громадських об'єднань.

Існує ряд особливостей, які відрізняють інформаційні ресурси від інших видів ресурсів:

– вони не піддаються споживанню і піддаються не фізичному, а моральному зношенню;

– вони за своєю суттю нематеріальні і не зводяться до фізичного носія, в якому втілені;

– їх використання дозволяє різко скоротити споживання інших видів ресурсів, що в кінцевому підсумку призводить до колосальної економії коштів;

– процес їх створення і використання здійснюється за допомогою комп'ютерної техніки.

3. *Методи і засоби прикладної математики* - алгоритми і програмні засоби (комплекси), що забезпечують функціонування апаратних платформ (систем).

4. *Організаційні заходи*, що забезпечують функціонування компонентів інформаційного простору (конференції, діяльність робочих груп фахівців і ін.).

5. *Правові заходи (норми*) - інформаційне законодавство, міжнародні угоди і договори, інші національні та міжнародні нормативні правові акти.

6. *Ринок інформаційних технологій, засобів зв'язку, інформатизації та телекомунікацій, інформаційних продуктів і послуг*.

Інформаційний простір соціальних систем включає в себе наступні.

1. Одиниці інформаційного простору, які генерують інформацію:

– у ЗМІ - групові комунікатори (редакції ЗМІ) і ключові комунікатори (комунікатори, безпосередньо включені до редакції ЗМІ, які персоніфікують інформацію даного ЗМІ);

– ньюсмейкери (англ. Newsmaker - букв. "творець новин") - лідери громадської думки (політики, лідери економіки, представники культурної еліти та ін.);

– експерти (інтерпретатори) - спеціалісти, які активно і професійно працюють з інформацією, від їх коментарів (інтерпретації) залежить характер і форма інформаційних потоків (політологи, економісти, соціологи та ін.);

– лідери думок - досить активні люди, які на відміну від перерахованих вище категорій не зав'язані на певні канали розповсюдження інформації, що мають сукупну потребу в поширенні інформації (в малих і середніх соціальних групах);

– виробники спеціальної інформації (театр, кіно, реклама у всіх її проявах поза ЗМІ, мода, товари, гроші (в масових комунікаціях), архітектура і т.п.).

2. Канали комунікацій:

– сформовані ЗМІ та МК (друковані, електронні та інші носії);

– канали міжособистісних комунікацій (міжособистісне спілкування);

– спеціалізовані - спрямовані на вузькі групи - професійні, елітарні і т.п. (спеціалізовані професійні видання, частково - Internet);

– решта (товарно-грошові канали).

3. Області - в соціальних системах формуються за певними соціально-психологічним принципам, включаються в певну мережу (інформаційні канали). Області, включені в певні канали в даний момент часу, можуть перетинатися; розрізняють також області, не включені в канал (и), але які знаходяться під впливом контексту, загального ритму інформаційних процесів і синхронізуються через вторинні впливи.

Стосовно інформації області (в соціальних системах) діляться на (у тому числі в процентному співвідношенні):

– генератори інформації (суперноватори) ~ 3%;

– новатори (швидко сприймають нове від генераторів) ~ 15%;

– центр (помірні новатори / помірні консерватори) ~ 30%;

– суперконсерватори (практично не сприймають змін за рахунок жорстких внутрішніх бар'єрів на все нове) ~ 15%.

Крім перерахованих вище, в інформаційному просторі можна виділити особливі компоненти, значимі для інформаційної політики.

До одного з таких компонентів, зокрема, відноситься *віртуальна реальність*, сформована у вигляді віртуальних аналогів реальних об'єктів і процесів (наприклад, чати і форуми, електронний банкінг, система електронної торгівлі, геоінформаційні системи, системи електронного документообігу, системи автоматизованого проектування і моделювання фізичних процесів і т.п.), які базуються на відповідних програмно-апаратних платформах і інформаційно-телекомунікаційних мережах та системах зв'язку і сприймаються людиною (користувачем) як модель-замінник дійсної реальності або ж як якась реальність, первинна по відношенню до об'єктивної реальності (в разі повного " занурення" людини в ВР).

Хоча людина з моменту зародження цивілізації оточувала себе предметами і процесами, що не існували раніше в природі, тобто якоюсь штучною, рукотворною реальністю, під сучасною ВР, як правило, розуміють віртуальну модель дійсності, побудовану насамперед на інформаційних технологіях, які дають можливість:

– формувати в кіберпросторі цілком адекватну дійсній реальність (або довільно, цілеспрямовано і зловмисно змінену) ВР як певну модель світу (об'єктів, процесів) в будь-якій зручній для сприйняття людською свідомістю формі;

– прив'язувати до елементів цієї моделі будь-які необхідні дані і оперувати ними;

– моделювати результати впливу (управління) до їх реалізації в реальному світі;

– впливати на об'єктивну (дійсну) реальність через її сполучення з ВР шляхом передачі інформаційних повідомлень (керуючих впливів).

В процесі суспільних відносин структура інформаційного простору видозмінюється. Крім удосконалення технічних засобів в процесі інформаційно-телекомунікаційної революції, найбільш значущі для інформаційної політики зміни в інформаційному просторі відбуваються в процесі його професійної сегментації.

Професійна сегментація інформаційного простору являє собою різновид структурування інформаційного простору, пов'язану з професійною діяльністю в ньому різних спільнот, які здійснюють в ньому таку цілком або частково, в ході якої певні його сегменти досить умовно за певними, характерним для такої професійної діяльності ознаками і особливостям вигляду, змісту , функцій та організації взаємної комунікації, об'єднуються в формально відмінні від інших сегментів інформаційного простору "зони".

Суб'єкти діяльності в інформаційному просторі

Склад, ступінь впливу та особливості взаємодії суб'єктів діяльності в інформаційному просторі мають ряд істотних особливостей і водночас володіють загальними базовими властивостями для суб'єктів діяльності кожної сфери.

Суб'єкти діяльності в інформаційному просторі можуть бути як індивідуальними, так і груповими.

Віднесення розглянутих суб'єктів діяльності в інформаційному просторі до одного з цих видів іноді може бути досить умовним, оскільки у ряді випадків велику корпорацію, яка здійснює масштабні інформаційні проекти (PR, медійна діяльність, бізнес-комунікація і пр.), незважаючи на можливу наявність в ній ряду самостійних підрозділів, що здійснюють відповідні види інформаційної діяльності, можна розглядати як індивідуальний суб'єкт, тому що найчастіше інформаційна діяльність таких суб'єктів підпорядкована єдиній логіці і цілі.

В інформаційному просторі групова належність суб'єктів діяльності розглядається в рамках реалізації інформаційної політики з позицій переважно суб'єкт-суб'єктних інформаційних взаємодій, а в інформаційному протиборстві - як об'єкт психологічного (інформаційно-психологічного) впливу. У більшості випадків об'єктом психологічного впливу виступає не одна людина, а цілі соціальні групи людей.

Різні соціальні групи в ряді випадків формуються й існують в такій ролі тільки в інформаційному просторі. Соціальна група являє собою відносно стійку, яка складається в рамках історично визначеного суспільства сукупність людей, об'єднаних єдністю інтересів (а також культурних, національних цінностей і норм поведінки), що знаходяться в більш менш систематичному взаємодії.

Стійкість соціальних груп в інформаційному просторі, незважаючи на часом значну ступінь територіального віддалення членів такої соціальної групи один від одного, забезпечується насамперед наявністю можливостей підтримувати постійну взаємодію, використовуючи глобальні інформаційно-телекомунікаційні системи.

Інтереси, цінності і норми поведінки соціальних груп в інформаційному просторі можуть істотно відрізнятися від традиційних, так як інформаційний простір формує свої інтереси, культурні особливості, цінності та норми поведінки, а традиційні інтереси, цінності і норми при трансфері їх в інформаційний простір зазнають часто суттєві зміни .

Існують такі градації соціальних груп:

1) за розміром - групи великі, середні, малі, мікрогрупи;

2) за громадським статусом - формальні (офіційні) і неформальні (неофіційні);

3) за стійкістю взаємозв'язків членів групи один з одним - реальні (контактні) і умовні (формально виділені по якомусь ознакою);

4) за рівнем розвитку - дифузні, асоціації, корпорації, колективи;

5) за значимістю для членів - референтні (еталонні) і нереферентних.

Для інформаційного простору суспільства характерні деякі унікальні суб'єкти і спільноти, що не мають прямих аналогів в інших просторах.

До таких належать:

- віртуальне соціальне співтовариство (ВСС);
- онлайнове співтовариство;
- мережевий соціум;
- віртуальна коаліція.

Віртуальні соціальні спільноти - соціальні системи, що включають в себе сукупність різних соціальних систем та їх окремих елементів, сегментів інформаційного простору, джерел інтелектуальних і матеріальних ресурсів, розподілених по земній кулі і об'єднаних в рамках досягнення спільної мети єдиної для всіх елементів віртуальної системи ідеологією, що є поряд з відкритими телекомунікаційними мережами (ВТКМ), які забезпечують для елементів системи взаємодія між собою, головним системоутворюючим фактором.

Онлайнове співтовариство є співтовариством суб'єктів діяльності, засноване на масовому перенесенні людьми, групами та організаціями інформаційної активності і взаємодій інтермереж в режимі онлайн. Розвиток Internet супроводжується масовим перенесенням людьми своєї інформаційної

активності, а також і інформаційних взаємодій один з одним, з середовища, створюваного традиційними інформаційно-комунікаційними технологіями у віртуальне середовище мережі Internet, тобто в онлайн. Тим самим один з основних результатів соціально-економічних додатків Internet-технологій полягає в появі в суспільстві великого числа онлайнових співтовариств.

Онлайнові спільноти в простому випадку є групою людей, спілкування яких заснована на використанні Internet-технологій (WEB-форуми, списки розсилки, чати тощо). У складніших випадках - додатково до віртуального способу спілкування люди використовують особливі методи координації та узгодження своєї діяльності, які відрізняються як від ринкових, так і від ієрархічних моделей управління соціально-економічними системами.

Групи людей, які здійснюють свою соціально-економічну діяльність в останньому режимі, утворюють так звані повнофункціональні онлайнові спільноти. Різновидом онлайнового співтовариства є, наприклад, мережева економіка в якій учасники реалізують переважно економічні цілі і завдання, здійснюючи свої економічні взаємодії за допомогою Internet-технологій.

Мережевий соціум - це група людей, взаємодія яких протікає переважно в глобальних комп'ютерних мережах. Обов'язковою характеристикою мережевого соціуму є усвідомлення своєї спільності, члени соціуму пов'язані спільною ідеологією, традицією тощо. У реальному житті будь-яка група взаємодіє в зовнішньому середовищі. Унікальність же мережевих спільнот полягає в тому, що вони діють при повній відсутності зовнішнього середовища.

Віртуальні коаліції - це суб'єкти геополітичної конкуренції, характерні для інформаційного суспільства та глобального інформаційного простору. Крім традиційних суб'єктів геополітичної конкуренції, діючих на глобальному та регіональному рівні, - держав і різного роду міждержавних коаліцій - в інформаційному просторі виникають принципово нові утворення, які включаються в геополітичну боротьбу - "віртуальні" союзи і коаліції, в які на рівних правах можуть входити держави, транснаціональні корпорації, медіа-холдинги тощо, масштаби діяльності яких мають глобальний характер (тобто охоплюють значні географічні території і / або сегменти інформаційного простору), а результати діяльності можуть призводити до наслідків, що впливають на політику держав і їх коаліцій на міжнародному рівні. При цьому володіння державним суверенітетом, власною територією і населенням зовсім не є обов'язковою умовою участі суб'єкта в геополітичній конкуренції, що суттєво відрізняє інформаційне суспільство від індустріального.

Безпосередньо до *суб'єктів діяльності в інформаційному просторі суспільства*, що реалізує державну інформаційну політику, відносяться:

органи державної влади та управління;

*засоби масової інформації і масової комунікації (*ЗМІ та МК).

Органи державної влади і управління в процесі побудови інформаційного суспільства і розвитку інформаційної інфраструктури формують такий суб'єкт

діяльності в інформаційному просторі суспільства, як "електронний уряд" (англ. - E-government).

В США під електронним урядом розуміють державні комп'ютерні системи, призначені для взаємодії з населенням країни (громадянами США, а також іноземцями, наприклад туристами) і структурами, що не входять в уряд. Такими структурами можуть бути бізнес, громадські організації, регіональні і муніципальні органи влади та ін.

Разом з тим однозначного визначення поняття електронного уряду не існує. У випадку під даним терміном розуміється не тільки мережева інфраструктура виконавчої влади, але в цілому вся інфраструктура державної влади і управління, тобто "електронна держава", "електронний державний апарат".

Основою електронного уряду є державна мережева інформаційна інфраструктура як інформаційно-телекомунікаційна система, що забезпечує оптимальне з точки зору суспільства функціонування всіх гілок і рівнів державної влади і управління.

В цьому випадку під "електронним урядом" розуміється мережева інформаційно-телекомунікаційна інфраструктура, підтримуюча процес виконання органами виконавчої влади своїх функцій у суспільстві.

Типовий приклад систем електронного уряду - це подання в Internet інформації про роботу державних структур або оплата податків.

На базі розвитку сучасних методів інформаційного обміну між органами державної влади та суспільством створюються принципово нові можливості для забезпечення інформаційної відкритості та гласності прийняття рішень, для підвищення рівня довіри і взаємодії між суспільством і органами державної влади.

До засобів масової інформації і масової комунікації відносяться інформаційні агентства, періодичні друковані видання, радіо-, теле-, відеопрограми, кінохронікальні програми, інші форми періодичного поширення масової інформації (наприклад, Internet-видання). *ЗМІ і МК утворюють систему засобів масового інформування*, які здійснюють розповсюдження масової соціально значимої інформації, об'єктом впливу для якої виступає масову свідомість. Іноді для позначення ЗМІ та МК використовується термін "мас-медіа" (англ. - Mass-media).

Одна з властивостей ЗМІ І МК, яка використовується в інформаційних війнах, це те, що в цілому *мас-медіа будують свою картину ("віртуальну модель") дійсності, масштаби і суть якої не збігаються з реальними вимірами*. Тим самим *ЗМІ і МК належить особлива роль в наростаючому процесі застосування методів інформаційно-психологічного впливу*. На рубежі XXI століття ЗМІ та МК з передавальної ланки в складному механізмі політики перетворюються на її творця. У поєднанні із засобами вторгнення в психіку людини, маніпулювання його свідомістю ЗМІ та МК можуть стати масовим

каналом впливу на населення країни, керуючи плином подій в житті суспільства.

Інформаційний простір як об'єкт управління в системі державної інформаційної політики

Як об'єкт управління державної інформаційної політики інформаційний простір суспільства (інформаційно-психологічний простір) відноситься до складних динамічних об'єктів з не до кінця прогнозованою реакцією на дії. Для інформаційного простору суспільства характерна наявність прихованих для суб'єкта управління об'єктів і зв'язків, виявлення та облік яких в процесі планування та реалізації управляючих інформаційних впливів ускладнений, а часом і неможливий.

Разом з тим, розвиток засобів і технологій інформаційного управління в поєднанні з використанням управляючих впливів у сфері політики, економіки та культури, робить інформаційний простір досить надійно керованим об'єктом.

Основними структурними елементами інформаційного простору суспільства, на які має здійснюватися управлінський вплив при реалізації державної інформаційної політики, є

суб'єкти, що реалізують і здійснюють масове інформування (ЗМІ та МК), а також

суб'єкти, які активно актуалізують свої інтереси в інформаційному просторі і *генерують значущі в масштабах суспільства і системі його цінностей та інтересів інформаційні потоки*.

Основні суб'єкти управління, які залучаються для генерації управляючих інформаційних впливів, є:

органи державної влади та управління (насамперед, структури, котрі вступають в активну комунікацію з населенням - служби зв'язків із громадськістю та підрозділи, що реалізують концепцію електронного уряду),

державні та недержавні засоби масового інформування, а також

недержавні суспільно-політичні об'єднання, чия інформаційна та комунікативна діяльність відповідає офіційно декларованим національним інтересам.

Об'єктами управління в інформаційному просторі суспільства для суб'єктів, що реалізують державну інформаційну політику, виступають, в загальному випадку, *всі елементи та системи, існуючі в цьому просторі*.

При плануванні та реалізації керуючих впливів на елементи та системи інформаційного простору суспільства в рамках державної інформаційної політики використовується систематизація об'єктів управління, яка дозволяє розподілити види, форми, характер і засоби управління. У загальному випадку така систематизація може бути проведена таким чином.

1. *Об'єкти, що мають матеріально-технічну природу* - вся *інформаційно-телекомунікаційна інфраструктура суспільства*. Державна інформаційна політика у відношенні цих об'єктів реалізується насамперед шляхом формування умов, що забезпечують стійке функціонування і розвиток цієї

інфраструктури, доступність для всіх членів суспільства, інтеграцію їх у інформаційний простір і здійснювану в ньому професійну та комунікативну діяльність.

2. *Об'єкти, що мають віртуальну / віртуально-матеріальну природу - інформація, що циркулює в інформаційному просторі суспільства та його інформаційні ресурси*. Управлінським завданням державної інформаційної політики щодо цих об'єктів є *контроль за інформаційними процесами і потоками, інформаційне і правове їх регулювання* (у тому числі шляхом регулювання суспільних відносин у сфері інформаційного обміну), *забезпечення захисту інформації та інформаційних ресурсів, а також формування інформаційного фону і створення інформаційних потоків / полів,* характер і зміст яких (їх впливу на реципієнтів) відповідає цілям і *завданням органів державної влади та національним інтересам* щодо збереження соціальної та політичної стабільності в суспільстві, розвитку культури та науки, та іншим соціально значущим завданням.

3. *Об'єкти, що мають людську природу - люди та їх спільноти*. Управління даними об'єктами в рамках державної інформаційної політики демократичної держави має здійснюватися за принципами *суб'єкт-суб'єктних відносин, інформаційної відкритості та рівноправної інтерактивної комунікації*.

Специфічним об'єктом управління для державної інформаційної політики є *інформаційний простір геополітичного конкурента*, з яким ведеться явне або приховане інформаційне протиборство. В цьому випадку методами управління є переважно приховані, маніпулятивні методи, а застосовувані засоби і технології відносяться до арсеналу ведення інформаційного протиборства та проведення інформаційно-психологічних операцій (акцій інформаційно-психологічного впливу).

8.3. Національний інформаційний простір. Особливості формування та сучасний стан національного інформаційного простору України.

У науці та законодавстві України представлено багато визначень національного інформаційного простору. Розглянемо деякі з них. Отже, під ***національним інформаційним простором*** розуміють:

- інформаційний простір, на який розповсюджується юрисдикція країни;
- сферу, у якій здійснюються інформаційні процеси та встановлюються інформаційні відносини між суб’єктами під юрисдикцією держави;
- сфера (об`ємний простір), у якій здійснюються інформаційні процеси і на яку поширюється юрисдикція України (проект Закону України “Про інформаційний суверенітет та інформаційну безпеку України”);
- середовище, в якому здійснюється продукування, зберігання та поширення інформації і на яку розповсюджується юрисдикція України (проект

“Концепції інформаційної безпеки України”, розробленій УЦЕПД ім. Разумкова);

- середовище на території держави, де на основі наявної інформаційної інфраструктури здійснюється формування, збір, зберігання та розповсюдження інформації (як національного так і закордонного походження), а також інформаційна взаємодія організацій та громадян і задоволення їхніх інформаційних потреб відповідно до чинного національного законодавства;

- сукупність національних інформаційних ресурсів та інформаційної інфраструктури, які дозволяють на основі єдиних принципів і загальних правил забезпечувати інформаційну взаємодію громадян, суспільства, держави з їх рівним правом доступу до відкритих інформаційних ресурсів та максимально повним задоволенням інформаційних потреб суб`єктів держави на всій її території з додержанням балансу інтересів на входження у світовий інформаційний простір та забезпечення інформаційної безпеки відповідно до Конституції України та міжнародних правових норм (бачення Національного інституту стратегічних досліджень);

- важлива ознака суверенної й незалежної держави, яка дбає про формування й розвиток його на всій території України на основі єдиних принципів і за загальними правилами з додержанням балансу інтересів особи, суспільства, держави;

- сфера інформаційних обмінів, яка складається з розгалуженої системи структур, що забезпечують створення нової інформації, зберігання та захист наявної, а також організацію її використання за допомогою мережі засобів комунікації усередині країни та за кордоном з метою забезпечення інформаційних інтересів та потреб громадян і з рештою - інформаційної безпеки держави.

Виходячи з зазначеного, держава має захищати свій національний інформаційний простір і забезпечувати його розвиток та використання в інтересах власного суспільства та громадян. Саме тому розвинуті держави розглядають розбудову власного інформаційного простору як основу свого соціально-економічного, політичного й культурного розвитку та здійснюють цілеспрямовану державну інформаційну політику з урахуванням змін і тенденцій у глобальному інформаційному просторі.

Чинне законодавство не визначає правовий статус інформаційного простору України – важливу ознаку й передумову формування інформаційного суспільства, входження України у світове інформаційне співтовариство, один із головних чинників збереження інформаційного суверенітету, зміцнення державності та забезпечення національної безпеки України.

Світовий досвід і сучасні вітчизняні наукові дослідження свідчать про те, що сформувати юридично обґрунтоване поняття “інформаційний простір України” можна враховуючи сукупність елементів інформаційного простору держави та функціональні напрями державної діяльності, що передбачено

поняттям “національний інформаційний простір” і виходячи виключно із суверенного права України на самостійне й незалежне вирішення цього питання.

Інформаційний простір створюється державою та суспільством з певними цілями, характеризується певними ознаками. Інформаційний простір – це середовище, у якому циркулюють інформаційні потоки, його топологічні властивості задаються інформаційною інфраструктурою. В свою чергу, інформаційний потік – інформація, яка переміщується у просторі й часі, а інформаційна інфраструктура - частина інформаційного простору, що забезпечує створення й циркуляцію в ньому інформаційних потоків.

На думку фахівців, доцільно визначити такі основні елементи інформаційного простору України:

- національні інформаційні ресурси України – це окремі документи і масиви документів, результати інтелектуальної, творчої та інформаційної діяльності, бази й банки даних, всі види архівів, бібліотеки, музейні фонди та інші, що містять дані, відомості й знання, зафіксовані на відповідних носіях інформації, є об`єктами права власності всіх суб`єктів України і мають споживацьку вартість (політичну, економічну, соціокультурну, оборонну, історичну, ринкову, інформаційну тощо);
- національна інформаційна інфраструктура, до складу якої входять:
- організаційні структури, що забезпечують формування, функціонування й розвиток інформаційного простору, а також збирання, обробку, зберігання, поширення та ефективне використання інформаційних ресурсів. Обслуговуючу роль щодо діяльності цих елементів виконують науково-методичне, інформаційне, матеріально-технічне, кадрове, фінансове забезпечення;
- інформаційно-телекомунікаційні структури – це територіально розподілені державні і корпоративні комп`ютерні мережі, телекомунікаційні мережі й системи спеціального призначення і загального користування, мережі й канали передачі даних, засоби комутації та управління інформаційними потоками;
- інформаційні технології – організована сукупність систем, засобів, методів і способів, яка на базі інформаційної інфраструктури забезпечує процеси обробки, зберігання, розвитку, поширення, використання та захисту інформаційних ресурсів;
- система засобів масової інформації – це сукупність друкованих і електронних засобів масової інформації – теле-, радіокомпаній, інформаційних агентств, комплексів книговидання, кінематографічного, бібліотечного, архівного тощо.

На думку фахівців, інформаційна політика держав на сучасному етапі має реалізуватися за чотирма основними напрямами:

- *розвиток національного інформаційного простору* (питання пов’язані з діяльністю засобів масової інформації та комунікації, інформаційних агентств, телекомунікацій, бібліотек, архівів тощо);
- *розвиток інформаційного суспільства* (вироблення та використання

новітніх ІКТ та упровадження заснованих на них формах діяльності - Е-уряд, Е-банкінг, електронний документообіг тощо);

- *розвиток офіційної комунікації* (процеси інформування громадськості, формування позитивного іміджу держави тощо);
- *забезпечення інформаційної безпеки держави* (захист інформаційного суверенітету, забезпечення інформаційних прав та свобод громадян, визначення режимів функціонування інформації тощо).

Щодо реалізації державної інформаційної політики в Україні, як сукупності напрямів діяльності держави в інформаційній сфері, то аналіз наявної ситуації засвідчує, що інформаційна сфера в цілому досі залишається позбавленою цілісної системи регулювання. Проте, якщо в питаннях розвитку інформаційного суспільства та забезпечення інформаційної безпеки є певна системність зокрема, як в частині державного управління та законодавчого регулювання, так і бюджетного фінансування, то питання розвитку національного інформаційного простору та офіційної комунікації на державному рівні врегульовані меншою мірою.

Протягом останніх років Україна стабільно утримує середні позиції у світових рейтингах розвитку інформаційного суспільства, хоча позитивна динаміка забезпечується не стільки завдяки імплементації найсучасніших ІКТ, скільки за рахунок «наздоганяючого» запровадження телекомунікацій чи стільникового мобільного зв'язку, що говорить про недостатність заходів державної політики на означеному напрямі.

Означена ситуація пов'язана як з об'єктивними чинниками (випереджальними темпами розвитку інформаційних технологій та платформ розповсюдження інформації - Інтернет-видань, мобільного та Інтернет телебачення та радіо тощо), так і суб'єктивними чинниками (суспільною чутливістю питань, пов'язаних з державним регулюванням діяльності засобів масової інформації та комунікації).

Проте, внаслідок недостатньої урегульованості, в національному інформаційному просторі України нині спостерігається низка негативних явищ, які стоять на заваді як розвитку суб'єктів ринку, так і забезпеченню інформаційних прав та свобод громадян, а подекуди й створюють загрози національній безпеці України.

Актуальною проблемою постає діяльність нових типів ЗМК поза правовим полем - зокрема, визначення свого статусу та порядку реєстрації (ліцензування) потребують як так звані конвергентні аудіовізуальні ЗМК, так і Інтернет-видання (електронна преса).

Окремою проблемою, зокрема через суспільну чутливість питання, постає законодавче регулювання відповідальності за розміщення інформації в мережі Інтернет, що стосується насамперед двох вимірів: захисту авторських прав і захисту честі та гідності.

Практика ЗМІ останніх років, актуалізує проблему професійної компетентності та моральної відповідальності журналістів перед суспільством,

зокрема у контексті забезпечення права та свобод громадян в отриманні достовірної й повної інформації.

Серед чинників, які перешкоджають розвитку та забезпеченню безпеки інформаційного простору України варто відзначити такі: наступальна політика іноземних держав в галузі глобального поширення інформації та новітніх ІТ; активна протиправна діяльність різних суб'єктів (від держав до індивідів) в інформаційному просторі, спрямована на здійснення деструктивного впливу як технічного, так і соціально-психологічного характеру; технологічне та кадрове відставання у розвитку ІТКС; недостатні темпи науково-технічного і культурного розвитку українського суспільства; низька правова, організаційна та програмно-технічна забезпеченість в галузі інформаційної безпеки тощо.

Стан інформаційного простору України характеризується також наявністю протиріччя між потребами суспільства в розширенні вільного обміну інформацією і необхідністю окремих обмежень на її поширення. Необхідно відзначити, що порушенню інформаційної безпеки сприяє безсистемність захисту інформації і слабка координація дій щодо захисту інформації в загальнодержавному масштабі.

Загалом вирішення проблем розвитку та забезпечення безпеки інформаційного простору вимагає загальносистемного підходу – здійснення заходів у трьох вимірах: концептуальному, законодавчому та інституціональному.

Завдання щодо розвитку інформаційного простору України:

– удосконалити нормативно-правову базу з питань забезпечення розвитку інформаційної сфери та прискорити її адаптацію до європейських правових норм та стандартів;

– забезпечити єдині принципи і загальні правила взаємодії всіх суб'єктів інформаційної діяльності при оптимальному співвідношенні державного регулювання і саморегулюючих початків у формуванні й розвитку інформаційного простору держави;

– забезпечити належну координацію дій усіх зацікавлених суб'єктів під час запровадження інструментів е-демократії;

– покращити умови для безпечної інформаційної взаємодії держави, організацій і громадян, а також максимально повного задоволення інформаційних потреб держави, організацій і громадян на всій території держави;

– удосконалити інституціональний механізм формування, координації та здійснення контролю за виконанням завдань розбудови інформаційного суспільства;

– забезпечити дотримання конституційних прав громадян на інформацію;

– підвищити рівень інформаційної представленості України в Інтернет-просторі та присутності в ньому українських інформаційних ресурсів;

– забезпечити прийняття системних державних рішень, спрямованих на стимулювання створення національних інноваційних структур (центрів,

наукових парків і технопарків) для розроблення конкурентоспроможних вітчизняних інформаційно-комунікаційних технологій;

– підвищити на державному рівні значущість українського сегмента Інтернету як одного з найважливіших інструментів розвитку інформаційного суспільства та конкурентоспроможності держави;

– розробити на національному та місцевому рівні механізм ефективної громадської участі та громадського контролю за реалізацією пріоритету розбудови інформаційного суспільства.

– стимулювання розвитку національного виробництва текстового і аудіовізуального контенту, зокрема шляхом створення системи квотування та проведення цільових конкурсів на надання грантів;

– забезпечення функціонування Суспільного телебачення і радіомовлення України, у тому числі його належного фінансування;

– створення системи мовлення територіальних громад, яка сприятиме розширенню комунікативних можливостей та зниженню конфліктності всередині громад;

– підтримка вітчизняної книговидавничої справи, зокрема перекладів іноземних творів, забезпечення ними навчальних закладів і бібліотек;

– розвиток правових інструментів захисту прав людини і громадянина на вільний доступ до інформації, її поширення, оброблення, зберігання та захист;

– комплексна підтримка розвитку механізмів саморегуляції засобів масової інформації на засадах соціальної відповідальності;

– підвищення медіа-грамотності суспільства, сприяння підготовці професійних кадрів для медіа-сфери з високим рівнем компетентності;

– удосконалення законодавчого регулювання інформаційної сфери відповідно до актуальних загроз національній безпеці;

– задоволення потреб населення тимчасово окупованих територій в об'єктивній, оперативній і достовірній інформації;

– повне покриття території України цифровим та Інтернет-мовленням замість аналогового і надання рівних можливостей доступу кожному громадянину до інформаційних ресурсів мережі Інтернет;

– формування системи державної підтримки виробництва вітчизняного аудіовізуального продукту;

– пропагування, у тому числі через аудіовізуальні засоби, зокрема соціальну рекламу, основних етапів і досвіду державотворення, цінностей свободи, демократії, патріотизму, національної єдності, захисту України від зовнішніх і внутрішніх загроз;

– забезпечити баланс інтересів держави і світового співтовариства при входженні України в глобальний інформаційний простір та забезпечення її національного інформаційного суверенітету.

Питання для самоконтролю

1. Поясніть сутність та співвідношення понять «інформаційна сфера», «інформаційне середовище», «інформаційний простір».
2. Якими є виміри інформаційного простору відповідно до Доктрини інформаційних операцій США?
3. Якими є властивості та функції інформаційного простору?
4. Назвіть основні елементи структури інформаційного простору.
5. Назвіть основних суб'єктів та об'єкти інформаційного простору.
6. Назвіть особливості сучасного стану національного інформаційного простору України.
7. Які завдання щодо формування й розвитку інформаційного простору стоять перед Україною?

Список використаної літератури

1. Андріяш В. І. Державна політика: концептуальні аспекти визначення. Електронний ресурс. – Режим доступу: http://www.dy.nayka.com.ua/?op=1&z=626
2. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти/ За загальною редакцією д-ра юрид. наук, проф. Бандурки О.М..: Монографія. – Харків: Вид-во Ун-ту внутр. Справ, 2000. – 368 с.
3. Ашманов И. Информационный суверенитет: новая реальность: презентация. -Електронний ресурс. Режим доступу: http://rossiyanavsegda.ru/read/948/
4. Богуш В. М., Кривуца В. Г., Кудін А. М. «Інформаційна безпека: Термінологічний навчальний довідник». - за ред. Кривуци В. Г. – Київ, 2004. - 508 с.
5. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В. Л. Бурячок, Г.М.Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП УКРАЇНА», 2015. – 449 с.
6. Жарков Я.М., Дзюба М.Т., Замаруєва І.В., ін. Інформаційна безпека особистості, суспільства, держави: Підручник. – К.: Видавничо-поліграфічний центр "Київський університет", 2008. – 274 с.
7. Забезпечення інформаційної безпеки держави: Навчальний посібник / В. Б. Дудикевич, І. Р. Опірський, П. І. Гаранюк, В. С. Зачепило, А. І. Партика. Львів : Видавництво Львівської політехніки, 2017. 204 с.
8. Іванченко Є.В., Іванченко І.С., Хорошко В.О., Хохлачова Ю.Є.Забезпечення інформаційної безпеки держави Є.В. Іванченко [та ін.] ; за ред. проф. В.О. Хорошка ; Вид-во Нац. авіац. ун-ту, 2016. 254 с.
9. История развития компьютера. Електронний ресурс. Режим доступу: http://daypic.ru/internet/43409
10. Інформаційна безпека України в умовах євроінтеграції: конспект лекцій. Електронний ресурс. – Режим доступу: http://pidruchniki.com/1584072028356/politologiya/informatsiyna_bezpeka_ukrayini_v_umovah_yevrointegratsiyi
11. Карпенко В. Інформаційна політика та безпека: підручник. – Київ, 2006. -Електронний ресурс. Режим доступу: http://ukrlife.org/main/karp/bezpeka15.htm
12. Климчук О. О. Забезпечення інформаційної безпеки держави : підручник / [О. О. Климчук, В. М. Петрик, М. М. Присяжнюк та ін.] ; за заг. ред. О. А. Семченка та В. М. Петрика. – К. : ДНУ «Книжкова палата України», 2015. – 672 с.
13. Климчук О. О. Забезпечення інформаційної безпеки у провідних країнах світу : навч. посіб. / [О. О. Климчук, Д. С. Мельник, В. М. Панченко, В. М. Петрик та ін.] ; за заг. ред. В. М. Петрика. – К. : Вид-во ІСЗЗІ НТУУ «КПІ», 2014. – 260 с.

14. Либкинд А. Информационная безопасность – история проблемы и ее решение. Електронний ресурс. Режим доступу: http://psyvert.ru/meta/infosec/

15. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. - К.: КНТ, 2006.

16. Манойло А.В. Государственная информационная политика в особых условиях: Монография. Глава 3. Електронний ресурс. – Режим доступу: http://www.evartist.narod.ru/text24/0027.htm

17. Національний інформаційний простір України: проблеми формування та державного регулювання: Аналітична доповідь НІСД України. [Електронний ресурс]. – Режим доступу: www.niss.gov.ua/public/File/2013_table/1119_dop.pdf

18. Національний інформаційний суверенітет у контексті розвитку новітніх інформаційних технологій / [О. С. Онищенко, В. М. Горовий, В. І. Попик та ін.]. – К. : НБУВ, 2011. – 154 с.

19. Олійник О. В., Соснін О. В., Шиманський Л. Є. Політико-правові аспекти формування інформаційного суспільства суверенної і незалежної держави. Електронний ресурс. - Режим доступу: http://old.niss.gov.ua/book/Sosnin_2.htm

20. Остроухов В.В., Присяжнюк М.М., Петрик В.М. та ін. Інформаційна безпека (соціально-правові аспекти): Підручник / За ред. Є.Д.Скулиша. – К., 2010. – 776 с.

21. Пєвцов Г.В., Залкін С.В., Сідченко С.О., Хударковський К.І. Інформаційна безпека у воєнній сфері: проблеми, методологія, система забезпечення: [монографія]. – Харків : Цифрова друкарня № 1, 2013. – 270 с.

22. Петрик В.М., Присяжнюк М.М., Мельник Д.С. та ін. Забезпечення інформаційної безпеки держави: підручник ; за заг. ред. О.А. Семченка та В.М. Петрика. - К.: ДНУ «Книжкова палата України», 2015. - 672 с.

23. Про Рекомендації парламентських слухань на тему: "Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України": Постанова Верховної Ради України від 31.03.2016 № 1073-VIII. http://zakon3.rada.gov.ua/laws/show/1073-19

24. Соснін О.В. Інформаційна політика України: проблеми розбудови. [Електронний ресурс] – Режим доступу: http://www.niisp.gov.ua/vydanna/panorama

25. Тихомиров О.О. Класифікації забезпечення інформаційної безпеки. Електронний ресурс. – Режим доступу: http://tihoma-law.at.ua/Tihomyrov_klasifikacii_zabezpechennya_ infobezpeky.pdf

26. Урсул А., Цырдя Т. Информационная безопасность. сущность, содержание и принципы ее обеспечения. [Електронний ресурс]. – Режим доступу: http://www.security.ase.md/publ/ru/pubru22.html

27. Юдін О.К., Богуш В.М. Інформаційна безпека держави: Навч. посіб. – Харків: Консул, 2005. – С.39-41.

Список нормативно-правових документів

1. Конституція України: прийнята на п’ятій сесії Верховної Ради України 28 червня 1996 р. – К.: Преса України, 1997. – 80 с.
2. Закон України «Про інформацію» // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 651; Із змінами від 06.04.2000, ВВР. – 2000. – № 27. – Ст. 213; від 07.02.2002, ВВР. – 2002. – № 29. – Ст. 194; від 03.04.2003, ВВР. – 2003. – № 28. – Ст. 214.
3. Закон України «Про державну таємницю» від 21 січня 1994 р. // Відомості Верховної Ради України. - 1994. - № 16. – Ст. 93.
4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 02.08.1994 // Відомості ВРУ. - 1994. - № 31. – ст. 286
5. Закон України «Про національну програму інформатизації» від 17.07.1998 // Відомості Верховної Ради України. - 1998. - № 27. – Ст.181
6. Закон України від 13.01.2011 № 2939-VI «Про доступ до публічної інформації». [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2939-17
7. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007−2015 роки» від 9 січня 2007 року № 537-V // Відомості Верховної Ради України. − 2007. –№ 12. – Ст. 102.
8. Закон України «Про захист персональних даних» від 01.06.2010 р. № 2297-VI // Відомості ВРУ. - 2010 р. - № 34. – ст. 1188, стаття 481
9. Закон України «Про основні засади забезпечення кібербезпеки України» // Відомості ВРУ. - 2017 р. - № 45. - стор. 42, стаття 403
10. Закон України «Про національну безпеку України» // Відомості Верховної Ради України. – 2018. – № 31. – Ст. 241.
11. Розпорядження КМУ від 15 травня 2013 р. № 386-р «Про схвалення Стратегії розвитку інформаційного суспільства в Україні». [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/386-2013-%D1%80/page
12. Указ Президента України від 26 травня 2015 р. № 287/2015 «Про рішення Ради нац. безпеки і оборони України від 6 травня 2015 р. «Про Стратегію національної безпеки України» // Офіційний вісник Президента України. - 2015 р. - № 13. - стор. 50. - стаття 874
13. Указ Президента України від 15 березня 2016 року №96/2016 «Про рішення Ради нац.безпеки і оборони України від 27 січня 2016 р. «Про Стратегію кібербезпеки України» // Офіційний вісник Президента України. - 2016 р. - № 10. - стор. 39. - стаття 198
14. Указ Президента України від 25 лютого 2017 року № 47 «Про рішення Ради нац.безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» // Офіційний вісник Президента України. - 2017 р. - № 5. - стор. 15. - стаття 102
15. Конвенція Ради Європи щодо кіберзлочинності // Офіційний вісник України. -2007 р. - № 65. - стор. 107. - стаття 2535