**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»**

**Інститут публічної служби та управління**

**Кафедра публічного управління та регіоналістики**

**Д.держ.упр., проф. Приходченко Л.Л.**
**К.н.держ.упр. Хромова Ю.О.**

# КОНСПЕКТ ЛЕКЦІЙ

**з дисципліни**

# «ІНФОРМАЦІЙНА БЕЗПЕКА»

Розглянуто та схвалено на засіданні
кафедри публічного управління та регіоналістики.
Протокол № 1 від 31 серпня 2023 р.

Одеса – 2023

Інформаційна безпека: Конспект лекцій. Укладачі: Приходченко Л.Л., Хромова Ю.О. «Одеська політехніка». 2023. 191 с.

Конспект лекцій укладено відповідно до робочої програми навчальної дисципліни «Інформаційна безпека». Метою викладання навчальної дисципліни «Інформаційна безпека» є формування комплексу знань з основ теорії та практики, практичних умінь та навичок, а також інших компетентностей щодо забезпечення ефективного захисту інформації, оволодіння методичними підходами для аналізу комплексу проблем, що виникають у процесі запобігання та усунення загроз в інформаційній сфері, розроблення і реалізації конкретних заходів щодо їх розв'язання в умовах широкого застосування інформаційних технологій.

***Ключові слова***: національна безпека, інформаційна безпека, державна інформаційна політика, державна політика, національні інтереси, національний інформаційний суверенітет, забезпечення інформаційної безпеки, кібербезпека, інформаційні війни, загрози інформаційній безпеці, інформаційні впливи, інформаційне протиборство, інформаційний простір, механізми протидії інформаційним війнам та захисту інформаційного простору, публічне управління, система публічного управління, управління, російська військова агресія.

## ЗМІСТ


| | | |
|---|---|---|
| ***Лекція 1*** | Вступ до дисципліни. Теоретичні засади інформаційної безпеки. | **6** |
| ***Лекція 2*** | Теоретичні засади інформаційної безпеки | **19** |
| ***Лекція 3*** | Інформація як об’єкт інформаційної безпеки | **32** |
| ***Лекція 4*** | Взаємозв’язок інформаційної діяльності та інформаційної безпеки | **49** |
| ***Лекція 5*** | Національні інтереси у сфері інформаційної безпеки | **62** |
| ***Лекція 6*** | Національний інформаційний суверенітет та державна інформаційна політика | **72** |
| ***Лекція 7*** | Загрози інформаційній безпеці | **84** |
| ***Лекція 8*** | Безпека інформаційного простору | **91** |
| ***Лекція 9*** | Інформаційні війни як джерело загроз безпеці держави | **103** |
| ***Лекція 10*** | Нормативно-правове та інституційне забезпечення інформаційної безпеки України | **120** |
| ***Лекція 11*** | Інформаційна безпека України: особливості, моделі, механізми | **136** |
| ***Лекція 12*** | Механізми протидії інформаційним війнам та захисту інформаційного простору України | **148** |
| ***Лекція 13*** | Інформаційна безпека системи публічного управління та адміністрування | **161** |
| ***Лекція 14*** | Інформаційна безпека України в умовах російської військової агресії | **170** |
| ***Лекція 15*** | Адаптація міжнародного досвіду та перспектив розвитку забезпечення інформаційної безпеки України | **180** |
| **Рекомендована література** | | **188** |

# ЗАГАЛЬНІ МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ДЛЯ ОПРАЦЮВАННЯ ЛЕКЦІЙНОГО МАТЕРІАЛУ З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ІНФОРМАЦІЙНА БЕЗПЕКА»

Важливе місце у вивченні студентами дисципліни «Інформаційна безпека» відіграють лекції.

Лекції слугують тим підґрунтям та інструментом, що спрямовують студентів у найбільш раціональному напрямі щодо вивчення навчальної дисципліни та надають йому знання в обсязі, необхідному для подальшого поглибленого вивчення матеріалу навчальної дисципліни, роз'яснюють найбільш складні поняття та положення.

Самостійна робота на лекції містить у собі такі види діяльності:

– активне слухання лектора;

– виділення головного матеріалу лекції;

– конспектування основних положень;

– підбиття підсумку сказаного;

– формулювання висновку або узагальнення.

Плідна робота студентів на лекціях є запорукою подальшого успішного оволодіння тим необхідним масивом знань, що сприятиме формуванню із студента фахівця з необхідним рівнем знань та навичок.

Систематичне *опрацювання лекційного матеріалу* має важливе значення для його засвоєння. Студенту рекомендується опрацьовувати матеріал в той день, коли читалася лекція. При цьому слід перевірити повноту і правильність запису, доповнити пропущене, дописати незакінчені фрази, докреслити схеми тощо.

На даному етапі варто розібратися в сутності кожного поняття, визначення і положення, домогтися розуміння логічного змісту формулювань. Після такої роботи слід співставити матеріал лекції з програмою дисципліни і з допомогою рекомендованої літератури доповнити конспект матеріалом, що не розглядався на лекції. На заключному етапі рекомендується сформулювати та записати резюме (висновок) до матеріалу лекції. При нерозумінні окремих питань студенту належить звернутися за консультацією до викладача.

Звичайно, що матеріал попередньої лекції до наступної може стати забутим. Тому студенту напередодні лекції слід переглянути конспект попередньої лекції. Інакше студент ризикує не зрозуміти лектора та загубити зв'язок між викладеним раніше матеріалом і новим.

Таким чином, робота студента над конспектом лекцій повинна проводитись в напрямку вдосконалення самого конспекту, в напрямку засвоєння матеріалу; в напрямку подальшого розширення та поглиблення питань, що викладенні на лекції.

Після *завершення вивчення* теми студенту слід проаналізувати отриману інформацію, з'ясувати які нові теоретичні відомості він одержав та як їх застосувати в практичній діяльності. На завершення роботи з конкретною темою треба прочитати питання для самоконтролю та мислено або письмово дати відповіді на них. У разі виникнення потреби, студенту слід звернутися за консультацією до викладача.

Оскільки основною формою опанування програмного матеріалу є самостійна робота, студент має уявляти власний рівень розуміння кожної теми дисципліни. Тому до кожної теми лекції та практичного заняття наведені питання для самоконтролю.

При підготовці до *практичних занять* студенту необхідно напередодні ознайомитися із змістом відповідного заняття та теоретичними положеннями за допомогою рекомендованої літератури і конспекту лекцій.

На початку лекції, як правило, викладач оголошує тему лекції, план її проведення та необхідну навчальну літературу і нормативно-правові джерела. Крім того, посилання на наукову і спеціальну літературу а також нормативно-правові джерела здійснюються викладачем в ході проведення лекції. Тому, під час лекції студенти повинні уважно слухати викладача, аналізувати отримувану інформацію, а також конспектувати найбільш важливі та необхідні масиви інформації, що надається.

В кінці лекції студент може задати викладачеві питання щодо роз'яснення незрозумілих положень прослуханої лекції. Належне ведення конспекту під час лекції сприятиме збереженню необхідної інформації та надасть йому змогу в подальшому проаналізувати її.

Робота над конспектами лекцій. При підготовці до практичних занять студент уважно читає складений ним конспект лекції та аналізує повторно отримувану інформацію.

При опрацюванні матеріалу лекції він звіряє наявність викладеного на лекції та законспектованого ним матеріалу із планом семінарського заняття, що знаходиться у навчально-методичному комплексі та методичних матеріалах для проведення семінарських та практичних занять із обраної дисципліни.

При відсутності у конспекті матеріалу з окремих питань лекції, неповне розкриття того чи іншого питання лекції або винесенні їх на самостійне опрацювання чи написання реферату, доповіді зобов'язує студента звернутися до рекомендованих підручників, навчальних посібників та нормативно-правових актів.

Вивчення навчального матеріалу з підручників, навчальних посібників, робота з нормативно-правовими джерелами, опрацювання матеріалу за першоджерелами, науковою і спеціальною літературою. Працювати із підручниками, навчальними посібниками та нормативно-правовим джерелами, науковою і спеціальною літературою необхідно так, щоб отримати з них максимум теоретичних знань та необхідних відомостей.

При роботі з цими джерелами студент, в першу чергу, повинен ознайомитись із їх змістом, щоб визначити, чи необхідно опрацьовувати дане джерело і чи має воно відношення до навчального курсу, що вивчається, а лише після цього відбирає необхідний для вивчення матеріал з цього джерела (глави, розділи і т. ін.) та розпочинає його вивчення. При опрацюванні матеріалу необхідно з'ясувати суть питання, що вивчається, не уникаючи при цьому визначення суті незрозумілих чи незнайомих слів, термінів та не з'ясувавши їх змісту у словниках, довідниках, контексті речення.

При вивченні матеріалу за підручником, навчальним посібником, роботі із науковою і спеціальною літературою необхідно аналізувати прочитане із прослуханою та законспектованою лекцією, робити логічні висновки, відмічати незрозумілі положення з метою їх подальшого з'ясування на практичному занятті.

Тому під час опрацювання студентом матеріалу за підручником, навчальним посібником, опрацюванні матеріалів нормативно-правових актів бажано і необхідно відпрацювати зручну для себе певну систему позначень (підкреслювання, помітки на полях книги чи нормативно-правового акту, виписки, позначення маркерами різних кольорів, формулювання інших авторів та нормативно-правових джерел, посилання на інші джерела, виписки необхідних відомостей на окремих листках та ін.) та фіксації опрацьованого матеріалу.

Крім того, при роботі із науковою та спеціальною літературою студент може отримати посилання на джерела не вказані в навчально-методичному комплексі, що є, безперечно, цінним для самостійного поглибленого вивчення правового матеріалу.

# ЛЕКЦІЯ 1
# ВСТУП ДО ДИСЦИПЛІНИ. ТЕОРЕТИЧНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

**ПИТАННЯ, ЯКІ РОЗГЛЯДАЮТЬСЯ:**

1.1 Підходи до визначення поняття «інформаційна безпека»: сутнісне та змістовне наповнення.
1.2 Принципи, форми та методи забезпечення інформаційної безпеки держави.
1.3 Інформаційна безпека: її роль та місце в системі національної безпеки України.
1.4 Критерії визначення об'єктів інформаційної небезпеки та їх обґрунтування, їх ієрархія.
1.5 Основні завдання інформаційної безпеки.

## ВИКЛАД МАТЕРІАЛУ

***Вступ до дисципліни***

Метою викладання навчальної дисципліни «Інформаційна безпека» є формування комплексу знань з основ теорії та практики, практичних умінь та навичок, а також інших компетентностей щодо забезпечення ефективного захисту інформації, оволодіння методичними підходами для аналізу комплексу проблем, що виникають у процесі запобігання та усунення загроз в інформаційній сфері, розроблення і реалізації конкретних заходів щодо їх розв'язання в умовах широкого застосування інформаційних технологій.

Предметом навчальної дисципліни «Інформаційна безпека» є процеси, методи та засоби захисту інформації, запобігання та усунення загроз в інформаційній сфері, підтримки та удосконалення систем управління інформаційної безпеки у загальній системі національної безпеки в Україні.

Завдання навчальної дисципліни:

- формування знань щодо: концептуальних засад, принципів, форм та методів забезпечення інформаційної безпеки; кращих практик світового досвіду застосування методів та засобів забезпечення інформаційної безпеки держави; взаємозв'язку інформаційної безпеки з інформаційним суверенітетом, національною безпекою та правами людини; загального напряму і тенденцій розвитку стратегії захисту інформації в Україні;
- вироблення аналітичних навичок аналізу інформаційних загроз та протидії з використанням знань теорії і практики інформаційної безпеки у практиці публічного управління, моделювання систем та процесів захисту інформації з врахуванням загроз та дестабілізуючих факторів інформаційної безпеки, інформаційного протиборства;
- удосконалення навичок аналітичної, виконавчо-розпорядчої діяльності, розроблення і реалізації конкретних заходів щодо забезпечення ефективного захисту інформації, з достатньою обґрунтованістю, використанням різноманітних інформаційних джерел, з розумінням професійного та суспільного контексту ситуації, забезпечуючи науковий підхід до визначення напрямів і можливостей вдосконалення системи інформаційної безпеки України.

***Методи:***

Логіка викладання курсу вибудувана на основі застосування компетентнісного підходу. Вихідними принципами побудови навчально-пізнавального процесу є принципи системності, орієнтованості на наявний практичний досвід здобувачів вищої освіти, самоактивності, орієнтації на результат, зворотного зв'язку тощо. При вивченні курсу навчальної дисципліни «Інформаційна безпека» використовується низка взаємопов'язаних методів навчання, а саме:

1) В ході проведення лекційних занять застосовується монологічно-проблемний метод за допомогою якого висвітлюється складна природа формування та функціонування системи інформаційної безпеки, пошуково-показовий метод, за допомогою якого

забезпечується активність та стимулюється пізнавальний інтерес до вивчення матеріалу та самостійного пошуку. Активно використовується метод візуалізації. Лекції вибудувані на основі використання методів концентрації, контрасту, ступінчастості, що у сукупності надає змогу відобразити комплексно та у системних взаємозв'язках феномени забезпечення інформаційної безпеки.

2) При проведенні практичних занять використовується низка інтерактивних методів навчання задля активізації здобувачів вищої освіти, зокрема частина практичних занять побудована у формі тренінгів, активно використовуються метод колективно-групового навчання («мозкового штурму»), технології ситуативного моделювання (елементи імітаційних ігор), технології опрацювання дискусійних питань (дискусії, оцінювальні дискусії, «займи позицію – зміни позицію», шкала думок тощо).

3) Задля стимулювання навчальної та пізнавальної діяльності здобувачів вищої освіти в залежності від теми та форми проведення заняття застосовується проблемний виклад навчального матеріалу, частково-пошуковий та дослідницький методи.

4) Навчальним курсом передбачено самостійне опрацювання навчального матеріалу, яке передбачає застосування таких методів як самостійне опрацювання фахової літератури, комунікацію, самозвіт, моделювання ситуацій, процесів тощо.

5) Для формування «гнучких навичок» у ході курсу застосовується сукупність методів, спрямованих на розвиток організаційних, когнітивних та інформаційних, комунікативних, життєвих, громадських навичок, зокрема до таких методів та форм віднесемо роботу в групах, тренінги та евристичні методи навчання, також інтерактивні методи.

6) В умовах карантинних обмежень технічне забезпечення курсу в режимі дистанційного навчання відбувається за допомогою використання електронних ресурсів, так за допомогою платформи Google Meet та використання можливостей Zoom проводяться лекції та консультації з важливих питань, проводяться практичні заняття у формі дистанційних тренінгів, за допомогою Google-Classroom доводяться завдання, здійснюється контроль за виконанням завдань та самостійною роботою, за допомогою Google-форм проводиться поточний та підсумковий контроль якості знань.

***Форми проведення занять*:** навчальні заняття (лекції, практичні заняття як в очній формі, так і он-лайн, а також консультації); виконання індивідуальних завдань на практичних заняттях та під час самостійної роботи, контрольні заходи, самостійна робота. Використовується індивідуальна та групова форма роботи здобувачів з застосуванням Google-класів та Google-форм.

***Практичне значення та використання отриманих знань.***

У процесі опанування дисципліни «Інформаційна безпека» здобувачі отримують необхідні знання (формування необхідних компетентностей) під час лекційних і практичних занять та виконання самостійної роботи. Усі види занять розроблені відповідно до положень вимог кредитно-модульної системи організації навчального процесу. У процесі навчання здобувач повинен набути професійних компетентностей та отримати результати навчання. Сформовані під час вивчення дисципліни «Інформаційна безпека» компетентності вдосконалюються на переддипломній практиці та надають можливість успішно скласти кваліфікаційний екзамен та використати набути знання під час написання кваліфікаційної робити (постреквізити).

Протягом вивчення дисципліни формуються наступні гнучкі навички та якості (softskills): стратегічне та тактичне мислення, лідерські якості щодо здійснення управлінської діяльності із застосування методів та засобів забезпечення інформаційної безпеки держави; набуття вмінь та навичок надання консультації органам державної влади і органам місцевого самоврядування щодо аналізу інформаційних загроз та їх протидії, здійснення

експертно-аналітичного супроводу захисту інформації; готовність брати на себе відповідальність в процесі прийняття управлінських рішень.

***Програмні результати навчання:***

ПРН7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища

ПРН10. Формувати елементи (складові) стратегії національної безпеки держави (за сферами забезпечення та видами діяльності).

ПРН14. Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію з питань національної безпеки до фахівців і нефахівців, зокрема до осіб, які навчаються.

ПРН15. Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів.

***1.1. Підходи до визначення поняття «інформаційна безпека»: сутнісне та змістовне наповнення.***

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, адже 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 дійсності. «Відкриття» поняття інформації сучасною наукою відбулося в середині XX століття і, на часі науковцями представлено чимало підходів до розуміння поняття «інформація», які підчас несумісні і протирічать один одному.

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

Що стосується поняття «інформаційна безпека», то насамперед слід зазначити, що 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. Ми ж за вихідні засаду візьмемо розуміння того, що безпека це 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.

Поняття інформаційної безпеки як стану, знайшло своє відображення також у чинній Стратегії інформаційної безпеки (затверджена Указом Президента України від 28 грудня 2021 року № 685/2021), відповідно до якої інформаційна безпека України – складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави.

Дане визначення поняття інформаційної безпеки сформульовані *з позиції статусного*

*підходу*. З позиції ж концептуального підходу, інформаційна безпека сприймається як рівень захищеності життєво важливих інтересів людини, суспільства і держави в інформаційній сфері від зовнішніх та внутрішніх загроз (А. Форос).

У межах *концептуального підход*у, дослідження інформаційної безпеки акцентоване на можливості соціальних та інформаційних систем ефективно функціонувати в умовах активізації зовнішніх та внутрішніх загроз. В цьому контексті інформаційна безпека – це спроможність системи протистояти випадковим або навмисним внутрішнім і зовнішнім загрозам (К. Захаренко).

Досить поширеним є підхід, за якого досліджуване явище розуміється як *суспільні (соціальні) відносини*. Так, інформаційна безпека – це вид суспільних інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності; суспільних правовідносин, пов'язаних із створенням, розповсюдженням, зберіганням та використанням інформації (Р. Калюжний, В. Цимбалюк).

В межах *інструментального підходу* інформаційна безпека сприймається як сукупність засобів забезпечення інформаційного суверенітету України, захисту інформаційної сфери від зовнішніх і внутрішніх інформаційних загроз. Ця безпека має включати ефективну протидію сукупності інформаційних загроз (Л. Наливайко).

З позиції *протекціоністського підходу*, який є досить розповсюдженим серед іноземних науковців, інформаційна безпека ототожнюється із захистом. Зокрема, в дослідженнях Alkhudhayr F., Alfarraj S., Aljameeli B., Elkhdiri S., інформаційна безпека визначається як захист інформації, системи та апаратного забезпечення, які використовують, зберігають і передають інформацію, для забезпечення цілісності, конфіденційності та доступності даних, а також захищені операційні процедури. О. Дзьобан та Є. Мануйлов зазначають, що, інформаційна безпека – це і захист інформації, і захист від інформації. Відповідно на основі існуючих формулювань стосовно інформаційної безпеки, можна зазначити, що представлений підхід до сутності інформаційної безпеки обумовлює сприйняття останньої як *захисту інформації (інформаційних ресурсів, систем, засобів забезпечення) та захисту суспільства від деструктивних інформаційних впливів*.

Дуже важливим є *процесуальний підхід*, згідно з яким інформаційна безпека представляється, як процес або сукупність процесів, які виникають і протікають в інформаційних та соціальних системах і призначені для досягнення цілей публічного управління в інформаційній сфері. В цьому контексті інформаційна безпека – це одна з характеристик інформаційної системи, яка на певний момент часу володіє деяким станом (рівнем) захищеності, а захист інформації – це процес, який повинен виконуватися неперервно на всьому протязі життєвого циклу інформаційної системи (О. Шумейко).

Зосередження уваги на *внутрішньому суб'єктивному сприйнятті інформаційної безпеки*, формує поняття інформаційної безпеки: «відчутна інформаційна безпека», яка визначається як суб'єктивна ймовірність, з якою споживачі інформації вважають, що їхня особиста інформація не буде переглядатися, зберігатися або змінюватися неналежними сторонами під час транспортування або зберігання у спосіб, що відповідає їхнім впевненим очікуванням (K. Challappa Ramnath A. Paul, A. Pavlou).

Таким чином, під *інформаційною безпекою* слід 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.1.1).

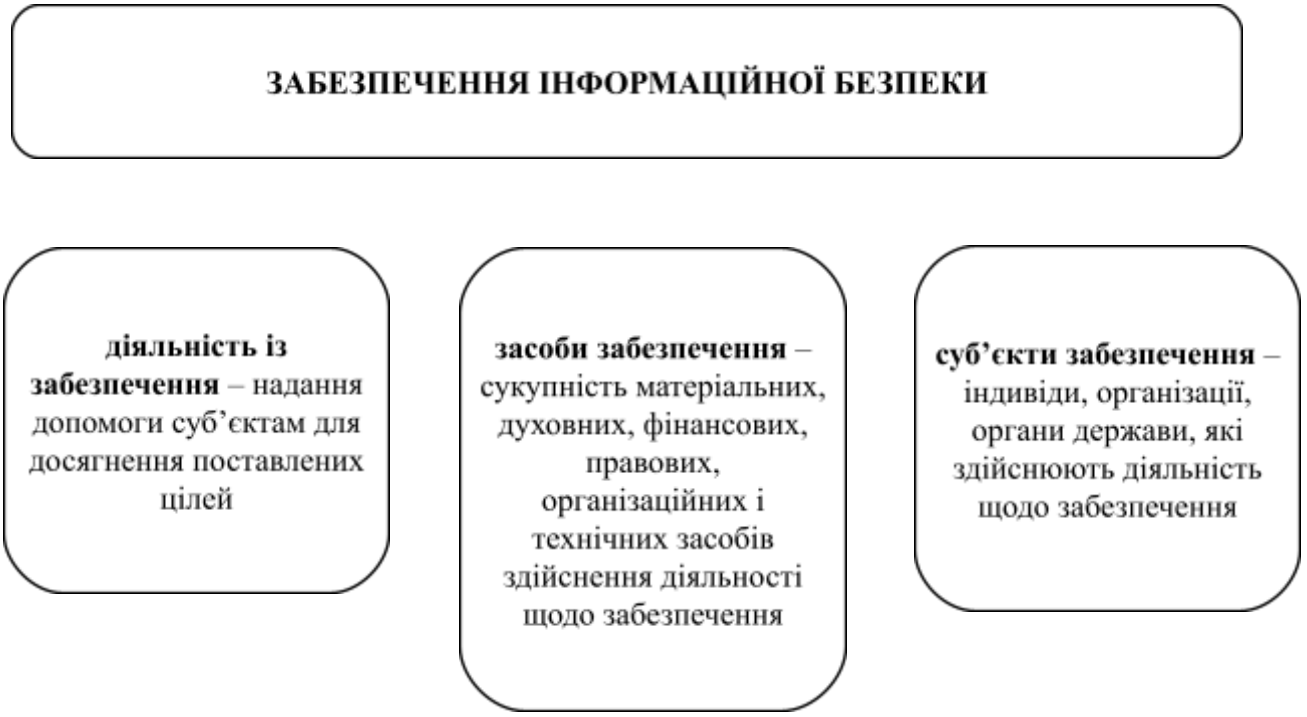



Рисунок 1.1. Структура забезпечення інформаційної безпеки.

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;

– суб’єкти забезпечення – сукупність матеріальних, духовних, фінансових, правових, організаційних і технічних засобів здійснення діяльності щодо забезпечення діяльність із забезпечення/надання допомоги суб’єктам для досягнення поставлених цілей - захист 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).

### *1.2 Принципи, форми та методи забезпечення інформаційної безпеки держави*.

*Принципи забезпечення інформаційної безпеки* - є вихідними положеннями, нормами і правилами поведінки, які диктують усім суб’єктам правила поведінки. Комплекс принципів у даному випадку представляє собою вихідні положення, норми і правила поведінки,

спрямовані на формування і забезпечення функціонування системи забезпечення інформаційної безпеки.

Зважаючи на те, що процес удосконалення системи забезпечення інформаційної безпеки триває, найбільш прийнятним підходом буде систематизація принципів окремо правових і окремо організаційних. Це сприятиме вдосконаленню як правової бази забезпечення інформаційної безпеки, так і системи його організаційного забезпечення.

*До правових принципів забезпечення інформаційної безпеки* доцільно включення наступних: законності; пріоритету норм міжнародного права над національним законодавством; права власності; економічної доцільності.

*Принцип законності* полягає у застосуванні механізмів забезпечення інформаційної безпеки та механізмів і технологій управління системою забезпечення інформаційної безпеки тільки на основі чинного законодавства та нормативно-правової бази регулювання як суспільних інформаційних відносин, так і міжнародного інформаційного співробітництва.

Незважаючи на те, що вказані права і свободи стосовно інформаційної діяльності захищаються Законом, у тому числі правовими санкціями Кримінального кодексу України (ст. 177, 229, 231, 232, 330 тощо), у зв'язку з відсутністю необхідного комплексу механізмів захисту цих прав і свобод вони можуть бути і порушені. Причиною цього може бути те, що права і свободи інформаційної діяльності не корелюються з системою експортного контролю за зовнішньоекономічними операціями щодо товарів, технологій і послуг, що підлягають експортному контролю.

*Принцип пріоритету норм міжнародного права над національним законодавством*, за винятком Конституції України, в системі забезпечення інформаційної безпеки полягатиме в прямій дії загальновизнаних принципів і норм міжнародного права, міжнародних договорів на всій території країни на рівні Конституції України.

Легітимність обмежень на поширення інформації світовим співтовариством визначається тільки у випадках, коли такі обмеження і механізми забезпечення встановлені національними законами.

*Принцип економічної доцільності системи забезпечення інформаційної безпеки* полягає в оцінюванні секретності та конфіденційності як споживацьких властивостей і включення їх вартості, на підставі вимог законодавства, до загальної ціни виробленої продукції. Відповідно до чинного законодавства фінансування витрат на здійснення діяльності, пов'язаної з державною таємницею, в бюджетних установах і організаціях здійснюється за рахунок державного бюджету України, бюджету Автономної Республіки Крим та місцевих бюджетів. Кошти на зазначені витрати передбачаються у відповідних бюджетах окремим рядком.

*До організаційних принципів* забезпечення інформаційної безпеки можна віднести наступні: об'єктивності; наукового підходу до організації захисту інформації; комплексного підходу; безперервності забезпечення інформаційної безпеки; єдиноначальності; персональної відповідальності; централізовано-децентралізованого державного управління.

Практичне застосування організаційних принципів є основою, яка зв'язує в єдину систему всі інші елементи забезпечення інформаційної безпеки. Організаційні принципи зазнали значно менших змін ніж правові, що вони відображають за своєю цінністю загальні правила і підходи до забезпечення інформаційної безпеки і можуть застосовуватися будь-якою соціально-політичною та економічною системою.

*Принцип об'єктивності в системі забезпечення інформаційної безпеки* має надзвичайно важливе, визначальне значення. Тільки на основі об'єктивної оцінки реальних і потенційних загроз інформації і сфері її обігу, стану правового й організаційного забезпечення, а також реальних можливостей застосування матеріально-технічних, кадрових і фінансових ресурсів хоча б у мінімально необхідних і достатніх обсягах можна забезпечити

захист інформації та інформаційну безпеку або послабити дію загроз безпеці сфери її обігу.

*Принцип наукового підходу до організації забезпечення інформаційної безпеки* передбачає: як всебічне пізнання об'єктивних законів і закономірностей розвитку інформаційної сфери та механізмів їх практичної реалізації, так і наукове осмислення і юридичне закріплення на рівні законодавчих, нормативно-правових актів та інших державних рішень усього комплексу проблем, пов'язаних із формуванням, удосконаленням системи забезпечення інформаційної безпеки та управління цією системою.

Наукове осмислення існуючих проблем є основою для розробки і впровадження доцільних й ефективних механізмів регулювання суспільних відносин, пов'язаних із забезпеченням інформаційної безпеки та прав суб'єктів інформаційної діяльності як у середині країни.

*Принцип комплексного підходу до організації забезпечення інформаційної безпеки* передбачає створення органічно взаємозв'язаної сукупності сил, засобів і спеціальних методів, спрямованих на забезпечення безпеки інформації, що підлягає захисту та сфери її обігу. Для забезпечення реалізації цього принципу необхідне повне знання всіх компонентів об'єкта захисту, тобто його складових, до яких слід віднести наступні: інформаційні ресурси, що підлягають захисту, серед яких: відомості, віднесені до державної таємниці, до іншої інформації з обмеженим доступом та відкрита інформація, важлива для особи, суспільства, держави; сферу обігу інформаційних ресурсів, що підлягають захисту; інформаційно-телекомунікаційні системи, різних класів і призначення; громадян.

*Принцип безперервності забезпечення інформаційної безпеки* полягає у повсякденному (безперервному) застосуванні як загальних, так і спеціальних засобів і методів забезпечення інформаційної безпеки на всіх її етапах життєвого циклу. Так, Закон України «Про інформацію», гарантує право на інформацію, орієнтує на добування, придбання, накопичення, користування і поширення інформації. І передбачає необхідність впровадження активних, превентивних, ефективних і різноманітних заходів і спеціальних методів; забезпечує безпеку інформації і сфери її обігу у просторі і часі від реальних і потенційних загроз як у звичайних, так і в екстремальних умовах.

*Форми забезпечення інформаційної безпеки* утворюють власне інструмент, з допомогою якого сили інформаційної безпеки вирішують весь комплекс завдань із захисту життєво важливих інтересів особистості, суспільства та держави. Тому необхідне чітке юридичне оформлення під час розробки нормативних актів, які регулюють діяльність органів інформаційної безпеки.

*Інформаційний патронат* – форма забезпечення інформаційної безпеки фізичних і юридичних осіб з боку держави. Він припускає забезпечення органів управління системи інформаційної безпеки держави відомостями про дестабілізуючі фактори і загрози стану інформованості фізичних і юридичних осіб (інформаційне забезпечення інформаційної безпеки) і, власне, захист життєво важливих інтересів цих осіб від інформаційних загроз або, як ще кажуть, – інформаційний захист. При цьому інформаційне забезпечення інформаційної безпеки включає збирання (добування) відомостей про дестабілізуючі фактори та інформаційні загрози, їхню обробку, обмін інформацією між органами керування і силами та засобами системи інформаційної безпеки. Його основу складає збирання (добування) необхідних відомостей, здійснюване в процесі розвідувальної, контррозвідувальної, оперативно-розшукової і оперативно-інформаційної діяльності.

*Інформаційний захист* досягається шляхом внесення в порядок законодавчої ініціативи законопроектів, здійснення судового захисту проведення оперативних заходів силами і засобами інформаційної безпеки.

*Інформаційна кооперація* – це форма забезпечення інформаційної безпеки між

рівноправними суб'єктами інформаційного процесу (фізичними, юридичними, міжнародними), який включає сукупність їхніх взаємоузгоджених дій, спрямованих на одержання відомостей про дестабілізуючі фактори, дестабілізуючі й інформаційні загрози та захист від них доступними законними способами і засобами.

*Загальні методи забезпечення інформаційної безпеки* можна поділити на правові, організаційно-технічні й економічні.

*До правових методів забезпечення інформаційної безпеки* належать розробка нормативних правових актів, що регламентують відносини у інформаційній сфері, і нормативних методичних документів із питань забезпечення інформаційної безпеки.

*Організаційно-технічними методами забезпечення інформаційної безпеки є:* створення й удосконалення системи забезпечення інформаційної безпеки; розробка, використання й удосконалення засобів захисту інформації і методів контролю ефективності цих засобів, розвиток захищених телекомунікаційних систем, підвищення надійності спеціального програмного забезпечення; створення систем і засобів запобігання несанкціонованому доступу до інформації, що обробляється, і спеціальним впливам, які призводять до руйнування, знищення, спотворення інформації, а також зміна штатних режимів функціонування систем і засобів та зв'язку тощо.

*Економічні методи забезпечення інформаційної безпеки містять:* розробку програм забезпечення інформаційної безпеки України і визначення порядку їх фінансування; удосконалення системи фінансування робіт із реалізації правових і організаційно-технічних методів захисту інформації, створення системи страхування інформаційних ризиків фізичних і юридичних осіб.

Отже, завданням державного управління в сфері інформаційної безпеки є створення відповідних правових, організаційних, науково-технічних, економічних, фінансових, методичних та гуманітарних засад регулювання процесу.

### *1.3 Інформаційна безпека: її роль та місце в системі національної безпеки України.*

Ч. 1 ст. 17 Конституції України чітко передбачено, що: «захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу».

Правові засади забезпечення національної безпеки України регулюються Законом України «Про національну безпеку України» від 21 червня 2018 р., який визначає дефінітивну конструкцію у сфері національної безпеки.

Згідно з п. 9 ч. 1 ст. 1 Закону України «Про національну безпеку України» під національною безпекою України розуміється: «захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз».

При цьому в п. 6 ч. 1 ст. 1 даного Закону дається визначення загрозам національної безпеки України, а саме: «явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України». Оскільки національна безпека є складною системою, вона має численні підсистеми, елементи та компоненти.

Основними елементами національної безпеки є політична, економічна, інформаційна, воєнна, соціальна, екологічна, інноваційна, науково-технічна безпека. Враховуючи бурхливий розвиток інформаційно-комунікаційних технологій, повну комп'ютеризацію, створення глобального інформаційного простору, сформувалися принципово нові першооснови – інформаційне суспільство, кіберпростір, які мають необмежений потенціал і значний вплив на політичну, економічну, соціальну і культурний розвиток держави.

Власне створення інформаційного суспільства спричинило появу багатьох кіберзагроз у важливих сферах життєдіяльності суспільства (банківська, військова, критична

інфраструктура тощо), для яких держави справедливо відносять інформаційну безпеку як самостійний елемент національної безпеки до національно ї безпеки.

Глобалізація сучасного інформаційного простору призводить до послаблення інформаційного суверенітету держави, а рівень розвитку та безпеки інформаційного простору впливає на стан безпеки будь-якої держави загалом.

Якщо звернутися до Доктрини інформаційної безпеки України, в якій під інформаційною безпекою України розуміється стан захищеності її національних інтересів в інформаційній сфері, що визначаються сукупністю збалансованих інтересів особи, суспільства та держави, то можна узагальнити, що основним напрямком політики держави стосовно забезпечення інформаційної безпеки є додержання конституційних прав і свобод людини в інформаційній сфері. Метою доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу рф в умовах розв'язаної нею гібридної війни. Доктрина визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями, пріоритети державної політики в цій сфері.

Інформаційна безпека –це складне, системне та багаторівневе явище, на стан і перспективи розвитку якого безпосередньо впливають зовнішні та внутрішні фактори, найважливішими з яких є: 1) політична ситуація у світі; 2) наявність потенційних зовнішніх і внутрішніх загроз; 3) стан і рівень розвитку інформації та зв'язку в країні; 4) внутрішньополітична ситуація в державі.

Забезпечення інформаційної безпеки завдяки послідовній реалізації чітко сформульованої національної інформаційної стратегії може суттєво сприяти забезпеченню успіху у вирішенні завдань у політичній, військово-політичній, військовій, соціальній, економічній та інших сферах діяльності держави. Так, реалізація успішної інформаційної політики може істотно впливати на вирішення внутрішньополітичних, зовнішньополітичних і військових конфліктів. Важливим компонентом війни є вторгнення в інформаційно-комунікаційний простір певної держави задля придушення опору та формування глобального політичного стандарту, який відповідає інтересам агресора.

Для цього використовуються найрізноманітніші засоби маніпулювання громадською думкою: втручання в роботу інформаційно-телекомунікаційних систем і мереж; розвиток кіберзлочинності; вплив у ЗМІ та маніпулювання громадською думкою.

Варто також зосередитись на тому, що Стратегія національної безпеки України визначає сучасні загрози національній безпеці України в інформаційній сфері як ведення інформаційної війни проти України та відсутність цілісної комунікаційної політики держави, недостатній рівень медіакультурності суспільства.

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.

Відтак, інформаційна безпека є важливою сферою забезпечення національної безпеки, яка характеризує стан захищеності національних інтересів в інформаційній просторі від зовнішніх та внутрішніх загроз у формі несанкціонованого вторгнення в інформаційні системи та атак на критично важливі інфраструктури. Це сукупність правових заходів що забезпечують збереження і цілісність інформації та нормативно-правовий порядок доступу до неї.

Система державної інформаційної безпеки є невід'ємною частиною загальної системи національної безпеки держави і являє собою сукупність органів державної влади, недержавних структур і громадян, які повинні скоординовано здійснювати діяльність щодо забезпечення безпеки інформації на основі єдиних правових норм ефективно протистояти інформаційним загрозам у сучасних умовах. Саме діяльність органів державної влади має бути скерована на реалізацію конкретних завдань у цій сфері та об'єднана єдиним призначенням – забезпечення належних умов для реалізації завдань забезпечення інформаційної безпеки України.

### *1.4 Критерії визначення об'єктів інформаційної небезпеки та їх обґрунтування, їх ієрархія.*

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 (рис. 2).

Рис. 1.2. Об’єкти інформаційної безпеки

***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).

### *1.5 Основні завдання інформаційної безпеки.*

Інформаційна безпека – це багатогранна галузь діяльності, в якій успіх може принести тільки систематичний, комплексний підхід.

Основними задачами інформаційної безпеки є:

· забезпечення доступності інформації;
· забезпечення цілісності інформації;
· забезпечення конфіденційності інформації;
· забезпечення вірогідності інформації;
· забезпечення юридичної значимості інформації, представленої у вигляді електронного документа;
· забезпечення невідстежуваності дій користувача.

Доступність – це властивість інформаційного об’єкта щодо одержання його користувачем за прийнятний час.

Інформаційні системи створюються для отримання певних інформаційних послуг. Якщо з тих чи інших причин надати ці послуги користувачам стає неможливо, це, очевидно, завдає збитку всім суб’єктам інформаційних відносин. Тому, не протиставляючи доступність решті аспектів, ми виділяємо її як найважливіший елемент інформаційної безпеки.

Особливо яскраво основна роль доступності виявляється в різного роду системах управління виробництвом, транспортом тощо. Зовні менш драматичні, але також вельми неприємні наслідки – і матеріальні, і моральні – може мати тривала недоступність інформаційних послуг, якими користується велика кількість людей (продаж залізничних та

авіаквитків, банківські послуги тощо).

Цілісність – це властивість інформаційного об’єкта зберігати свою структуру і/або зміст у процесі передавання і зберігання.

Розрізняють цілісність статичну (тобто незмінність інформаційних об’єктів) і динамічну (стосується коректного виконання складних дій (транзакцій). Засоби контролю динамічної цілісності застосовуються, зокрема, при аналізі потоку фінансових повідомлень з метою виявлення крадіжки, переупорядковування або дублювання окремих повідомлень.

Цілісність є найважливішим аспектом ІБ в тих випадках, коли інформація служить “керівництвом до дії”. Рецептура ліків, зміст медичних процедур, набір і характеристики комплектуючих виробів, хід технологічного процесу – все це приклади інформації, порушення цілісності якої може призвести до небажаних наслідків. Неприємно і спотворення офіційної інформації, будь то текст закону або сторінка Web-сервера якої-небудь урядової організації.

Конфіденційність – це властивість інформації бути доступною тільки обмеженому колу користувачів інформаційної системи, в якій циркулює дана інформація.

Конфіденційність – найбільш опрацьований у нашій країні аспект інформаційної безпеки. На жаль, практична реалізація заходів щодо забезпечення конфіденційності сучасних інформаційних систем пов’язана із серйозними труднощами. По-перше, відомості про технічні канали витоку інформації є закритими, тому більшість користувачів позбавлено можливості мати уявлення про потенційні ризики. По-друге, на шляху призначеної для користувача криптографії, як основного засобу забезпечення конфіденційності, стоять численні законодавчі перепони і технічні проблеми.

Вірогідність – це властивість інформації, яка полягає у строгій приналежності об’єкту, що є її джерелом, або тому об’єкту, від якого ця інформація прийнята.

Юридична значимість – це властивість інформації, представленої у вигляді електронного документа, мати юридичну силу.

З цією метою суб’єкти, що мають потребу в підтвердженні юридичної значимості переданого повідомлення, домовляються про прийняття деяких атрибутів інформації, що описують її здатність бути юридично значимою. Дана властивість інформації особливо актуальна в системах електронних платежів, де здійснюється операція з пересилання коштів.

Невідстежуваність – це здатність користувача робити деякі дії в інформаційній системі непомітно для інших об'єктів.

Актуальність даної вимоги виникла завдяки появі таких понять, як електронні гроші та Internet-banking. Так, для авторизації доступу до електронної платіжної системи користувач повинен надати деякі відомості, що однозначно його ідентифікують. У процесі розвитку даних систем може з’явитися реальна небезпека, що, наприклад, усі платіжні операції будуть контролюватися, тим самим виникнуть умови для тотального стеження за користувачами інформаційних систем.

Існує кілька шляхів вирішення проблеми неможливості стеження:

заборона за допомогою законодавчих актів будь-якого тотального стеження за користувачами інформаційних систем;

застосування криптографічних методів для підтримки неможливості слідкування.

Інформаційна безпека може розглядатися не тільки стосовно деяких конфіденційних відомостей, але і стосовно здатності інформаційної системи виконувати задані функції.

Інформаційна безпека в рамках забезпечення працездатності ІС повинна забезпечувати захист від:

порушення функціонування інформаційної системи шляхом впливу на інформаційні канали, канали сигналізації, керування і віддаленого завантаження баз даних, комутаційного устаткування, системне і прикладне програмне забезпечення;

несанкціонованого доступу до інформаційних ресурсів і від намагань використання ресурсів мережі, що призводять до витоку даних, порушення цілісності мережі й інформації, зміни функціонування підсистем розподілу інформації, доступності баз даних;

руйнування засобів захисту, що вбудовуються, і зовнішніх засобів;

неправомірних дій користувачів і обслуговуючого персоналу мережі.

Пріоритети серед перерахованих задач інформаційної безпеки визначаються

індивідуально для кожної конкретної ІС і залежать від вимог, що висуваються безпосередньо до інформаційних систем.

Якщо повернутися до аналізу інтересів різних категорій суб'єктів інформаційних відносин, то майже для всіх, хто реально використовує ІС, на першому місці стоїть доступність. Практично не поступається їй за важливістю цілісність – який сенс в інформаційній послузі, якщо вона містить спотворені відомості?

З погляду державних структур захисні заходи в першу чергу покликані забезпечити конфіденційність, цілісність і доступність інформації.

Комерційним структурам, ймовірно, важливіше всього цілісність і доступність даних і послуг. На відміну від державних, комерційні організації більш відкриті і динамічні, тому ймовірні загрози для них відрізняються не тільки кількістю, але і якістю.

Для розв'язання задач забезпечення безпеки в інформаційних системах необхідно:

захистити інформацію під час її зберігання, оброблення і передавання мережею;

підтвердити дійсність об'єктів даних і користувачів (автентифікація сторін, що встановлюють зв'язок);

знайти і попередити порушення цілісності об'єктів даних;

захистити технічні пристрої і приміщення;

захистити конфіденційну інформацію від витоку і від вбудованих електронних пристроїв знімання інформації;

захистити програмні засоби від під'єднання програмних закладок і вірусів;

захистити від несанкціонованого доступу до інформаційного ресурсу і технічних засобів мережі, зокрема, до засобів керування, щоб запобігти зниженню рівня захищеності інформації і самої мережі в цілому;

організувати заходи, що спрямовані на забезпечення збереження конфіденційних даних.

Конкретна реалізація загальних принципів забезпечення інформаційної безпеки може полягати в організаційних або технічних заходах захисту інформації.

## ПИТАННЯ ДЛЯ САМОПЕРЕВІРКИ

1. Дайте визначення понять «інформація», «інформаційна безпека» і «забезпечення інформаційної безпеки держави».

2. Які підходи щодо визначення феномену інформаційної безпеки Ви знаєте?

3. Вкажіть принципи, охарактеризуйте форми та методи забезпечення інформаційної безпеки держави.

4. Визначте роль та місце інформаційної безпеки в системі національної безпеки України.

5. Якими є критерії визначення об'єктів інформаційної небезпеки? Подайте їх ієрархію та обґрунтуйте.

6. Назвіть основні завдання інформаційної безпеки та аргументуйте свій вибір.

## МЕТОДИЧНІ РЕКОМЕНДАЦІЇ для опрацювання лекційного матеріалу

Опрацюйте лекційний матеріал та рекомендовані нижче додаткові джерела. При вивченні теоретичних питань належить зосередити увагу на з'ясуванні сутності сучасних підходів до визначення феномену інформаційної безпеки, уточненні категорійно-понятійного апарату. Слід також звернути увагу на роль та місце інформаційної безпеки в системі національної безпеки України, зокрема, з огляду на воєнний стан.

При опрацюванні матеріалу необхідно з'ясувати сутність кожного питання, що вивчається, не уникаючи при цьому визначення сутності основних термінів: «інформація», «інформаційна безпека», «забезпечення інформаційної безпеки держави», «принципи інформаційної безпеки», «суб'єкти інформаційної безпеки», «об'єкт інформаційної безпеки»,

«форми та методи інформаційної безпеки». Для з'ясування їх змісту можна скористатися словниками, довідниками, іншою науковою літературою.

При вивченні матеріалу за підручником, навчальним посібником, роботі із науковою і спеціальною літературою необхідно аналізувати прочитане із прослуханою та законспектованою лекцією, робити логічні висновки, відмічати основні сутнісні положення з метою їх подальшого з'ясування на відповідному практичному занятті.

# ЛЕКЦІЯ 2
# ТЕОРЕТИЧНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

**План викладу:**

2.1 Об'єктно-орієнтований підхід до інформаційної безпеки.
2.2 Сутність інформаційної безпеки держави, суспільства та особи.
2.3 Складові інформаційної безпеки: інформаційно-технічний та інформаційно-психологічний захист.
2.4 Стратегічні цілі у сфері інформаційної безпеки України: стан та перспективи розвитку.

## *2.1 Об'єктно-орієнтований підхід до інформаційної безпеки*

У теперішній час інформаційна безпека є відносно замкнутою дисципліною, розвиток якої не завжди синхронізований із змінами в інших галузях інформаційних технологій. Зокрема, в інформаційній безпеці поки не знайшли віддзеркалення основні положення об'єктно-орієнтованого підходу, що став основою для побудови сучасних інформаційних систем. Спроби створення великих систем ще в 60-х роках минулого століття розкрили численні проблеми програмування, головна з яких є складність створюваних і супроводжуваних систем. Результатами досліджень у галузі технології програмування стали спочатку структуроване програмування, потім об'єктно-орієнтований підхід.

*Об'єктно-орієнтований підхід* є основою сучасної технології програмування, випробуваним методом боротьби зі складністю систем. Складність має двояку природу. По-перше, складні не тільки апаратно-програмні системи, які необхідно захищати, але і самі засоби безпеки. По-друге, швидко зростає складність сімейства нормативних документів, таких, наприклад, як профілі захисту на основі «загальних критеріїв», мова про які попереду. Ця складність менш очевидна, але нею також не можна нехтувати – необхідно спочатку будувати сімейства документів за об'єктним принципом.

Будь-який розумний метод боротьби зі складністю спирається на принцип «Divide et impera» – «розділяй і володарюй». У даному контексті цей принцип означає, що складна система інформаційної безпеки на верхньому рівні повинна складатися з невеликої кількості відносно незалежних компонентів. Потім декомпозиції піддаються виділені на першому етапі компоненти, і так далі – до заданого рівня деталізації. Результатом є система у вигляді ієрархії з декількома рівнями абстракції.

Об'єктно-орієнтований підхід використовує об'єктну декомпозицію, тобто, поведінка системи описується в термінах взаємодії об'єктів.

Об'єкти реального світу володіють, як правило, декількома відносно незалежними характеристиками. Стосовно об'єктної моделі такі характеристики називаються гранями. Зазначимо, що три основні грані інформаційної безпеки – доступністю, цілісністю і конфіденційністю.

Поняття рівня деталізації важливе не тільки для візуалізації об'єктів, але і для систематичного розгляду складних систем, представлених в ієрархічному вигляді. Покажемо яким чином можна застосувати об'єктно-орієнтований підхід до питань інформаційної безпеки. Фактично три грані інформаційної безпеки вже було введено: це доступність, цілісність і конфіденційність. Їх можна розглядати відносно незалежно, і вважається, що якщо всі вони забезпечені, то забезпечена і інформаційна безпека у цілому.

Таким чином, ми структурували нашу мету. Тепер потрібно структурувати засоби її досягнення. Введемо такі грані:

– законодавчі заходи забезпечення інформаційної безпеки;
– адміністративні заходи (накази та інші дії керівництва організацій, пов'язаних з інформаційними системами, що захищаються);

– організаційні (процедурні) заходи (заходи безпеки, орієнтовані на людей);
– інженерно-технічні заходи.

Виходячи з цього, маємо таке поняття.

*Захист інформації* – це комплекс заходів, спрямованих на забезпечення інформаційної безпеки.

Далі кожна з виділених граней буде розглядатися детальніше. Тут же відзначимо, що, в принципі, їх можна розглядати і як результат варіювання рівня деталізації. Тому в подальшому будуть вживатися словосполучення «законодавчий рівень», «адміністративний рівень» і т.п.).

Закони і нормативні акти орієнтовані на всіх суб'єктів інформаційних відносин незалежно від їх організаційної приналежності (це можуть бути як юридичні, так і фізичні особи) в межах країни, адміністративні заходи – на всіх суб'єктів у межах організації, процедурні – на окремих людей (або невеликі категорії суб'єктів), інженерно-технічні – на устаткування і програмне забезпечення.

Продемонструємо тепер, як можна розглядати систему захисту ІС, варіюючи рівень деталізації.

Нехай інтереси суб'єктів інформаційних відносин концентруються навколо інформаційної системи певної організації, яка має у своєму розпорядженні два територіально рознесені виробничі майданчики, на кожному з яких є сервери, що обслуговують своїх і зовнішніх користувачів. Один з майданчиків обладнаний зовнішнім підключенням (тобто має вихід в Internet).

Нульовому рівню деталізації відповідає інформаційна система в цілому. Вже тут необхідно врахувати закони, застосовні до організацій, що мають в своєму розпорядженні інформаційні системи. Можливо, яку-небудь інформацію не можна зберігати і обробляти на комп'ютерах, якщо ІС не була атестована на відповідність певним вимогам.

На адміністративному рівні можуть декларуватися цілі, заради яких створювалася ІС, загальні правила закупівель, впровадження нових компонентів, експлуатації і т.п.

На процедурному рівні потрібно визначити вимоги до фізичної безпеки ІС і шляхи їх виконання, правила протипожежної безпеки тощо.

На інженерно-технічному рівні можуть бути визначені переважні апаратно-програмні платформи тощо.

На першому рівні деталізації визначаються сервіси і користувачі, або, інакше кажучи, здійснюється поділ на клієнтську і серверну частину (рис. 2.1).

Рисунок 2.1 – ІС при розгляді з рівнем деталізації 1

На цьому рівні потрібно сформулювати вимоги до сервісів (до їх наявності, до доступності, цілісності і конфіденційності інформаційних послуг, що надаються), викласти способи виконання цих вимог, визначити загальні правила поведінки користувачів, необхідний рівень їх попередньої підготовки, методи контролю їх поведінки, порядок

заохочення і покарання тощо. Можуть бути сформульовані вимоги і переваги щодо серверних і клієнтських платформ.

На другому рівні деталізації (рис.2.2) ще не описується внутрішня структура ІС організації і деталі Internet. Констатується тільки існування зв'язку між цими мережами, наявність в них користувачів, а також внутрішніх та зовнішніх сервісів без опису їхнього змісту.

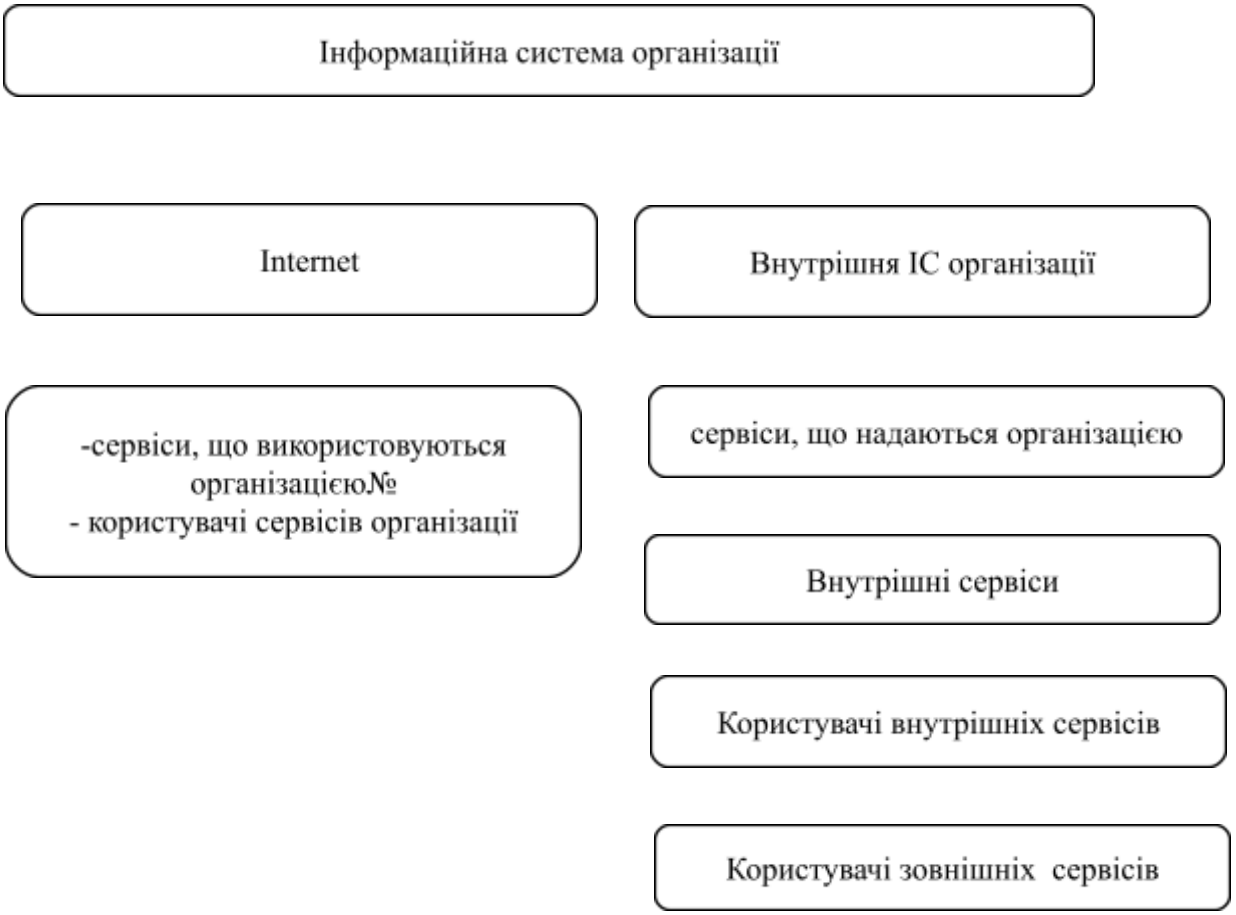



Рисунок 2.2 – ІС при розгляді з рівнем деталізації 2

Для рівня деталізації 2, повинні враховуватися закони, застосовні до організацій, ІС яких забезпечені зовнішніми підключеннями. Мова йде про допустимість такого підключення, про його захист, про відповідальність користувачів, що звертаються до зовнішніх сервісів, і про відповідальність організацій, що відкривають свої сервіси для зовнішнього доступу. Конкретизація аналогічної спрямованості, з урахуванням наявності зовнішнього підключення, повинна бути виконана на адміністративному, процедурному і інженерно-технічному рівнях.

### *2.2 Сутність інформаційної безпеки держави, суспільства та особи*

При розгляді питання про особливості інформаційної трансформації суспільства безумовним є той факт, що переважним ресурсом у всіх сферах життєдіяльності буде інформація. І як наслідок, очевидно, і те, що акцент у розвитку суспільства у найближчій перспективі буде зроблено на технологіях обробки та передачі величезних обсягів інформації.

Подібна тенденція виразно проявляється і в даний час. Причому акторами, зацікавленими у розвитку даного сектора, є не тільки численні бізнес-структури, які активно застосовують і стимулюють різноманітні нововведення в даній галузі, щоб завоювати перевагу в конкурентній боротьбі та «поділити» зростаючий перспективний ринок, а й державні структури, для яких ситуація впритул наближається до питання національної

безпеки. Проте, тут виникає проблема, не характерна для попереднього, індустріального етапу розвитку суспільства, - проблеми контролю інформації, забезпечення доступу до неї, тобто, «інформаційної безпеки».

Слід зазначити, що коло питань, які підпадають під розряд цієї характеристики інформаційного суспільства, досить широке. Крім основної складової захисту інформації, що передбачається при розмові про інформаційну безпеку (запобігання несанкціонованому доступу до інформаційних ресурсів та забезпечення збереження інформації), сюди можна також віднести і забезпечення доступності інформації, і перевірку її достовірності, організацію ефективних і доцільних способів передачі інформації, деякі інші.

Як відокремлена складова інформаційної безпеки, якій необхідно надати особливого значення, ми виділяємо таку властивість, як *оперування інформаційним контекстом*. Зазначена характеристика може бути розглянута у двох варіаціях: з одного боку, захист від небажаної інформації широких верств населення або окремих груп осіб (іншими словами, йдеться про своєрідну цензуру); з іншого боку, цілеспрямованого «вливання» (вкидання) інформації або управління інформаційними потоками (підганяння інформації, її вибіркове висвітлення або навіть фальсифікація) з метою реалізації будь-яких інтересів. Причому вищезазначені аспекти такої характеристики, як інформаційна безпека, можуть бути розглянуті на будь-якому рівні соціологічного аналізу, а в якості суб'єкта, носія даної характеристики, можна назвати і державу, і особистість, і окремі бізнес-структури, соціальні інститути, і навіть суспільство.

Для держави всі питання звернення інформації набувають категоричної значущості. Це зумовлюється тим, що в умовах інформаційного суспільства інформація - це, перш за все, стратегічний ресурс, що опосередковує (визначає) функціонування будь-якої сфери суспільства, отже, спроможність держави залежить від забезпечення «інформаційної безпеки». Цей стратегічний ресурс диференційований з різних соціальних сфер:

1. *Економічна сфера*. Характерною рисою сучасної економіки є не тільки рівень фактичного виробництва (виробітку кількості товару), скільки престиж державної економіки на світовій арені, довіра до економічних інститутів усередині країни та їх вплив на інститути економіки зовні. Свого роду маркетинг, об'єктом якого виступає не якийсь продукт, а держава, точніше державна економіка чи бренд.

2. *Сфера міжнародної політики*. Сучасні міжнародні відносини від фізичного (збройного) протистояння перейшли до розряду інформаційної боротьби, де чільну роль набуває дипломатія та ЗМІ. Символічно це можна уявити так: вирішення міжнародних конфліктів переважно перемістилося від поля бою до кабінетів.

3. *Засоби масової інформації*. Ця галузь також стала невід'ємним атрибутом міжнародної політики. Використання ЗМІ спрямоване як на формування правильного (вигідного) погляду світової громадськості з будь-якого питання, так й прямого тиску на деякі політичні інститути.

4. *Сфера внутрішньої політики*. Так, основним засобом легітимації влади переважної більшості розвинутих країн є її виборність. Саме процедура обрання, з її рейтингами окремих лідерів чи політичних партій – плацдарм для інформаційної боротьби у чистому вигляді. Є й інший бік процесу управління державою: інформація, будучи визначальним агентом функціонування суспільства, здатна значно впливати на соціальні інститути та населення, змінюючи, тим самим, траєкторію розвитку політичної ситуації загалом. Прецедент такого роду ми можемо зобразити на застосуванні подій в Україні через військову агресію з боку Росії, де явно відзначаються ознаки інформаційного впливу на маси, разом із засобами масової інформації.

5. *Оборонна сфера*. Ставши високотехнологічним споживачем наукової галузі

безпосередньо залежить від контролю за інформаційними потоками. Доступ (як фізичний, так й інформаційний) до новинок у галузі «hi – tech» та інших складових оборонної промисловості має бути суворо обмежений, оскільки це є питанням національної безпеки. Оборонна галузь найчастіше використовується як гарант економічної спроможності держави і як опора при введенні політики на різних рівнях.

Також очевидним є той факт, що перелічені сфери життєдіяльності будь-якої держави перебувають у взаємозв'язку один з одним, отже, даний об'єкт потребує аналізу з позицій структурно-функціонального підходу. Резюмуючи, зазначимо, що проблеми в одній сфері інформаційної безпеки здатні завдати шкоди всій системі. З одного боку, перелічені аспекти, пов'язані зі зверненням інформації у різних сферах суспільства, були характерні й для індустріального етапу. Але з іншого боку, ситуація для інформаційної епохи принципово відмінна у зв'язку з тим, що ці галузі набули статусу публічної сфери, де будь-які події підлягають розголосу через офіційні джерела та ЗМІ, володіючи при цьому підвищеною соціальною значимістю. Додатковим фактором, що посилює вплив інформаційних потоків на різні сфери суспільства, є багаторазове ускладнення засобів комунікації, що робить оборотність інформації та площу, що покривається нею, граничними.

Таким чином, підсумуємо: вкрай висока швидкість передачі інформації, її повсюдність і нелімітованість (повністю обмежити розповсюдження будь-якої інформації, за винятком приватних ситуацій, практично неможливо), разом з категоричною соціальною значимістю робить інформацію найважливішим соціальним ресурсом інформаційного суспільства.

Як наслідок, контроль над інформаційними потоками представляє можливість значного впливу на різні сфери суспільства, окремі соціальні інститути та всю систему.

Ще одним істотним моментом, що стосується інформації як основного ресурсу інформаційного суспільства, є *інформаційна безпека особистості*. З урахуванням того, що крім фізичних і психічних особливостей, властивих будь-якому індивіду, особистість набуває і віртуальну характеристику, що є масивом різнорідної інформації про будь-яку особу, оперування даною персональною інформацією стає соціально значущою потребою для громадян інформаційного суспільства.

Інформаційне поле надає вичерпну інформацію про індивіда: це сфера діяльності, професія, друзі, галузь інтересів, хобі тощо. Крім цього можуть бути зафіксовані окремі факти біографії, фото-, відео-матеріали за участю індивіда, висловлювання, у тому числі щодо соціально-економічних і політичних питань, на підставі яких можна скласти ціннісну модель і виявити основні поведінкові установки.

Також в інформаційному масиві найчастіше містяться конфіденційні дані: місце проживання, контактні телефони, номери банківських рахунків та пластикових карток, паспортні дані тощо.

Таким чином, персональна сполученість з інформаційним полем і навіть залежність від нього характерні для будь-якої особистості, соціалізованої за допомогою культури суспільства інформаційної доби. Якщо інформаційна безпека в глобальному масштабі і на рівні окремих держав є предметом професійної роботи спеціалізованих управлінь і відомств, то особиста інформаційна безпека - це перспективний напрямок майбутнього.

Ця сфера діяльності теоретично повинна буде надавати цілий спектр послуг, подібно до «створення сприятливого особистісного образу в інформаційному полі» або «зачистки персонального іміджу від фактів біографії, що ганьблять». Негативною стороною поняття «особистість в інформаційному просторі» є можливість реалізації сценаріїв, характерних для антиутопії Джорджа Оруелла «1984»): тотальний контроль держави над особистістю.

Цікавим прикладом у даному випадку буде досвід Китаю, оскільки діджиталізація (точніше навіть роботизація) взагалі життя громадян, має високий рівень впровадження та

забезпечення системи контролю. Відтак, у цій країні система контролю здійснює інтегрування різних джерел інформації, а саме: адреси мешкання людей, їх сімейні відносини, відповідний контроль народжуваності тощо. Також у цій країні використовується програма, що дозволяє виявляти осіб завдяки спеціальним аналітичним та прогнозним моделям. Зазначена програма автоматично проводить розпізнавання осіб, вона стежить і аналізує їхні дії, наприклад, якщо людина купила ніж, або мотузку і мішок, вона відповідно потрапить до числа осіб, які ведуть підозрілу діяльність. У зв'язку з цим цікаво відмітити, що по всьому Китаю розміщено 176 млн відеокамер спостереження. Для впровадження зазначеного проекту було розміщено відеокамери, що дозволяють розпізнавати людей, розроблено різноманітні мобільні додатки, платіжні системи, інтернет-платформи, відповідні бази дорожніх, соціальних та комунальних служб, об'єднані у спеціальній єдиній інформаційній системі. Це дозволяє відзначити, що у країні здійснюється тотальний контроль над населенням.

Зазначене припущення також підтверджується тим, що з січня 2021 року набула чинності відповідна система «соціального кредиту», яка передбачає при цьому, що кожна людина має певний рейтинг на старті свого життя, а потім отримує бали або у неї їх забирають залежно від її дій. Отже, кількість балів, які людина накопичила за певний період часу, відкриває їй доступ до різних сервісів. Фахівці вказують, що такий масштабний проект спрямований на побудову ідеального суспільства (будь-яка дія людини враховується та оцінюється) і відповідно формує право слухняність, надійні та ввічливі взаємини між людьми.

Передбачуваний рейтинг будуватиметься на певних сферах життя: 1) державній (податки, рахунки, погашення кредитів тощо); 2) суспільній (норми народжуваності, робота, освіта, прояв чесності у зазначеній сфері, дотримання правил дорожнього руху); 3) поведінці у мережі (культура спілкування з користувачами, надійність інформації, яку людина розміщує, покупки, що здійснюються в інтернет-магазинах тощо). Аналіз зазначеної інформації дозволяє програмі сформувати певні бали кожної людини.

Цим розширеним поясненням особливостей китайської інформатизації підкреслимо, що європейські країни тримають вектор на забезпечення прав громадян на приватне життя, захист персональних даних осіб. Вважаємо, що це пов'язано із патернами вільного життя європейців, лише можна нагадати громадські хвилювання: під час впровадження мобільного додатку, який стежив за фізичними особами та повідомляв, якщо вони мали будь-який контакт з Covid-інфікованим у Чеській Республіці; через передачу повноважень щодо розробки державної платформи з надання публічних послуг у Швейцарії на користь приватних компаній; та інші.

Адже, сьогодні при цьому реалізація зазначених віще завдань абсолютно не обов'язково пов'язана з відкритою формою контролю за населенням, існує велика кількість технічних і технологічних можливостей для впливу на латентному рівні. Ми можемо виділити лише деякі з таких прикладів: точкове усунення невигідної або дискредитуючої інформації для заінтересованих сторін; поширення власної інтерпретації подій, спотворення інформації, з метою сформувати «правильне» розуміння в окремих групах чи у населення загалом; вкидання дезінформації чи компромату, з метою підриву авторитету окремих політичних сил чи персоналій тощо.

### *3. Складові інформаційної безпеки: інформаційно-технічний та інформаційно-психологічний захист*

У зв'язку з широкою інформатизацією основних сторін життєдіяльності інформаційна сфера стала важливою частиною суспільної життя, багато в чому визначального напряму соціально-політичного та економічного розвитку країни.

*Інформаційна сфера* – сфера діяльності суб'єктів суспільного життя, пов'язана зі

створенням, збором, перетворенням, зберіганням, поширенням та використанням інформації, можна розділити на дві складові: інформаційно-технічну сферу та інформаційно-психологічну сферу.

*Інформаційно-технічна сфера* пов'язана з інформаційним забезпеченням усіх сторін життєдіяльності особистості, суспільства та держави за допомогою використання інформаційних та телекомунікаційних систем.

*Інформаційно-психологічна сфера* утворюється сукупністю людей та інформації, якою вони обмінюються та яку сприймають, суспільних відносин, що виникають у зв'язку з інформаційним обміном та інформаційно-психологічними впливами на людину. Цим двом складовим інформаційної сфери відповідають два види інформаційної безпеки: *інформаційно-технічна безпека та інформаційно-психологічна безпека*.

Під *інформаційно-психологічною безпекою* розуміємо захищеність громадян, окремих груп та соціальних верств, об'єднань людей та населення країни в цілому від негативних інформаційно-психологічних впливів.

В основі пошуку конструктивних рішень у галузі захисту від негативних інформаційно-психологічних впливів має лежати відповідне концептуальне та науково-методичне забезпечення.

До базових понять у цій галузі слід віднести такі як інформація, індивід, особистість, психіка, свідомість (індивідуальна, групова, масова, суспільна), підсвідомість, інформаційно-психологічний та психофізичний вплив, загроза інформаційно-психологічної безпеки та інші.

1. *Людина як соціально-біологічна цілісність.* В даний час людина - філогенетично сформований вид, «людина розумна» (Homo sapiens) – розуміється як певна цілісність, обумовлена єдністю біологічного та соціального. Біологічна складова – індивід (лат. individuum – неподільне, особа) є сукупністю природних, генетично обумовлених властивостей, що розвиваються від зародження до закінчення життя.

Соціальна складова – особистості – носій властивостей, що визначають соціальну природу людини, її свідому діяльність. Особистість проходить свій життєвий шлях, здійснюється її соціалізація, тобто, оволодіння в процесі взаємодії з соціальним середовищем певною системою знань, механізмами соціальної поведінки та засвоєння її норм. Соціалізація включає як цілеспрямований вплив на особистість (виховання), так і стихійні, спонтанні процеси, що впливають на її формування. Особистість характеризується властивою їй смисловою структурою (характером, інтересами, системою поглядів, ціннісних установок, переваг і т.п.), що розкривається в її діях та вчинках.

Соціальні, (у широкому сенсі слова), психологічні риси та властивості людини разом із біологічними якостями та є його компонентами як цілісної системи. При цьому сукупність індивідуальних та особистісних властивостей у кожного окремої людини, що утворюється у розвитку, неповторна і складає суть індивідуальності людини. Людська індивідуальність реалізується в людині як суб'єкт діяльності (праці, пізнання, спілкування), тобто, у процесі активного ставлення людини до дійсності, в ході якого відбувається досягнення суб'єктом поставлених раніше цілей, задоволення різноманітних потреб та освоєння суспільного досвіду.

Будь-яка спільнота людей, кожна група виробляє свою власну систему поглядів світу, свою картину світу. З одного боку формування цієї системи підпорядковане загальним закономірностям, з іншого – воно відбиває специфіку реальної життєвої практики цієї групи. Правила побудови людиною своєї поведінки відповідає існуючим у даному співтоваристві або групі стандартів. При цьому поведінку можна визначити як цілісну активність людини, спрямовану на задоволення біологічних, фізіологічних, психологічних та соціальних потреб.

*2. Інформація та її сприйняття людиною.* Наше століття називають віком інформатики. Цим підкреслюється, що не лише організація всього життя у наші дні, але й сама життєздатність сучасного суспільства залежить від його інформаційного забезпечення. Втручаючись у регулювання інформаційних потоків, впливаючи на хід обробки та споживання інформації, можна впливати на ті чи інші події та процеси, що відбуваються у суспільному житті.

Інформаційно-психологічну безпеку можна розглядати з позицій впливу інформаційної сфери на індивідуальну, масову та суспільну свідомість, що відображають ставлення громадян і суспільства до минулого, теперішнього та майбутнього. При цьому під впливом інформаційної сфери будемо розуміти найширше коло процесів, починаючи від формування чи руйнування тих чи інших моральних, ідеологічних та політичних цінностей, включаючи інформаційну політику держави, систему освіти, діяльність засобів масової інформації, події культурного життя, масових явищ, тощо.

Зазначимо, що обмін інформацією є фундаментальною властивістю організму людини, так само як обмін енергією та речовиною. В основі зачаття, розвитку та психофізіологічного формування організму людини лежать інформаційні процеси різних рівнів (космічні, планетарні, клітинні, молекулярні, квантові та ін.). Людина еволюційно сформувалась як дуже складна біоінформаційна система, в якій найбільшого розвитку отримав процес переробки інформації через механізм центральної нервової системи.

Прийом та переробку інформації в людському організмі здійснює нервова система через процес сприйняття подразнення рецепторами, тобто, через відчуття. Отримана людиною інформація у формі зорових, слухових та інших образів зберігається у його пам’яті.

*3. Психіка та психічні процеси.* Для виявлення найбільш важливих та загальних особливостей інформаційно-психологічних впливів на особистість, групову, масову та громадську свідомість необхідні, перш за все, знання такої людської сутності як психіка та закономірностей її функціонування.

Дослідженнями науковців встановлено, що приблизно 97% психічної діяльності людини протікає лише на рівні підсвідомості і лише 3% - в усвідомленому стані. Останні дослідження нейрофізіологів показують, що наша оперативна пам’ять, що формує наш «здоровий глузд», – це лише мала частина нашої «сумарної» пам’яті, яку має людина. Головний її резерв та «сховище» - підсвідомість. У ньому міститься від 70% до 99% обсягу пам’яті (всіх знань).

Вочевидь, при інформаційно-психологічному впливі на несвідомому рівні можна впливати на мотиви та зміст діяльності, програмувати поведінку на основі персональних стереотипів, а також активізувати сприйняття та творче мислення. Неусвідомлюваний інформаційно-психологічний вплив через підсвідомість становить особливу загрозу, тому що воно ніяк не проявляється та не реєструється свідомістю. Життєві (соціальні) установки у разі безперешкодного проникнення у свідомість, вносять спотворення в її діяльність, що в кінцевому підсумку позначається на поведінці людини.

Знаючи методи інформаційно-психологічного впливу на підсвідомість, ми зможемо вчасно усвідомити та розпізнати факт їх застосування Отже, зможемо грамотно фільтрувати потоки інформації, захистивши себе від негативного інформаційно-психологічного впливу.

*4. Групова, масова та суспільна свідомість*. До понятійного ряду, пов’язаного з терміном «свідомість» (маючи на увазі «індивідуальну свідомість»), також відносяться «групова свідомість», «масова свідомість» та «суспільна свідомість».

*Групова свідомість* - це вид свідомості суспільства, що відображає збіг поглядів, переконань, уявлень, інтересів, ціннісних орієнтацій для деякої обмеженої у розмірах спільності людей, що виділяється на основі певних ознак (характеру виконуваної діяльності,

соціальної чи класової приналежності, рівня розвитку, віку, тощо).

У колективі (групі) на людину впливає навколишнє середовище, формується загальний настрій. Відбувається це тому, що аж ніяк не кожна людина прагне виробити власну думку щодо кожного приводу: багато людей вважають за краще покладатися на міркування інших, засвоюють думки оточуючих так, якби вони були власними. Якщо таку думку поділяють багато хто, то набирає чинності «стадне почуття». Думки та особливо настрої оточуючих виявляються настільки заразливими, що людина діє як усі. Отже, групова свідомість – це спільні погляди, уявлення та почуття тих чи інших соціальних груп (класів, верств суспільства, професійних угруповань). При цьому групова свідомість однієї соціальної групи може суттєво відрізнятися від суспільної свідомості іншої. Наприклад, є відмінності в суспільній свідомості вікових верств населення, а також різних професійних груп.

*Масова свідомість* - специфічний вид свідомості суспільства, властивий значній неструктурованій масі людей, що відображає різні сторони життя суспільства, викликає інтерес масових спільностей. Основними різновидами маси, що зустрічаються на практиці, є: натовп; «зібрана публіка» – скупчення деякої кількості людей, які відчувають подібне очікування певних переживань або тих, хто цікавиться одним і тим ж предметом; «незбирана публіка», до якої відноситься частина електоральних мас, що виникають під впливом політичної реклами, маси шанувальників кумирів сучасної музики (є велика кількість людей, мислення та інтереси яких орієнтовані ідентичними стимулами одного напрямку), тощо. Люди можуть об’єднатися у масу стихійно, без сторонніх втручань, але такі об’єднання людей можуть створюватися і штучно з розрізнених людей, придатних для цього, і підтримуватись якийсь час сторонніми силами на користь цих сил.

Зазначимо, що масова свідомість характерна для нестабільних, тимчасових великих об’єднань людей, виникаючих як відображення, переживання та усвідомлення діючих обставин, у тому чи іншому відношенні загальних для членів різних соціальних груп, що виявляються тим самим у подібних життєвих умовах, та що зрівнюють їх у тому чи іншому плані.

Для того, щоб маніпулювати масовою свідомістю, бажано будь-яку масу спочатку перетворити на натовп, тобто, масу, що втратила організованість, позбавлену ясно усвідомленої спільності цілей та організації. Серед якостей індивідів, схильних до знаходження і в натовпі, необхідно відзначити зараження. В натовпі всяке почуття, всяка дія заразлива, і до того ж настільки, що індивід дуже легко приносить у жертву свої особисті інтереси інтересу колективному. Зникнення свідомої особистості та орієнтування почуттів та думок у певному напрямку –це основні риси, що характеризують натовп. Практично будь-який натовп згодом охоплює колективне збудження, в результаті якого учасники натовпу стають менш стійкі до будь-яких впливів. І як наслідок - зростання безвідповідальності, а значить та несвідоме бажання при здійсненні будь-яких вчинків більше керуватися емоціями та миттєвими бажаннями, ніж за принципами здорового тестування реальності. Крім того, підвищене емоційне збудження окремих індивідів по ланцюжку захоплює натовп загалом, якимось чудодійним чином вторгаючись у її енергетику. В результаті чого та наростає загальне колективне збудження.

*Під суспільною свідомістю* розуміється сукупність, що зачіпає спільні інтереси громадян поглядів, переконань, ідей, теорій, уявлень, вірувань, звичаїв та традицій, що склалися у суспільстві на цьому етапі історичного розвитку. Форми суспільної свідомості залежать від життя, улаштування соціальних інститутів, організації процесу пізнання тощо. Тому вони завжди тісно пов’язані з певного типу суспільними відносинами: економічними, політичними, моральними, естетичними, відносинами між членами наукової спільноти та ін. Суспільна свідомість є якісно особливою духовною системою, яка живе своїм самостійним

життям, розвивається та функціонує за своїми законами. Між індивідуальним та суспільною свідомістю відбувається постійна взаємодія. Кожен індивід протягом усього свого життя через відносини з іншими людьми, шляхом навчання та виховання відчуває вплив суспільної свідомості, хоч і належить до цього впливу не пасивно, а вибірково, активно.

*Громадська думка* формується під впливом усіх засобів масового інформаційно-психологічного впливу (телебачення, радіо, преса та ін.), хоча може виникати і стихійно, під впливом тих чи інших життєвих обставин та ситуацій. У формуванні індивідуальної, групової, масової та суспільної свідомості важливу роль грають життєві (соціальні, ідеологічні, політичні та інші) установки та стереотипи. Вони розглядаються як організована схильність особистості до певного сприйняття ситуації, її оцінці та наступних дій. Впливаючи певним чином (наприклад, за допомогою пропаганди) на формування життєвих установок та стереотипів людей, можна також впливати на формування групової, масової та суспільної свідомості.

*5. Впливи на психіку та свідомість людини*. Одне з базових понять інформаційно-психологічної безпеки – *інформаційно-психологічний вплив* може бути визначено як інформаційний вплив на психіку людини, що впливає на сприйняття ним реальної дійсності, у тому числі на його поведінкові функції, а також у деяких випадках на функціонування органів та систем організму людини. Інформаційно-психологічний вплив виступає як інтегруючий фактор, сприяє утворенню різних структур суспільства.

Будь-яка людина як особистість, активний соціальний суб’єкт, носій певного світогляду, який має певну правосвідомість та менталітет, з відповідними духовними ідеалами та ціннісними установками, можливо підданий безпосередньому інформаційно-психологічному впливу, який трансформуючись через його поведінку, дії (або бездіяльність), впливає на соціальні об’єкти різного рівня спільності, різної системно-структурної та функціональної організації.

Таким чином, за допомогою інформаційно-психологічного впливу можна впливати не лише на індивідуальну свідомість, а й на групову, масову та суспільну свідомість. Причому цей вплив може мати як позитивний, і негативний характер.

*Позитивний інформаційно-психологічний вплив* спрямований на активізацію психіки людини або спільноти людей з метою якнайшвидшого вирішення творчих проблем (єднання нації перед військовою загрозою, наснагу бійців перед боєм, боротьба зі стихійними лихами, подолання кризових ситуацій в економіці і т.д.).

*Негативний інформаційно-психологічний вплив* певною мірою корелюються також з маніпулятивними прийомами, спрямованими на програмування думок та устремлінь мас, їх настроїв і навіть психічний стан людей з метою забезпечення такої їхньої поведінки, яка потрібна тим, хто володіє засобами маніпуляції.

Залежно від переслідуваних цілей інформаційно-психологічний вплив, як правило, здійснюється на конкретні сфери індивідуальної, групової, масової та суспільної свідомості:

- мотиваційну (переконання, ціннісні орієнтації, потягу, бажання), коли треба надати вплив на людей до певних дій;

- пізнавальну (відчуття, сприйняття, уявлення, уява, пам’ять та мислення), коли необхідно змінити у потрібний бік уявлення, характер сприйняття нової інформації і, зрештою, «картину світу» людини;

- емоційну (емоції, почуття, настрої, вольові процеси), коли під прицілом знаходяться внутрішні переживання та вольова активність людей;

- комунікативну (взаємини, взаємодія, міжособистісне сприйняття) з метою створення соціально-психологічного комфорту або дискомфорту, спонукання людей співпрацювати або конфліктувати з оточуючими.

Інформаційно-психологічний вплив може здійснюватися за допомогою різних методів (прийомів, форм, методик) і засобів, більшість з яких, безперервно розвиваючись і вдосконалюючись, перетворилися сьогодні на складні технології впливу на психіку людей, а саме психотехнології.

Таким чином, поняття «негативний інформаційно-психологічний вплив», що є визначальним для інформаційно-психологічної безпеки, може бути сформульовано як інформаційно-психологічний вплив на людину, на групову, масову та суспільна свідомість з метою явного чи прихованого спонукання індивідуальних та соціальних суб'єктів до діям на шкоду власним інтересам інтересах окремих осіб, груп чи організацій, здійснюють цей вплив.

*Загроза інформаційно-психологічній безпеці людини* - це сукупність умов та факторів, що викликають деструктивний інформаційний вплив на психіку людей, який створює небезпеку її функціонування в певному місці та часі.

Джерелами загроз інформаційно-психологічній безпеці людини є природні, техногенні, соціальні фактори, розробка, створення та застосування спеціальних засобів, а також діяльність осіб, груп осіб, організацій, що негативно впливають на духовний, душевний та фізичний комфорт -руйнування єдиного інформаційного та духовного простору держави, її культури та традиційних устоїв суспільства та суспільної моралі.

Загрозою інформаційно-психологічній безпеці є монопольне володіння одним відомством силами та засобами впливу на психосферу людини та можливістю маніпулювання суспільною свідомістю.

Потенційними джерелами загроз інформаційно-психологічній безпеці є:

- фізичні особи, що мають від природи здатність неусвідомлюваного впливу на інших осіб та об'єднання цих осіб;
- релігійні та інші езотеричні та окультні групи та організації;
- будь-які програми для ЕОМ;
- генератори фізичних полів та випромінювань;
- природні комплекси та антропогенні зони;
- будь-які інформаційно-програмні та аудіо- відео продукти, що розповсюджуються каналами суспільного користування;
- література та засоби масової інформації, у тому числі такі, які використовують методи нейролінгвістичного програмування.

Основними загрозами інформаційно-психологічній безпеці можуть бути:

- руйнування єдиного інформаційного і духовного простору держави, традиційних устоїв суспільства і суспільної моралі;
- блокування на неусвідомлюваному рівні свободи волевиявлення людини, прищеплювання їй синдрому залежності;
- розроблення, створення і застосування спеціальних технічних і програмних засобів для деструктивного впливу на психіку людини;
- маніпуляція суспільною свідомістю з використанням засобів масової інформації та спеціальних засобів впливу;
- деструктивний вплив на психіку людини геопатогенних і антропогенних зон, генераторів фізичних полів та випромінювань.

### *2.4. Стратегічні цілі у сфері інформаційної безпеки України: стан та перспективи розвитку*

З метою адекватного реагування на поширення гібридних загроз в Україні наприкінці 2021 року на державному рівні була схвалена *Стратегія інформаційної безпеки* (затв. Указом Президента України від 28.12.2021 № 685/2021) як фундаментальний документ, який визначає

завдання та шляхи діяльності держави з метою недопущення кризових явищ у вітчизняному інформаційному просторі, посилення інформаційної безпеки та її складових. Очікується, що практичне впровадження цієї Стратегії має посилити можливості держави щодо забезпечення власної інформаційної безпеки, захисту інформаційного простору.

Основною загрозою безпеці України в цьому документі визначена Росія і проведена цією країною інформаційна політика. Стратегію планується реалізувати до 2025 року.

Метою цієї Стратегії є посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина.

Досягнення мети здійснюється шляхом ужиття заходів щодо стримування та протидії загрозам інформаційній безпеці України та нейтралізації інформаційної агресії, у тому числі спеціальних інформаційних операцій держави-агресора, спрямованих на підрив державного суверенітету, територіальної цілісності України, забезпечення інформаційної стійкості суспільства та держави, створення ефективної системи взаємодії між органами державної влади, органами місцевого самоврядування та суспільством, а також розвиток міжнародної співпраці у сфері інформаційної безпеки на засадах партнерства та взаємної підтримки.

Цим декларативним документом (Стратегія інформаційної безпеки) визначено важливих перспективних цілей.

*Перша* передбачає протидію дезінформації та інформаційним операціям, насамперед з боку держави-агресора, спрямованої проти України.

*Друга* – забезпечення всебічного розвитку української культури та утвердження української громадянської ідентичності.

*Третя* – підвищення рівня медіакультури та медіаграмотності суспільства.

*Четверта* – забезпечення дотримання прав особи на збір, зберігання, використання і поширення інформації, свободу вираження своїх поглядів і переконань, захист приватного життя, доступ до об’єктивної та достовірної інформації, а також забезпечення захисту прав журналістів.

*П’ята* – інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих територіях та на прилеглих до них територіях України, всеукраїнського інформаційного простору.

*Шоста* – розвиток інформаційного суспільства та підвищення рівня культури діалогу.

*Сьома* ціль – створення ефективної системи стратегічних комунікацій.

Отже, вказані цілі формують сфери, які потребують посилення контролю з боку держави, та є визначальними в контексті забезпечення інформаційної безпеки.

Таким чином, до переліку загроз та викликів, які стоять перед нашою державою, належать: повноформатна експансійна інформаційна політика РФ; досить низький рівень медіаграмотності громадян; динамічне збільшення кількості глобальних дезінформаційних кампаній; інформаційне домінування РФ на тимчасово окупованих територіях; використання технологій маніпулювання свідомістю пересічних громадян щодо наслідків вступу України в НАТО та ЄС тощо.

Зокрема планується, що успішна реалізація Стратегії інформаційної безпеки матиме такі позитивні наслідки, як: побудований захищений інформаційний простір, гарантування інформаційної безпеки держави та її складових; ефективне функціонування системи стратегічних комунікацій; запровадження механізмів ефективної протидії поширенню незаконного контенту тощо.

**ПИТАННЯ ДЛЯ САМОПЕРЕВІРКИ**

1. Охарактеризуйте сутність об’єктно-орієнтованого підходу до інформаційної безпеки.
2. Інформаційна безпека держави, суспільства та особи: ознаки, властивості, складові.
3. В яких соціальних сферах диференціюється інформаційна безпека як стратегічний ресурс держави?
4. На які конкретні сфери індивідуальної, групової, масової та суспільної свідомості здійснюється інформаційно-психологічний вплив? Від чого це залежить?
5. Вкажіть складові інформаційної безпеки та коротко їх охарактеризуйте.
6. Як Ви розумієте поняття «інформаційно-психологічної безпеки»? Обґрунтуйте свою відповідь.
7. Які потенційні джерела загроз інформаційно-психологічній безпеці людини Ви знаєте?
8. Охарактеризуйте загрози інформаційно-психологічній безпеці держави.

# ЛЕКЦІЯ 3
# ІНФОРМАЦІЯ ЯК ОБ'ЄКТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

**План викладу:**

3.1 Класифікація інформації. Види інформації як предмету захисту.
3.2 Критерії цінності інформації та стратегії комплексного захисту інформації та інформаційних ресурсів.
3.3 Режими доступу до інформації. Відповідальність за порушення законодавства до інформації.
3.4 Службова таємниця. Конфіденційна інформація. Комерційна таємниця. Професійна таємниця. Правові наслідки розголошення державної таємниці.
3.5 Персональні дані. Вимоги до обробки персональних даних.
3.6 Шляхи поширення недостовірної інформації та механізми протидії в умовах війни.

## *3.1 Класифікація інформації. Види інформації як предмету захисту.*

Закони України «Про інформацію» та «Про доступ до публічної інформації» 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. Вона 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* – це 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, проте 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 (ст. 6 Закону України «Про доступ до публічної інформації»):

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 перевищує 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.

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 законодавством, 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». 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.

### *3.2 Критерії цінності інформації та стратегії комплексного захисту інформації та інформаційних ресурсів.*

Документовані інформаційні ресурси – це інтелектуальна власність. Інтелектуальна власність складається з елементів – інформаційних продуктів (комерційно цінних ідей), реалізованих в інформаційному вигляді.

Інформаційний продукт (ІП) є результатом творчої праці певної організації (колективу

організації), що має конкретну цінність для власника.

Цінність інформаційного продукту можна визначити через: вартість (розмір прибутку при використанні, розмір збитків при втраті; правове значення для організації (установчі документи, програми та плани, договори з партнерами); перспективне наукове значення; техніко-технологічне значення.

Існують наступні види цінної інформації.

1. Технічна та технологічна: хімічна формула; рецепт; результат випробувань; дані контролю якості; методи виготовлення продукції; програмне забезпечення; виробничі показники.

2. Ділова: управлінські рішення; методи реалізації функцій; вартісні показники; результати дослідження ринку; списки клієнтів; економічні прогнози і т.д.

Основні напрямки формування цінної інформації (ЦІ) представлені в табл. 3.1

*Таблиця 3.1* Основні напрямки формування цінної інформації

| № | Область діяльності | Напрямки формування цінної інформації |
|---|---|---|
| 1. | Управління організацією | застосування нетрадиційних методів управління, порядок підготовки та прийняття рішення в областях діяльності |
| 2. | Прогнозування і планування | розширення або згорнення виробництва, очікуваний обсяг досліджень, програми розвитку, програми взаємодії з інофірмами, плани інвестицій, продаж, покупки |
| 3. | Фінансова діяльність | баланс, відомості про стан банківських рахунків, відомості про рівень прибутковості продукції, інформація про отримання кредитів, про колообіг фінансів, про виробничі операції, про боргові зобов'язання |
| 4. | Виробнича діяльність | виробничі потужності, тип обладнання, запаси сировини, матеріалів, комплектуючих, запаси готової продукції |
| 5. | Торговельна діяльність | інформація про ринкові стратегії, методи здійснення продажу, інформація про результати дослідження ринку, інформація про ефективність комерційної діяльності |
| 6. | Переговори і наради | за напрямками діяльності інформація щодо підготовки, змісту і результатів переговорів з посередниками і партнерами, про наради з персоналом |
| 7. | Формування цінової політики | структура ціни, очікувані ціни, методи оцінювання, розміри знижок |
| 8. | Формування складу клієнтів, компаньйонів, посередників, постачальників | відомості про зарубіжних і внутрішніх замовників, постачальників і користувачів |
| 9. | Вивчення напрямків інтересів конкурентів | методи аналітичної роботи, способи боротьби за ринок, результати маркетингових досліджень |
| 10. | Участь в торгах і аукціонах | стратегічна інформація, інформація про підготовку до торгів і результати торгівлі |
| 11. | Наукова і дослідницька діяльність | по створенню нової техніки відомості щодо програм перспективних досліджень і результатах |
| 12. | Використання нових технологій | інформація про їх зміст, специфіку застосування і отриманий ефект |
| 13. | Управління персоналом | персональні відомості про співробітників, методики добору, тестування кандидатів на посаду, результати поточної роботи з персоналом |

| | | |
|---|---|---|
| 14. | Організація безпеки підприємства | відомості щодо функціонування служби безпеки, змісту СЗІ, системи фізичного захисту |

До особливо цінної інформації прийнято відносити: відомості про виробництво і про продукцію; відомості про ринок і наукові розробки; матеріально-технічне забезпечення; умови контрактів і переговорів; відомості про персонал; відомості про систему безпеки; динаміка збуту продукції; ефективність послуг.

Для України характерно віднесення до особливо цінної інформації відомостей про фінансову діяльність та систему безпеки організації. Завжди цінною інформацією є «чужа» інформація, тобто інформація від підприємств, установ, організацій, партнерів і клієнтів, які співпрацюють з об’єктам захисту.

На стратегічний вибір впливають: ризик, на який готова йти організація; досвід реалізації чинних стратегій, позиції власників, наявність часу.

Стратегічним рішенням притаманна комплексність. Стратегія зазвичай є сукупністю взаємопов'язаних рішень, об’єднаних спільною метою, узгоджених між собою за термінами виконання та ресурсами. Такі рішення визначають пріоритети і напрямки розвитку фірми, її потенціалу, ринків, способи реакції на непередбачені події.

Практика сформувала нижченаведені вимоги до стратегічних рішень:

1. Реальність, що передбачає її відповідність ситуації, цілям, технічному та економічному потенціалу підприємства, досвіду і навичками працівників і менеджерів, культурі, існуючій системі управління;

2. Логічність, зрозумілість, прийнятність для більшості членів організації, внутрішня цілісність, несуперечність окремих елементів, підтримка ними один одного, що породжує синергетичний ефект;

3. Своєчасність (реалізація рішення повинна встигнути призупинити негативне розвиток ситуації або не дозволити упустити вигоду);

4. Сумісність із середовищем, що забезпечує можливість взаємодії з нею (стратегія перебуває під впливом змін в оточенні підприємства і сама може формувати ці зміни);

5. Спрямованість на формування конкурентних переваг;

6. Збереження свободи тактичного маневру;

7. Усунення причин, а не наслідків існуючої проблеми;

8. Чіткий розподіл за рівнями організації роботи з підготовки та прийняття рішень, а також відповідальності за них конкретних осіб;

9. Облік прихованих і явних, бажаних і небажаних наслідків, які можуть виникнути при реалізації стратегії або відмову від неї для фірми, її партнерів; в зв’язку з існуючим законодавством, етичною стороною справа, допустимим рівнем ризику та інше.

Розробка науково обґрунтованої системи стратегій організації як ключової умови її конкурентоспроможності та довгострокового успіху є однією з основних функцій її менеджерів, перш за все вищого рівня. Від них вимагається:

– виділяти, відстежувати і оцінювати ключові проблеми;

– адекватно і оперативно реагувати на зміни всередині і в оточенні організації;

– вибирати оптимальні варіанти дій з урахуванням інтересів основних суб'єктів, причетних до її діяльності;

– створювати сприятливий морально-психологічний клімат, заохочувати підприємницьку і творчу активність низових керівників і персоналу.

Вихідний момент формування стратегії – постановка глобальних якісних цілей і параметрів діяльності, які організація повинна досягти в майбутньому. В результаті ув’язки цілей і ресурсів формуються альтернативні варіанти розвитку, оцінювання яких дозволяє

вибрати кращу стратегію. Єдиних рецептів вироблення стратегій не існує. В одному випадку доцільно стратегічне планування (програмування) в іншому – ситуаційний підхід.

Виходячи з великої різноманітності умов, при яких може виникнути необхідність захисту інформації, загальна цільова установка на вирішення стратегічних питань полягала в розробці безлічі стратегій захисту, і вибір такого мінімального їх набору, який дозволяв би раціонально забезпечувати необхідний захист в будь-яких умовах.

Відповідно до найбільш реальних варіантів поєднань значень розглянутих факторів виділено три стратегії захисту:

– оборонна – захист від вже відомих загроз здійснюваний автономно, тобто без надання істотного впливу на інформаційно - керувальну систему;

– наступальна – захист від усієї множини потенційно можливих загроз, при здійсненні якої в архітектурі інформаційно - керувальної системи і технології її функціонування повинні враховуватися умови, продиктовані потребами захисту;

– упереджувальна – створення інформаційного середовища, в якому загрози інформації не мали б умов для прояву.

### *3.3 Режими доступу до інформації. Відповідальність за порушення законодавства до інформації.*

Залежно від типу інформації існують відповідні, специфічні правила поведінки при виконанні інформаційної діяльності, встановлені правовими нормами. Такі правила поведінки визначаються як режими доступу до інформації.

*Режим доступу до інформації* – це передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації. Особливою ознакою режиму доступу до інформації є специфіка його об’єкта – правові відносини, що виникають з приводу отримання, зберігання, використання та розповсюдження інформації.

Ключовими характеристиками режиму доступу до інформації є:

– суб’єкт визначення доступності цієї інформації:

– коло суб’єктів, які мають доступ до цієї інформації;

– особливі вимоги і правила зберігання та поширення цієї інформації;

– строк дії режиму.

Суб’єктом визначення доступності інформації є особа, до компетенції якої належить вирішення питань щодо встановлення обмежень на доступ до інформації та її матеріальних носіїв, а також надання права доступу до такої інформації.

Суб’єкт, що має доступ до інформації, – це особа, якій надано право ознайомлення з матеріальними носіями інформації або їх використання. Надання особі права доступу до інформації з обмеженим доступом зазвичай пов’язане із взяттям нею на себе зобов’язань щодо нерозголошення отриманої інформації.

Режим доступу до інформації означає певну сукупність правил, якими окреслено особливі вимоги і правила зберігання та поширення інформації. Ці правила визначають діяльність осіб, на яких покладена відповідальність за зберігання матеріальних носіїв інформації, установлюють необхідність застосування певних правових, організаційних, технічних та криптографічних засобів захисту інформації. Ці правила також визначають порядок надання доступу до такої інформації.

Нарешті, більшість видів інформації з обмеженим доступом мають визначений законодавством або власником інформації строк дії режиму обмеження доступу до інформації. Цей строк визначають, як правило, під час ухвалення рішення про обмеження доступу до інформації або її матеріальних носіїв. Після закінчення цього строку може бути прийняте рішення або про його поновлення, або про надання інформації статусу відкритої.

Право на доступ до публічної інформації гарантується юридичною відповідальністю за порушення законодавства про доступ до публічної інформації. Однією з гарантій дотримання права на інформацію є встановлення відповідальності за порушення законодавства про інформацію. Рішення, дії чи бездіяльність розпорядників інформації можуть бути оскаржені до керівника розпорядника, вищого органу або суду. Зокрема, відповідно до ст.7 Закону України «Про інформацію» суб'єкт інформаційних відносин може вимагати усунення будь-яких порушень його права на інформацію.

Відповідно до ст. 3 Закону України «Про доступ до публічної інформації» право на доступ до публічної інформації, серед іншого, гарантується встановленням юридичної відповідальності за порушення законодавства про доступ до публічної інформації.

Відповідно до ч.1 ст.27 Закону України «Про інформацію» порушення законодавства України про інформацію тягне за собою дисциплінарну, цивільну, адміністративну або кримінальну відповідальність згідно із законами України.

Відповідно до ст.24 Закону України «Про доступ до публічної інформації» відповідальність за порушення законодавства про доступ до публічної інформації несуть особи, винні у вчиненні таких порушень:

1) ненадання відповіді на запит;

2) ненадання інформації на запит;

3) безпідставна відмова у задоволенні запиту на інформацію;

4) не оприлюднення інформації відповідно до статті 15 цього Закону;

5) надання або оприлюднення недостовірної, неточної або неповної інформації;

6) несвоєчасне надання інформації;

7) необґрунтоване віднесення інформації до інформації з обмеженим доступом;

8) нездійснення реєстрації документів;

9) навмисне приховування або знищення інформації чи документів.

Особи, на думку яких їхні права та законні інтереси порушені розпорядниками інформації, мають право на відшкодування матеріальної та моральної шкоди в порядку, визначеному законом.

### *4.4. Службова інформація. Державна таємниця. Конфіденційна інформація. Професійна таємниця. Правові наслідки розголошення державної таємниці.*

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 внутрішньо-організаційних), 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.

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.

Види професійних таємниць згідно з 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.

*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.

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* – 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.

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».

### *3.5. Персональні дані. 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. Закон розділяє персональні дані на дві категорії: загальні та особливі (або їх ще називають чутливі). Це необхідно для того, щоб визначити ступінь ризику, внаслідок їх незаконної обробки (наприклад, збирання чи несанкціонованого витоку).

Наприклад, до загальної категорії можна віднести прізвище та ім’я особи, інформація про її місце проживання, дані, записані в посвідченні водія; підпис; IP-адреси та ін. Тобто це будь-які відомості, які дозволять прямо або опосередковано ідентифікувати людини.

Особлива категорія має вичерпний перелік видів персональних даних. Це інформація про расове або етнічне походження; політичні, релігійні, 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.

Тобто, це та інформація, яка може мати високий ризик для прав і свобод людини й потребує особливих умов для її обробки та захисту.

Крім того, наказом Уповноваженого Верховної Ради України з прав людини від

08.01.2014 р. затверджено Типовий порядок обробки персональних даних, у якому передбачено додаткові категорії персональних даних, обробка яких становить особливий ризик для прав і свобод суб’єктів:

притягнення до адміністративної 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.

Тому, працюючи з персональними даними, необхідно розрізняти їх категорію, мати законні підстави для їх обробки, вести записи та здійснювати документування усіх дій з такою інформацією.

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.

Правило щодо обмеження не застосовується, 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.

### *3.6. Шляхи поширення недостовірної інформації та механізми протидії в умовах війни*

Інформаційна безпека включає достатній рівень інформаційної культури особистості; спроможність держави створити умови для нормального розвитку й задоволення потреб людини в інформації, уникаючи при цьому інформаційних загроз; гарантії розвитку та використання інформаційного середовища в інтересах кожної особистості; захищеність від загроз. Останніми роками відбувається насичення соціальних мереж інформаційними потоками. На сьогодні практично немає наукового емпіричного та соціально-управлінського досвіду реагування на такі хвилі інформації.

Інформаційна безпека є дуже важливою під час військових дій, адже неправильно подана чи помилкова інформація може змусити населення панікувати, впливати на перебіг подій, прискорювати внутрішню міграцію населення, погіршувати імідж вищого військово-політичного керівництва, розпалювати недовіру до політиків, їхніх заяв і звернень, що може негативно позначитись на веденні бойових дій, крім того, може завдати непоправної шкоди для очікуваного результату військового конфлікту. Повномасштабне вторгнення РФ на територію України, знищення міст, сіл подається російськими ЗМІ як нібито «військова операція», виправдовуючи тим самим свої дії, та вказуючи при цьому на постійну небезпеку, яка йде від України

*Головними шляхами поширення недостовірної інформації* в умовах війни є соціальні мережі; підроблені акаунти відомих людей, політиків, телерадіомовні канали; особисті повідомлення або в групах Viber, WhatsApp, Telegram та інших месенджерах.

У сфері забезпечення інформаційної безпеки важливе місце посідає проблема чуток – недостовірних повідомлень, що мають різноманітну комунікативну форму. Чутки є найпершою формою суспільної комунікації, і незважаючи на технічний прогрес, появу Інтернету та інших телекомунікаційних технологій, не тільки не зменшили свого впливу, більше того, чутки стали «віртуальними».

Варто відзначити, що миттєва швидкість передачі повідомлень у мережі, максимальна анонімність інтернет-спілкування стали гарним живильним середовищем для поширення чуток. Порівняно зі звичайними чутками, інтернет-чутки передаються миттєво та швидко охоплюють гігантську аудиторію, впливаючи на свідомість та поведінку громадян.

Істотно збільшилася швидкість їхньої поширеності та масштабів охоплення аудиторії. Коли в мирних умовах плітки могли знищити чиюсь кар’єру чи особисте життя, то у воєнних умовах – драматично вплинути на долі сотень тисяч людей. Так звані «колишні», гвардія новітніх «експертів» є старими генераторами з видумування чуток, поширення пліток і поголосок.

База інформації «колишніх» – це особисті фантазії, тому що вони насправді не мають ніякої достовірної інформації ні про переговори, ні про тактичні чи стратегічні плани української влади і командування, тому що вони не бувають там, де приймаються серйозні рішення.

Окремо стоїть проблема поширення фейків. *Фейк* є навмисно сфабрикованою інформацією, яка не має ніяких підстав.

Ця інформація завжди комусь вигідна: якщо на сайті з’являється «жовта» новина, то

вона приносить більше трафіку; «зраду» та «перемогу» часто використовують як техніки політичної пропаганди, плітки під виглядом фактів використовують, щоб зіпсувати репутацію конкуренту. Фейки ґрунтуються на брехні, маніпуляціях та перекручуваннях фактів. Нині фейки та інша дезінформація поширюється через Інтернет.

Найчастіше для цього використовуються месенджери (Whatsapp, Viber, Telegram), соцмережі (Facebook, Twitter, Instagram), онлайн-платформи (Reddit, 4chan). Можна виділити такі види фейків:

- фейк-реклама характеризується тим, що просуває певний продукт (перевірити інформацію можна на офіційних сайтах);
- фейк- псевдо експерт має особливістю вказувати форму особи, ім'я, які не можна загуглити, не вказуються імена і посилання на офіційні ресурси (в таких випадках необхідно наводити справжні дослідження на схожу тематику);
- фейк-конспірологія заснований на теорії змови, абсурду (в таких випадках у соцмережах слід відразу писати коментар);
- фейк-клікбейт відрізняється від інших «сенсацією», «шоком», заголовок не відповідає тексту повідомлення.

З ціллю максимального просування фейків працюють ботоферми та «фабрики Інтернет-тролів». Широко практикується пранкінг, інші новітні форми дезінформування, просування особистостей, теорій, ідей, проєктів, партій – заради створення у свідомості людей якогось бажаного образу (позитивного чи негативного).

У сучасних умовах фейки використовуються ще й у битві наративів та культур. Найчастіше РФ застосовує такі наративи: «Україна – фашистська держава», «українці – бандерівці», «звільнення українців від націоналістів» тощо. Фейки дають можливість дистанційно управляти противником без насилля та кровопролиття. В контексті війни інформацією намагаються погіршити стосунки між людьми, схиляти їх до порушень норм поведінки, традиції, права, підривати довіру до влади, формувати панічні настрої тощо.

Фейкові неправдиві повідомлення націлені на заповнення недоліків або повну відсутність інформації у суспільстві зі сфер, які його цікавлять, з офіційних джерел. Більше стійкою буде інформаційна безпека, якщо вище буде довіра до офіційної інформації, тоді люди менше будуть вишукувати інформацію з невідомих джерел. Відтак, офіційні джерела завжди мають говорити правду без двомовності та недомови. Інформаційна безпека у першу чергу ґрунтується на довірі, немає довіри до офіційної інформації або вона дозована або зовсім відсутня, що є відкритим полем для операції противника.

*Механізмами захисту від психологічних наслідків інформаційних загроз мають бути такі*: свобода слова; незалежність ЗМІ та свобода друку; ЗМІ мають здійснювати свою діяльність на благо держави; органи державної влади мають звертати увагу ЗМІ та населення на відповідальність за подання свідомо неправдивих даних.

Ще одним важливим аспектом інформаційно-психологічної безпеки є блокування прихованого шкідливого інформаційного впливу, що особливо важливо для жителів фронтових та прифронтових територій.

Під час бойових дій виникає безліч фейкових новин про події в регіонах, рішення влади, думки та офіційні заяви, які можуть істотно вплинути на підсумок військового конфлікту. Так, з'явилися засновані на технології штучного інтелекту генератори синтезованого медіа-контенту – фейкових новин, «глибоких фейків» (Deep Fake), що дозволило робити реалістичні фото, аудіо та відео-підробки (створені навіть на основі лише голосу людини).

Науковці Технологічного університету Наньянга (Сінгапур) та китайські розробники в галузі штучного інтелекту із Sense Time розробили метод створення діпфейків на основі

звукозапису: штучний інтелект використовує голос однієї людини, що поєднує з фото або відео іншої людини – і синтезує цілком реалістичне відео того, як людина промовляє слова із джерела звуку; в такому разі людина на відео стає маріонеткою для оригінального голосу.

У глядача при перегляді діпфейкового відео створиться враження, що він дивиться справжнє відео. Можемо згадати діпфейкові відео про капітуляцію Президента Зеленського. Хоча відразу було зрозуміло, що це фейк, але ж легко уявити, наскільки руйнівним це може бути, коли технологію діпфейків стане важче виявити. Коли розкрити подібні відео стане неможливим, то сфабриковані медіа різко збільшать ризик діпфейкових новин і можуть розпалити недовіру до головних ЗМІ, адже підроблені відео та зображення може створювати будь-хто за допомогою безкоштовних програм, таких як Wombo та FaceApp.

Головними механізмами протистояння брехливій, перекрученій, неперевіреній інформації в умовах війни є такі. Насамперед, це підвищення медіа грамотності населення, що дозволяє йому захищатися від дезінформаційних впливів та допомагати підтримувати інформаційну безпеку держави.

*Медіаграмотність* містить такі компоненти, як критичне мислення, орієнтування в медіа, споживання медіа та дизайн медіа. Медіа-маніпуляція суспільною свідомістю або думками здійснюється за допомогою впливів на сприйняття людини через зір (медіадизайн); можливість орієнтуватися в інформаційному просторі, який є просто гігантським, а часу на повноцінне його вивчення бракує; через значні обсяги контенту, а також через неможливість критично сприймати інформацію через прихильність тільки конкретним ЗМІ.

Нині стало зрозумілим, що інформаційна війна є елементом повномасштабної війни, що медіаосвіта, медіаграмотність, вироблення стійкості до впливу дезінформації є питаннями національної безпеки. Свідомість українців атакують з метою виявити слабкі місця, які відкрила війна, та вдарити по них. А тому, щоб оминути пастки проросійських ресурсів й не поширювати дезінформацію, необхідно *по-перше*, застосовувати критичне мислення, а саме чітко бачити для чого використовується в певному медіа той чи інший контент як інструмент пропаганди чи маніпуляції, яке завдання ставить перед собою і зміст недійного матеріалу і сам цей медіа, в чому виявляється їхня шкода.

*По-друге*, потрібно щоденне об’єктивне висвітлення новин та іншої інформації через державні інтернет-видання, ЗМІ, звернення до народу. Регулярне надання інформації про основні події, тим більше під час війни допоможе розвіяти чутки та викрити фейки.

Ці дії дають змогу боротися з фейками, чутками, маніпуляціями, перекручуваннями та іншою дезінформацією щодо бойових дій, а також зміцнюють ставлення звичайних українців до влади, знижують рівень паніки серед народу, поліпшують морально-психологічний стан населення, яке проживає у прифронтовій зоні.

*По-третє*, слід запровадити юридичну відповідальність за створення та поширення фейків. Важливим компонентом забезпечення інформаційної безпеки суспільства є встановити кримінальну відповідальність за надання свідомо невірної, неперевіреної, перекрученої інформації, особливо коли дезінформація поширюється під час війни.

*По-четверте*, встановити жорсткий контроль підроблених акаунтів, що свідомо розсилають дезінформацію у вигляді фейків. Наприклад, контроль за поширенням фейкової інформації зараз втілюють найпопулярніші месенджери. WhatsApp особливим символом маркує повідомлення, які пересилалися дуже багато разів, що є важливою ознакою фейку.

*По-п’яте*, повномасштабне вторгнення російських військ на територію нашої країни супроводжується потужною агресією в кіберпросторі.

Для захисту інформаційного простору в умовах воєнних дій працює Ситуаційний центр забезпечення кібербезпеки при СБУ. Там діє система керування інформаційними подіями, яка відслідковує такі події в реальному часі та допомагає аналізувати стан інформаційної безпеки

держави, що дає змогу швидко виявляти, реагувати та упереджувати загрози для українського кіберпростору.

Виявленням фейків, діпфейків та їх нейтралізацією займатимуться сформовані спеціальні підрозділи в кіберполіції. Нині діє громадський рух кіберопору ворогові, що називається «КіберАрмія». Звичайні люди, разом із професіоналами, атакують ворога в кіберпросторі, завдають йому збитків та зривають плани. Крім того, під час війни, надзвичайно важливим стає нейтралізація численних інформаційних загроз, для чого необхідно проведення низки організаційно-правових заходів.

Вважаємо, що основними напрямками поліпшення системи забезпечення інформаційної безпеки держави мають стати:

- стратегічне стримування та припинення бойових дій та військових конфліктів, що можуть виникнути після зумисного застосування дезінформаційних технологій;
- поліпшення системи забезпечення інформаційної безпеки ЗСУ, інших військових формувань, включно з силами та засобами інформаційної протидії;
- прогнозування, виявлення та оцінка загроз, включаючи загрози для ЗСУ в сфері інформації.

У зв'язку з цим, зазначені напрями мають бути головними складовими діяльності органів, які формують інформаційну безпеку країни. Нині інформація як зброя є доволі серйозним засобом ведення війни оскільки її технологічна інноваційність, потужність є небезпечними.

Відповідно, інформаційна безпека України має базуватися на синхронізованих діях структур держави та громадянського суспільства. Під час війни суттєво зросла роль інформаційної культури як чинника підсилення опору дезінформаційній зброї громадянами та збереження державного суверенітету України.

Нинішня війна добре демонструє, що інформація використовується і в якості зброї масового ураження. У зв'язку з цим потрібно побудувати ефективний механізм, котрий би гарантував інформаційну безпеку України, в основу якого, на нашу думку, важливо покласти такі складові: технічну – створити належну технічну базу функціонування інформаційної безпеки; політичну – державна політика повинна бути направлена на забезпечення інформаційної безпеки; правову – оформлення всіх заходів інформаційної безпеки якісними нормативно-правовими актами.

Аналіз проблеми забезпечення інформаційної безпеки громадянина та держави під час бойових дій та конфліктів дозволяє дійти висновку, що інформаційна безпека відіграє надзвичайно важливу роль особливо під час війни. Адже дезінформація може викликати панічні настрої серед населення, негативно вплинути на перебіг подій, прискорювати внутрішню міграцію населення, що може негативно позначитись на даєздатності Збройних Сил України, а також на фізичному й психічному стані громадян.

Ефективно протидіяти інформаційній агресії видається, на нашу думку, можливим за рахунок залучення до цього процесу міжнародних організацій, інституцій та міжнародної спільноти загалом. Практика показує – кордонів для ведення інформаційної війни не існує.

## ПИТАННЯ ДЛЯ САМОПЕРЕВІРКИ

1. Які види інформації, відповідно до законодавства, є предметом захисту?
2. Вкажіть основні напрямки формування цінної інформації та охарактеризуйте їх.
3. Якими є критерії цінності інформації та стратегії комплексного захисту інформації та інформаційних ресурсів?
4. Окресліть умови, при яких може виникнути необхідність захисту інформації.
5. Які режими доступу до інформації Ви знаєте?

6. За які порушення про доступ до публічної інформації, відповідно до законодавства, настає відповідальність?
7. Яка інформація відноситься до державної таємниці? Охарактеризуйте правові наслідки розголошення державної таємниці.
8. Які види професійних таємниць, згідно з вітчизняним законодавством, Ви знаєте?
9. Надайте коротку характеристику вимог до обробки персональних даних.
10. На практичних прикладах визначте шляхи поширення недостовірної інформації та механізми протидії в умовах війни.

# ЛЕКЦІЯ 4
# ВЗАЄМОЗВ'ЯЗОК ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

**План викладу:**

4.1 Сутність, поняття та правове визначення поняття «інформаційна діяльність»: складові, засоби та структура

4.2 Інформаційні ресурси: сутність та види, основні функції, ієрархічні рівні.

4.3 Інформаційний ресурс як об'єкт інформаційної небезпеки: класифікація інформаційних ресурсів.

4.4 Особливості здійснення інформаційної діяльності в умовах постіндустріального суспільства.

4.5 Перспективи та напрями розвитку інформаційної діяльності та її вплив на процеси забезпечення інформаційної безпеки..

## *4.1 Сутність, поняття та правове визначення поняття «інформаційна діяльність»: складові, засоби та структура*

У сучасних умовах стрімкого розвитку глобального інформаційного суспільства, коли інформаційна сфера набуває ознак інтегрованого, транс-національного явища, першочергове завдання вітчизняного законодавця полягає в розробці дієвих механізмів забезпечення входження України до світового інформаційного простору, з одного боку, та убезпечення від можливих загроз, що є зворотнім боком цих процесів, з іншого боку. Ключовим сегментом цієї сфери, розвиток якої повинен бути пріоритетним, є інформаційна діяльність.

Відповідно до визначення, наданого у сучасному тлумачному словнику діяльність – це праця, систематичне застосування своїх сил в який-небудь сфері. У свою чергу, праця тлумачиться як знаходження в дії, виробнича діяльність зі створення, обробки чогось; служба; заняття (в тому числі як джерело заробітку).

Узагальнюючи наведені положення, сформулюємо, що діяльність як така – це систематичний, відносно тривалий процес докладання зусиль, спрямований на створення певних благ, що можуть мати як матеріальну, так і нематеріальну природу.

У вітчизняній науці розробленими є визначення різновидів інформаційної діяльності (інформаційно-аналітичної, інформаційно-наукової тощо), проте відсутня єдина, загальна дефініція, якою б усі вони охоплювалися.

Тлумачний словник комп'ютерних інформаційних систем і сховищ даних подає наступне визначення інформаційної діяльності: *інформаційна діяльність* – діяльність, що забезпечує збирання, обробку, збереження, пошук та розповсюдження інформації, а також формування організаційного ресурсу та організацію доступу до нього.

О.В. Синєокий визначає інформаційну діяльність як сукупність інформаційних дій, технічних засобів, організаційних умов і модернізаційних заходів, що ґрунтуються на ефективному використанні високих технологій, метою чого є оптимальне задоволення інформаційних потреб громадян і юридичних осіб, а також реалізація інформаційних функцій і завдань держави.

Як бачимо, запропонованим визначенням охоплено не тільки власне процес створення певних благ, але й об'єкти матеріального світу – технічні засоби – та сукупність зовнішніх умов, що мають вплив на протікання визначених процесів. Окрім того, невиправдано, на нашу думку, звужується коло учасників таких правовідносин (воно обмежене особами приватного права та державою, тоді як інформаційною правосуб'єктністю наділені також щонайменше ще й органи місцевого самоврядування) та, відповідно, обмежено трактується поняття інтересу, що задовольняється в ході такої діяльності. Так, поза увагою залишається публічний

інтерес, який також може задовольнятися внаслідок здійснення інформаційної діяльності органами публічної влади.

Законом України «Про інформацію» (в редакції від 27.07.2023), не містить визначення поняття інформаційної діяльності, проте законодавцем закріплюється перелік її видів. Зі свого боку, «постійне та систематичне збирання та опрацювання записаної інформації з метою зберігання, пошуку, використання чи пересилання, що виконуються якою-небудь особою чи організацією» розглядається як інформаційна діяльність» (ДСТУ 2392-94. Інформація та документація. Базові поняття. Терміни та визначення).

Зокрема, статтею 9 встановлено, що основними видами інформаційної діяльності є: створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації. При цьому одержання інформації розуміється як:

– набуття, придбання, накопичення відповідно до чинного законодавства України документованої або публічно оголошуваної інформації громадянами, юридичними особами або державою;

– використання інформації як задоволення інформаційних потреб громадян, юридичних осіб і держави;

– поширення інформації як розповсюдження, обнародування, реалізація у встановленому законом порядку документованої або публічно оголошуваної інформації;

– захист інформації як комплекс правових, організаційних, інформаційно-телекомунікаційних засобів і заходів, спрямованих на запобігання неправомірним діянням щодо інформації;

– зберігання як забезпечення належного стану інформації та її матеріальних носіїв.

Водночас з усього переліку видів інформаційної діяльності у чинному Законі України «Про інформацію» міститься лише визначення захисту інформації, який трактується як сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

У свою чергу, правовою доктриною напрацьовано визначення вперше використаних у чинному Законі України «Про інформацію» понять створення, збирання та охорони інформації.

Так, створення трактується як процес розумової діяльності людини, що полягає у певних логічних перетвореннях, для якого характерним є досягнення поставленої мети, а також наступне відображення створеної інформації на матеріальних носіях, в електронному вигляді або в усній формі тощо. Збирання інформації є пошуком необхідної інформації за допомогою використання особою певних методів та засобів.

Охорона інформації здійснюється відповідно до законодавства України про інформацію і є комплексом відповідних гарантій держави щодо рівності прав доступу до інформації, неможливості обмеження прав особи щодо вибору форм, джерел одержання інформації тощо.

Інформаційна діяльність у суспільстві здійснюється суб’єктами, які мають певні інтереси і прагнуть їх реалізувати, ставлячи перед собою відповідні цілі. Їхня взаємодія з іншими суб’єктами (клієнтами, партнерами та ін.) обумовлює механізми і форми організації інформаційної діяльності в суспільстві.

Закон України «Про інформацію» визначає, що суб’єктами інформаційних відносин є: фізичні особи; юридичні особи; об'єднання громадян; суб'єкти владних повноважень.

Суб'єкт владних повноважень - орган державної влади, орган місцевого самоврядування, інший суб'єкт, що здійснює владні управлінські функції відповідно до законодавства, у тому числі на виконання делегованих повноважень.

Поряд з цим з метою аналізу механізмів і форм організації інформаційної діяльності можна розглядати учасників інформаційних відносин відповідно до їхньої ролі у процесі життєдіяльності суспільства використовуючи як аналог поділ, до якого вдаються економісти. Критерієм поділу тут виступатиме однотипність функцій учасників інформаційних відносин.

За таких умов визначені суб'єкти виділятимуться на такі категорії:

– населення (або домогосподарства), куди входять громадяни України та інших держав, а також особи без громадянства. Так, Конституція України (ст. 17) справою всього українського народу називає, зокрема, захист інформаційної безпеки України;

– комерційні організації, що є юридичними особами України та інших держав, включаючи приватних підприємців;

– некомерційні організації – юридичні особи України та інших держав;

– органи державної (центральної рівня) влади

– органи місцевого самоврядування.

Особливу увагу серед суб'єктів інформаційних правовідносин слід приділити останнім двом із наведених – суб'єктам владних повноважень. Серед них виділяють органи загальної та органи спеціальної компетенції.

І. Органи загальної компетенції:

1) Верховна Рада України. Визначає загальні засади інформаційної політики держави. Приймає закони та постанови в інформаційній сфері.

До установчих повноважень парламенту належать призначення на посади та звільнення з посад половини складу Національної ради України з питань телебачення і радіомовлення, призначення за поданням Прем'єр-міністра України Голови Державного комітету телебачення і радіомовлення України. Верховна рада України здійснює парламентський контроль в інформаційній сфері;

2) Президент України. Підписує прийняті Верховною Радою України закони, видає укази та розпорядження з питань інформаційної політики та інформаційної безпеки.

У сфері установчих повноважень Президент України призначає на посади та звільняє з посад половину складу Національної ради України з питань телебачення і радіомовлення;

3) Кабінет Міністрів України. Проводить державну політику у сфері інформатизації, сприяє становленню єдиного інформаційного простору на території України;

4) місцеві державні адміністрації. Здійснюють на відповідних територіях державний контроль, зокрема, за додержанням законодавства про державну таємницю та інформацію.

5) органи місцевого самоврядування. До повноважень виконавчих комітетів місцевих рад належить, зокрема, сприяння діяльності Державної служби спеціального зв'язку та захисту інформації України, створення та забезпечення функціонування місцевих автоматизованих інформаційно-аналітичних систем.

ІІ. Органи спеціальної компетенції:

1) Національна рада з питань телебачення і радіомовлення. Є конституційним, постійно діючим колегіальним органом, метою діяльності якого є нагляд за дотриманням законів України у сфері телерадіомовлення, а також здійснення регуляторних повноважень, передбачених законами. Здійснює нагляд за: дотриманням телерадіоорганізаціями та провайдерами програмної послуги вимог законодавства у галузі телерадіомовлення; дотриманням ліцензіатами вимог законодавства України щодо реклами та спонсорства у сфері телерадіомовлення; дотриманням ліцензіатами ліцензійних умов та умов ліцензій; дотриманням ліцензіатами визначеного законодавством порядку мовлення під час проведення виборчих кампаній та референдумів; дотриманням стандартів та норм технічної якості телерадіопрограм; дотриманням телерадіоорганізаціями законодавства України у сфері кінематографії; дотриманням телерадіоорганізаціями вимог законодавства України щодо

частки вітчизняного продукту у їх програмах (передачах) та щодо вживання мов при здійсненні телерадіомовлення; дотриманням телерадіоорганізаціями законодавства у сфері захисту суспільної моралі;

2) Державний комітет інформаційної політики, телебачення і радіомовлення України. Є центральним органом виконавчої влади зі спеціальним статусом, діяльність якого спрямовується та координується Кабінетом Міністрів України. Комітет, зокрема: розробляє заходи щодо запобігання внутрішньому і зовнішньому інформаційному впливу, який загрожує інформаційній безпеці держави, суспільства, особи; бере участь у формуванні єдиного інформаційного простору, сприянні розвитку інформаційного суспільства; реалізує разом з іншими державними органами завдання щодо забезпечення інформаційної безпеки; готує пропозиції щодо вдосконалення системи державного управління у сфері телебачення і радіомовлення, інформаційній та видавничій сферах, поліграфії; вживає заходів щодо надання державної фінансової підтримки засобам масової інформації, творчим спілкам у сфері засобів масової інформації;

3) Державна служба спеціального зв'язку та захисту інформації. Є державним органом, який призначений для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, а також інших завдань відповідно до закону;

4) Служба безпеки України – державний правоохоронний орган спеціального призначення, який забезпечує державну безпеку України. Здійснює 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;

5) Державну службу з питань електронного урядування. Є центральним органом виконавчої влади, діяльність якого спрямовується і координується Кабінетом Міністрів України через Міністра освіти і науки. Утворюється для реалізації державної політики у сфері наукової, науково-технічної та інноваційної діяльності, інформатизації, формування і використання національних електронних інформаційних ресурсів, створення умов для розвитку інформаційного суспільства;

6) Книжкова палата України – державна наукова установа у сфері видавничої справи та інформаційної діяльності, є Національним агентством України Міжнародної стандартної нумерації книг (ISBN) та Міжнародної стандартної нумерації нотних видань (ISMN).

### *4.2. Інформаційні ресурси: сутність та види, основні функції, ієрархічні рівні*

За тлумачним словником, слово «ресурси» походить від французького ressourse - допоміжні засоби (грошові кошти, цінності, запаси, можливості, джерела прибутків тощо). Наявність корисних ресурсів у будь-якій сфері діяльності - це гарантія і застава її стабільності та процвітання. В сучасному понятті в складі ресурсів можна виділити матеріальні, енергетичні, трудові, фінансові, технологічні та інформаційні ресурси.

Виникнення поняття інформаційні ресурси пов'язано із зростаючою залежністю від наявності інформації, рівня розвитку та ефективності використання засобів її обробки та передачі. 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 будемо 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)».

Інформаційний ресурс має низку характерних особливостей:

– на відміну від інших (матеріальних) ресурсів, він практично невичерпний;

– з використанням інформаційних ресурсів 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;

– інформаційні ресурси не є самостійними і самі по собі мають лише потенційне значення. Тільки поєднуючись з іншими ресурсами – досвідом, працею, кваліфікацією, технікою, енергією, сировиною – він є рушійною силою;

– ефективність застосування інформаційних ресурсів 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;

– інформаційні ресурси виникають в результаті не просто розумової праці, а її творчої частини.

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.

Класифікації інформаційних ресурсів представлена на рисунку 4.1.

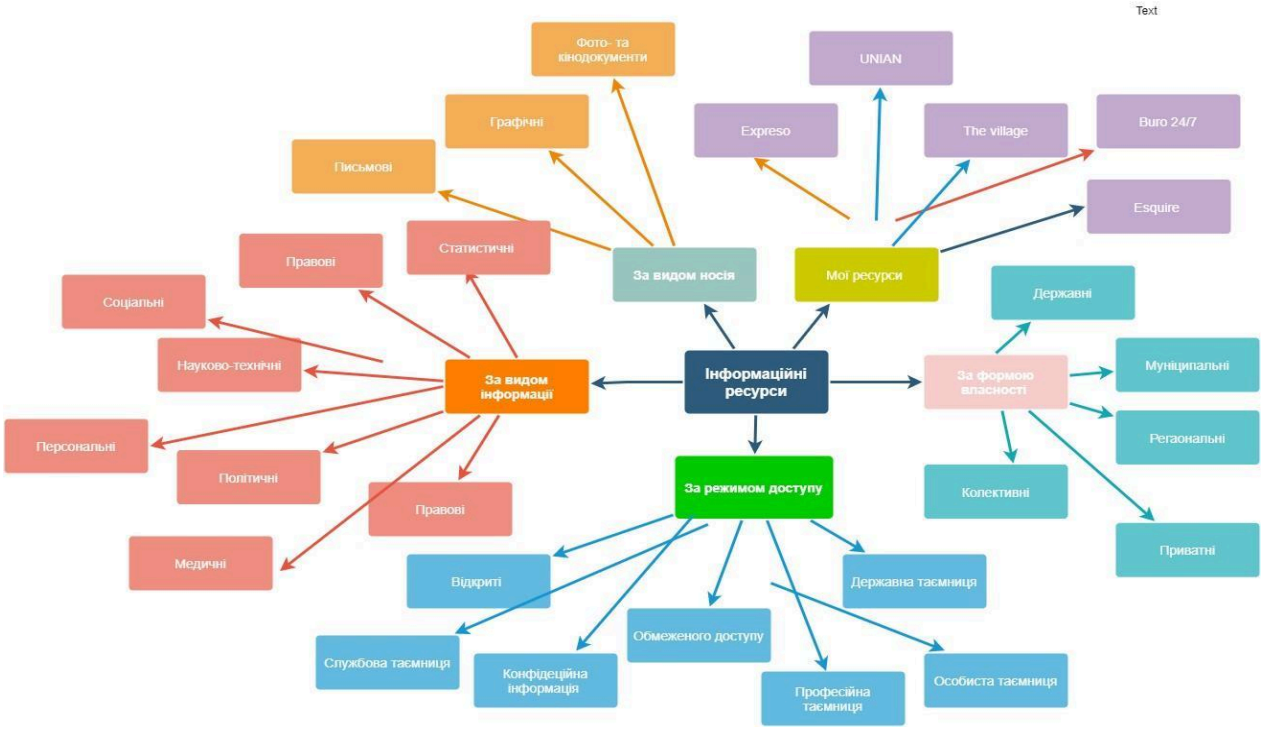



Рис.4.1 – Класифікації інформаційних ресурсів

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. Вітчизняне 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.

### *4.3 Інформаційний ресурс як об’єкт інформаційної небезпеки: класифікація інформаційних ресурсів*

Швидкий розвиток стимулював створення новітнього інформаційного суспільства і, як наслідок, це спонукало до виникнення таких явищ як «кіберзагрози» та «кібератаки» у публічному управлінні, банківській, воєнній, критичній інфраструктурі.

Інформаційний суверенітет та інформаційна безпека України гарантується і забезпечується безпосередньо на законодавчому рівні. Нове звучання інформаційна безпека набула через повномасштабне вторгнення держави агресора в Україну, де проводить жорстокі підступні військові дії не лише на території нашої держави, але й в інформаційному просторі. Відповідно до Указу Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»» було встановлено, що «інформаційна політика російської федерації – загроза не лише для України, але й для інших демократичних держав».

Спеціальні інформаційні операції країни-агресора спрямовуються на ключові демократичні інституції (зокрема, виборчі), а спеціальні служби держави-агресора намагаються посилити внутрішні протиріччя в Україні та інших демократичних державах. Застосовані технології гібридної війни проти України, у тому числі моделі і механізми інформаційного втручання, поширюються на інші держави, швидко адаптуючись до локальних контекстів та регуляторних політик. Обмежувальні заходи (санкції) та ефективний механізм моніторингу і відповідальності за їх порушення є одним із дієвих механізмів відповіді на дезінформаційну активність рф як держави-агресора.

Крім того, тривалий час спеціальні служби країни-агресора проводять свої спеціальні інформаційні операції, більшість із яких спрямовані на підрив національної безпеки України, її національних інтересів, ліквідацію української державності та знищення української ідентичності, провокування проявів екстремізму, панічних настроїв у суспільстві, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації в Україні.

У результаті тимчасової окупації у 2014 році державою-агресором частини території України були захоплені розташовані на цій території об’єкти інформаційної інфраструктури, зокрема й об’єкти Концерну радіомовлення, радіозв’язку та телебачення.

Державою-агресором застосовуються методи тотального придушення свободи слова, контролю над редакційною політикою засобів масової інформації та інших інформаційних ресурсів, що функціонують на цих територіях. На тимчасово окупованих територіях, у районах здійснення заходів із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії рф у Донецькій, Луганській, Запорізькій областях розгорнуто безпрецедентну інформаційну кампанію. Використовуючи також регулярне постачання на тимчасово окуповані території потужного передавального обладнання та блокування українських інформаційних ресурсів, Російська Федерація намагається створити альтернативну викривлену інформаційну реальність, побудовану на наративах держави-агресора.

Інформаційний тиск, що здійснюється державою-агресором, негативно відображається й на дітях, які проживають на тимчасово окупованих територіях, адже через свій вік вони є особливо вразливими для впливу інформаційних кампаній. В Україні триває процес становлення системи стратегічних комунікацій.

Органами державної влади України здійснено низку організаційних та практичних заходів зі зміцнення власної інституційної спроможності у сфері стратегічних комунікацій, однак не створено дієвого механізму координації і взаємодії між усіма органами державної влади, залученими до здійснення заходів із протидії загрозам в інформаційній сфері. Зазначене послаблює можливості до розбудови комплексного стратегічного планування інформаційного потоку, здійснення системної комунікативної діяльності Кабінету Міністрів України, об’єднання всіх ключових суб’єктів у сфері інформаційних відносин, суб’єктів формування і реалізації державної політики щодо ефективного захисту національного інформаційного простору, утвердження позитивного іміджу України, реалізації цілей захисту національної безпеки України в інформаційній сфері.

Регулювання відносин у сфері інформаційної діяльності не відповідає сучасним викликам та загрозам. Необхідність гарантування інформаційної безпеки зумовлюється, по-перше, потребою забезпечення національної безпеки України в цілому, по-друге, існуванням таких загроз інформаційній сфері країни, які можуть завдавати значної шкоди загальним національним інтересам, по-третє, урахуванням того, що за допомогою інформації можна впливати на зміну свідомості і поведінку людей.

Завдання інформаційної безпеки – створення системи протидії інформаційним загрозам та захист власного інформаційного простору, інформаційної інфраструктури, інформаційних ресурсів держави. При виникненні криз, загостренні конфліктів інформаційна боротьба може перерости в інформаційну війну, яка здійснюється за допомогою інформаційної зброї. Показниками, виступають цілеспрямованість, масштабність та комплексність дій тощо. Отже, державна політика щодо забезпечення інформаційної безпеки є важливою складовою національної безпеки. В її основі повинна бути системна превентивна діяльність органів державного управління щодо надання гарантій інформаційної безпеки особистості, соціальним групам, суспільству і державі в цілому. Аналіз свідчить про існування реальних загроз інформаційній безпеці України.

Інформаційна безпека працює задля запобігання можливого нанесення шкоди шляхом упередженого інформування населення, яка як наслідки призводить до неправдивого та незаконного висвітлення інформації, її розповсюдження, використання та поширення.

### *4.4 Особливості здійснення інформаційної діяльності в умовах постіндустріального суспільства.*

Досліджуючи інформаційну діяльність в постіндустріальному суспільстві як діяльність зі збирання, зберігання, а також обробки, розповсюдження, реалізації інформації, знань за

допомогою інформаційно-комунікаційних технологій (вони включають технічні засоби, людський капітал) в обставинах потоків інформації, що різко збільшилися, є можливість відзначити її великий вплив на будь-які галузі людського життя.

Стан людської цивілізації пов'язаний з розвитком інформаційного суспільства. Рівень інформаційного суспільства визначається кількістю та якістю накопичень інформації, її свободою та доступністю. Одним із елементів та функцій інформаційного суспільства вважаються інформаційні технології, спрямовані на регулювання, збереження, підтримання та вдосконалення системи управління нового мережевого суспільства. Якщо в історії людства інформація та знання передавалися на основі правил та розпоряджень, традицій та звичаїв, культурних зразків та стереотипів, то сьогодні головна роль відводиться технологіям.

Вступ сучасного суспільства в інформаційну стадію розвитку – об'єктивний та закономірний процес, у якому провідну роль відіграють інформація та знання, трансформовані у нових інформаційних та телекомунікаційних технологіях. Такі феномени, як інформаційні ресурси, нові інформаційні технології, інформатизація мають фундаментальну роль у розвитку інформаційного суспільства. Сьогодні є підстави говорити про формуванні нової інформаційної культури, яка може стати елементом загальної культури людства, нею стануть знання про інформаційне середовище, закони її функціонування, вміння орієнтуватися в інформаційних потоках.

Обробка інформації - об'єктивно існуюча реальність і процес, що породжує розширене відтворення знань. Подібно до того, як відповіді на одні питання породжують більшу кількість нових, але вищого порядку, інформація з розвитком людства накопичувалася і збільшувалася, породжуючи необхідність у розробці більш досконалих методів її збирання, зберігання, накопичення, зміни, захисту та транспортування.

Інформатизація суспільства часто породжує замкнутість людини в технічних засобах за її одночасної відкритості навколишнього світу. Спілкування через пристосування-гаджети створює одночасно і нові можливості, і нові загрози. У зв'язку з цим без грамотно збудованої системи адаптації та освіти, що відповідає таким новим викликам, не обійтися.

Основою формування постіндустріального суспільства виступає орієнтація на нові знання та технології. Однак, для їх повноцінного застосування і, тим самим, закладання основ такого суспільства важливо мати добре оснащену науково-технологічну базу. З іншого боку, суспільство має мати певний розумовий і фізичний потенціал, що становить основу людського капіталу. Порівнюючи інформаційну діяльність і постіндустріальне суспільство, слід зазначити, що показники, складові кожного притаманні іншому. Ресурсом обох вважаються знання, інформація, в основі обох лежить безпосередньо інтелектуальний капітал. Отже, можна стверджувати, що інформаційна діяльність вважається невід'ємною частиною всього постіндустріального суспільства, головним чинником розвитку останнього. Таким чином, постіндустріальне суспільство базується на інформаційній діяльності, на соціальних, економічних та правових відносинах, що виникають у процесі їхньої технологізації, та посиленні ролі «розумних» технологій у світовому економічному просторі.

### *4.5 Перспективи та напрями розвитку інформаційної діяльності та її вплив на процеси забезпечення інформаційної безпеки*

Формування системи забезпечення інформаційної безпеки держави ґрунтується на розробці механізму забезпечення інформаційної безпеки та комплексному поєднанні і реалізації найбільш ефективних методів, заходів та засобів її забезпечення. Вагомого значення має визначення найбільш важливих напрямів забезпечення інформаційної безпеки. Виходячи з вищезазначеного, забезпечення інформаційної безпеки є безперервним процесом, що

потребує необхідного планування, формування механізмів його впровадження та застосування широкого кола засобів, спрямованих на ефективне використання даного процесу і впровадження механізму моніторингу та контролю за ефективністю його реалізації. Першочерговим завданням у забезпеченні інформаційної безпеки держави є формування та впровадження цілісної системи економічної безпеки та механізму її забезпечення на засадах системності, єдності, спрямованості, комплексності, безперервності.

У зв'язку зі змінами, кон'юнктурою зовнішнього та внутрішнього середовища країни, появою нових викликів та загроз такий механізм має безперервно контролюватися, видозмінюватися та оновлюватися, щоб відповідати зростаючим вимогам часу та новим загрозам розвиткові інформаційного суспільства.

Забезпечення інформаційної безпеки здійснюється із впровадженням єдиної державної політики в інформаційній сфері та потребує розробки і прийняття необхідних правових засад, спрямованих на нормативно-правове регулювання відносин у сфері інформації, визначення структур та суб'єктів, відповідальних за безпеку та надання необхідних повноважень у регулюванні відносин у сфері інформації, формування органів забезпечення інформаційної безпеки та механізмів забезпечення інформаційної безпеки держави.

Заходи забезпечення інформаційної безпеки держави мають носити превентивний попереджувальний характер та спрямовуватися на недопущення реалізації потенційних загроз економічній безпеці держави в інформаційній сфері як для державних органів та розвитку суспільства, так і з метою забезпечення інформаційної безпеки суб'єктів підприємницької діяльності країни та її громадян. Із цією метою доцільним та необхідним є: впровадження моніторингу стану інформаційної сфери з проведенням систематичного аналізу та контролю можливості появи та реалізації потенційних загроз; виявлення джерел їхнього походження, характеру дії та об'єктів спрямування; розробка та впровадження своєчасних методів з їх попередження, а у випадку настання – своєчасної нейтралізації та ліквідації можливих наслідків їх негативної дії.

Механізм забезпечення інформаційної безпеки реалізується із застосуванням методів, інструментів та організаційно-економічних, правових, адміністративних, техніко-технологічних заходів із забезпечення економічної безпеки.

Основними заходами із забезпечення інформаційної безпеки держави є юридичні, організаційно-економічні та технологічні заходи, що базуються на таких засадах:

– створення нормативно-правової бази інформаційних відносин у суспільстві, що повною мірою регламентує механізми вільного доступу до створення, поширення, доступу до інформації будь-яким законним способом;

– забезпечення прав та охорона законних інтересів власників та розпорядників інформаційних ресурсів;

– персоніфікація відповідальності за засекречування, збереження, розсекречування інформації, що являє собою інформацію з обмеженим доступом, комерційну таємницю, чи інформацію з особистих даних;

– державна підтримка та розвиток сфери інформаційних послуг, що надаються громадянам та організаціям країни на основі розвитку сучасних комп'ютерних мереж, систем, баз та банків даних, доступ до яких гарантується та регламентується чинним законодавством країни.

Із метою забезпечення інформаційної безпеки держави необхідним є системне впровадження державної інформаційної політики, спрямованої на забезпечення реалізації стратегічних напрямів розвитку держави, а саме:

забезпечення захисту інформації та конституційних прав громадян в інформаційній сфері;

створення умов для інтеграції країни до світового інформаційного простору;

удосконалення вітчизняного законодавства в інформаційній сфері та сфері захисту інформації з метою приведення вітчизняного нормативно-правового поля в забезпеченні інформаційної безпеки до світових норм та стандартів;

захист інтелектуальної власності та продуктів інтелектуальної власності;

формування та розвиток у країні інформаційного суспільства та інтелектуальної економіки;

впровадження заходів ефективної протидії злочинам в інформаційній сфері, кіберзлочинності;

створення умов для розвитку прозорого та ефективного інформаційного та інформаційно-аналітичного забезпечення діяльності держаних, наукових, освітніх господарських та інших структур, установ та організацій;

розвиток взаємодії України зі світовим товариством в інформаційному полі та забезпечення прозорості відповідних інформаційних потоків;

системне впровадження ефективних державних засобів боротьби з піратством та порушенням прав інтелектуальної власності.

Основою формування та впровадження державної політики в інформаційній сфері є прийняття необхідних нормативно-правових актів, що визначають та регулюють відносини в інформаційній сфері та створення механізмів контролю за їхнім дотриманням. Впровадження виваженої та збалансованої державної політики в інформаційній сфері є основою забезпечення інформаційної безпеки держави. Вона має кілька основних базових напрямів розвитку:

- захист державної безпеки в інформаційній сфері;
- захист конституційних прав та свобод громадян на доступ, володіння та поширення інформації;
- захист національного інформаційного ринку та вітчизняних виробників інформаційної продукції;
- захист економічних інтересів держави у сфері інформації.

*Основними загрозами інформаційній безпеці держави є:* потенційні та наявні дії з метою повної чи часткової дестабілізації функціонування інформаційної сфери країни; потенційні чи реалізовані дії, що призводять до неправомірного володіння даними та їхнього несанкціонованого використання чи порушення цілісності інформаційної сфери, модифікації інформації в інформаційних системах, дестабілізації інформаційних потоків, знищення, псування; нерелевантна передача інформації в мережах та псування баз, банків даних, що призводить до значних матеріальних фінансових втрат як окремих суб’єктів господарювання, громадян країни, так і в цілому держави.

Основними загрозами інформаційної безпеки держави є загрози, пов’язані зі збереженням, розголошенням і використанням інформації та інформаційних ресурсів держави та її громадян:

- несанкціоноване ознайомлення з інформацією, що є конфіденційною та являє собою комерційну таємницю;
- розголошення конфіденційної інформації;
- незаконне володіння та використання конфіденційної інформації особами, що не мають права доступу до неї;
- зміна структури інформації та порушення її цілісності;
- порушення режиму доступу до інформації та можливості її використання;
- знищення інформації з метою нанесення прямих матеріальних збитків;

- псування мереж та інформаційних систем, програмних та технічних засобів обробки, передачі та збереження інформації;

- неконтрольоване використання інформаційних систем;

- відсутність належного контролю та необхідних умов дотримання інформаційної безпеки.

Із метою забезпечення інформаційної безпеки держави доцільними та необхідними є розробка наступних напрямів її захисту за такими групами, як організаційно-адміністративний захист, нормативно-правовий захист, та інженерно-технічний захист.

До групи організаційно-адміністративного захисту відносять регламентацію взаємовідносин між користувачами та суб'єктами інформаційного поля, що закріплюється на нормативно-правовій основі з визначенням власників та користувачів даної інформації, закріпленням їхніх прав на створення, володіння, використання, розповсюдження, збереження та зміну інформації в інформаційному полі. Таке закріплення здійснюється через нормативно-правові відносини та договірну діяльність. Першочергового значення в забезпеченні інформаційної безпеки мають організаційні заходи та створення механізму захисту інформації.

Наступною групою є група нормативно-правового захисту, що ґрунтується на закріплені взаємовідносин та регулюванні прав інформаційної та інтелектуальної власності на основі міжнародних конвенцій, міжнародних договорів, декларацій, державних та міжвідомчих нормативно-правових актів, договірної та нормативної діяльності між суб'єктами господарювання в межах країни.

Для групи інженерно-технічного захисту характерним є застосування комплексу сучасних технічних засобів, що використовуються з метою недопущення нанесення шкоди діяльності об'єктів безпеки на всіх її рівнях. У сучасних умовах підвищення ролі інформаційних технологій в Україні, як і світі, зростає необхідність у створенні та впровадженні системи ефективного захисту інформації.

Визначну роль у забезпеченні інформаційної безпеки держави має узгоджене функціонування державно-правового механізму. Державно-правовий механізм країни є взаємопов'язаною системою державних органів установ, що визначають нормативно-правове поле та регулюють суспільні, економічні та фінансово-господарські відносини між суб'єктами у сфері захисту інформації та забезпечення інформаційної безпеки.

Інформаційна політика держави будується на засадах створення інформаційного суспільства та освоєння єдиного інформаційного простору і спрямована на забезпечення потреб країни та її громадян в інформації. Одним із завдань інформаційної політики держави є інтеграція інформаційного поля країни до єдиного світового інформаційного поля. При цьому важливим та актуальним стає питання забезпечення інформаційної безпеки держави як на внутрішньо державному, так і міжнародному рівнях з урахуванням національних інтересів держави у процесі такого об'єднання.

Основним завданням забезпечення інформаційної безпеки держави є створення необхідних умов для забезпечення інформаційних потреб суспільства реалізація необхідних проактивних заходів щодо протидії потенційним та реальним загрозам та небезпекам в інформаційній сфері, пов'язаним із внутрішнім функціонуванням країни та її інтеграцією у міжнародний інформаційний простір.

Базовими напрямами державної інформаційної політики можна визначити наступні:

- нормативно-правове регулювання та приведення вітчизняного законодавства в інформаційній сфері до міжнародних норм та стандартів;

- забезпечення державного регулювання у сфері створення та використання інформаційних ресурсів та інформаційних технологій;
- охорона прав власників та користувачів інформаційних продуктів та об'єктів інтелектуальної власності в інформаційній сфері;
- удосконалення системи захисту інформації, що становить державну таємницю;
- забезпечення інформаційної безпеки в телекомунікаційних мережах;
- забезпечення інформаційної безпеки в мережах супутникового, стільникового та інших видів зв'язку;
- забезпечення інформаційної безпеки в галузі інформаційно-комп'ютерних технологій;
- забезпечення інформаційної безпеки інформаційних ресурсів при використанні системи Інтернет;
- забезпечення безпеки взаємодії вітчизняних інформаційних систем із зарубіжними аналогами та розширення співробітництва у сфері інформаційних технологій;
- створення умов, необхідних для формування спільного інформаційного простору на міжнародному рівні;
- забезпечення захисту інформаційних ресурсів держави, її громадян від кіберзлочинності та організація заходів та механізмів протидії кіберзлочинності на державному рівні;
- забезпечення захисту інформаційних ресурсів та інформаційної безпеки держави в умовах гібридної війни та військової агресії.

Формування системи забезпечення інформаційної безпеки держави та розбудова ефективного механізму її забезпечення в сучасних умовах не тільки спрямовані на захист інформаційної сфери держави від потенційних та наявних небезпек та загроз, але й здатні забезпечити ефективне функціонування та розвиток суспільних сфер країни.

Виважена, цілеспрямована інформаційна політика держави дає можливість покращити стан інформаційного поля країни та процесів його формування. В результаті розбудови сприятливого інформаційного поля та формування позитивного іміджу зростає авторитет країни на міжнародному просторі. Водночас для реалізації національних інтересів держави в інформаційній сфері необхідним є застосування нових концептуальних підходів до формування інформаційної, інвестиційної політики щодо регулювання у сфері інформаційних комунікаційних технологій, приведення вітчизняного законодавства у відповідність до міжнародних норм та забезпечення дотримання норм права в інформаційній сфері.

**ПИТАННЯ ДЛЯ САМОПЕРЕВІРКИ**

1. Надайте правове визначення поняття «інформаційна діяльність» та окресліть її складові, засоби та структуру.
2. Які види інформаційних ресурсів Ви знаєте? Коротко охарактеризуйте їх.
3. Які основні функції покладаються на інформаційні ресурси? Вкажіть відмінності між ними на ієрархічних рівнях.
4. Охарактеризуйте інформаційний ресурс як об'єкт інформаційної небезпеки та вкажіть характерні особливості.
5. Які ознаки притаманні електронним інформаційним ресурсам?
6. В чому полягають особливості здійснення інформаційної діяльності в умовах постіндустріального суспільства?
7. Яким чином реалізується механізм забезпечення інформаційної безпеки?
8. На яких засадах базуються юридичні, організаційно-економічні та технологічні заходи із забезпечення інформаційної безпеки держави?

9. Визначте перспективи та напрями розвитку інформаційної діяльності та її вплив на процеси забезпечення інформаційної безпеки та обґрунтуйте їх.

## ЛЕКЦІЯ 5
## НАЦІОНАЛЬНІ ІНТЕРЕСИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

**План викладу:**

5.1 Національні інтереси як реалізація природного права народу на самостійне існування та його включеність у світову цивілізацію.

5.2 Національні інтереси у сфері інформаційної безпеки: поняття та загальна характеристика.

5.3 Інтереси особи, суспільства та держави в інформаційній сфері.

5.4 Інформаційна безпека держави в умовах обмежень прав і свобод громадян у період воєнного стану

### *5.1 Національні інтереси як реалізація природного права народу на самостійне існування та його включеність у світову цивілізацію*

Національні інтереси завжди виступали і виступають нині у ролі дійової, рушійної сили історії, оскільки полягають у реалізації права кожного народу на самостійне існування та впровадження його у світову цивілізацію. Національні інтереси, на наш погляд, відображають фундаментальні цінності та прагнення українського народу, його потреби в гідних умовах життєдіяльності, а також цивілізовані шляхи їх створення і способи задоволення.

Національні інтереси України та їхня пріоритетність обумовлюються конкретною ситуацією, що склалася в країні та за її межами. Варто говорити про національні інтереси як внутрішні і про національно-державні інтереси - як зовнішні. Зауважимо, що такий поділ є до певної міри умовний, оскільки будь-який національний чи національно-державний інтерес має, як правило, і внутрішні, і зовнішні аспекти. Залежно від ступеня впливу на економічну, політичну, воєнну, науково-технічну та інші сфери функціонування держави національні інтереси можна класифікувати за ступенем важливості як життєво важливі, другорядні, критичні і за ступенем стійкості - стратегічні, оперативні і тактичні інтереси.

Формування життєво важливих інтересів відбувається протягом історичного становлення нації-держави як суб’єкта міжнародного права. До них можна віднести такі інтереси, як:

– підтримка і збереження територіальної цілісності України, захист її кордонів, суверенітету та державності;

– створення і забезпечення системи національної безпеки;

– інтеграція України в систему регіональної та глобальної безпеки;

– інтеграція України в світове економічне і політичне співтовариство, створення умов для залучення закордонних інвестицій, збереження старих та пошуки нових шляхів доступу до стратегічно важливих для економіки ресурсів;

– розвиток та підтримка процесів соціально-культурного і духовного відродження основ національної державності українського народу, його самобутності.

Стратегічні інтереси мають довгостроковий характер відповідно до обраного курсу розвитку держави. Загрози їм означають загрози життєво важливим інтересам України. Визначення стратегічних національних інтересів та їхнє юридичне оформлення як офіційно визнаних пріоритетів України, мають бути наслідком спільної праці всіх гілок влади. Формування їх є прерогативою Президента держави, однак Верховна Рада України оцінює

стратегічні інтереси за відповідністю життєво важливим інтересам України.

Оперативні (середньотермінові) інтереси, що виникають при вирішенні окремих проблем для подальшої реалізації стратегічних інтересів, виступають засобами впровадження в життя стратегічних завдань держави.

Тактичні інтереси, що виступають засобами впровадження в життя оперативних інтересів, як правило, короткострокові і після вирішення оперативних інтересів зникають. Категорія «національні інтереси» певною мірою кореспондується, на думку дослідників, з категоріями «індивідуальний», «загальнолюдський» і «державний» інтереси.

Науковий підхід до визначення національних і національно-державних інтересів, безперечно, передбачає врахування історичних, соціально-політичних та економіко-географічних чинників функціонування української нації. Вихідними засадами при цьому є чітке розуміння того, чим є сучасна українська нація у вузькому значенні як етнічно однорідна спільнота громадян української національності, що проживають в Україні, та в широкому - як відкрита поліетнічна спільнота, що історично склалася на території України, яка усвідомлює себе українським народом, а її члени - громадянами України, тобто мова йде про політичну націю.

Для нації як політичного суб’єкта найголовнішим є збереження її ідентичності і культурно-мовної самобутності у властивій саме цій нації формі, тобто у вигляді реалізації національної ідеї. Внаслідок цього пріоритетні політичні інтереси нації спрямовані на подальшу консолідацію спільноти, на створення чи збереження власної державності та налагодження відносин з іншими націями- державами.

Основним базовим національно-державним інтересом, геополітичним пріоритетом і стратегічним завданням зовнішньополітичного курсу України за умов глобалізації та євроінтеграції є її виживання, підвищення життєспроможності та зміцнення як вільної, суверенної, незалежної держави сучасного світу за умов збереження національних цінностей, захисту економічного та політичного суверенітету, власної соціально-культурної ідентичності, перетворення з об’єкта геополітичних ігор на повноцінний суб’єкт геополітики, тобто на самостійного гравця, який визначає свої цілі та дії на міжнародній арені.

Національні інтереси реалізуються державою через державні інтереси, які можуть мати самостійний характер (інтереси влади) і не збігаються з національними інтересами: наприклад, інтереси уряду чи інших елементів влади (законодавчої чи судової) бувають відмінними від національних інтересів.

Становлення системи національних інтересів України започатковане прийняттям Декларації про державний суверенітет України, Акту проголошення незалежності України від 24 серпня 1991 року, схваленого 1 грудня 1991 року всенародним голосуванням.

Фундаментальний національний інтерес, як зазначає Декларація про державний суверенітет України, «проголошує державний суверенітет України як верховенство, самостійність, повноту і неподільність влади Республіки в межах її території та незалежність і рівноправність у зовнішніх зносинах» і передбачає здійснення Україною як суб’єктом міжнародного права безпосередніх зносин з іншими державами: укладання з ними договорів, обмін дипломатичними, консульськими, торговельними представництвами, участь у діяльності міжнародних організацій в обсязі, необхідному для ефективного забезпечення національно-державного інтересу держави «у політичній, економічній, екологічній, інформаційній, науковій, технічній, культурній і спортивній сферах».

### 5.*2 Національні інтереси у сфері інформаційної безпеки: поняття та загальна характеристика*

Різні держави неоднаково успішно адаптуються до нових умов і глобальних викликів.

У цих умовах зазнає змін сфера втілення суверенітету держави – вона може розширюватися або звужуватися, переходячи на якісно нові рівні реалізації. Прискорена інтеграція національних економік у глобальні фінансові ринки, прозорість кордонів, зростання обсягів міжнародної торгівлі – всі ці та інші фактори поступово роблять держави дедалі взаємозалежнішими, змушуючи їх все частіше узгоджувати реалізацію своїх функцій з міждержавними організаціями політичного, економічного та військового спрямування.

При цьому збереження та зміцнення державного суверенітету не означає самоізоляції країни від міжнародного співтовариства, а навпаки створює сприятливі передумови для динамічного розвитку її відносин зі світом згідно із загальновизнаними нормами міжнародного права та власним розумінням своїх національних інтересів, на засадах взаємовигідного співробітництва та безпеки. В сучасному світі безпека неподільна, жодна держава не може забезпечити захист власних інтересів безпеки, спираючись виключно на власні ресурси.

Поняття «національні інтереси» є невід’ємним складовим елементом як системи національної безпеки, так і геополітики. У сучасній геополітиці під національними інтересами розуміють стратегічно важливі цілі, що їх ставить перед собою кожна держава, і засоби, за допомогою яких вона планує їх досягти.

Визначаючи, що «об’єктом забезпечення безпеки є інтереси безпеки», необхідно зазначити, що незалежно від рівня безпеки – національної, регіональної, міжнародної, – завжди об’єктом її забезпечення виступають інтереси того чи іншого суб’єкта і на сьогодні часто інтереси одного суб’єкта підміняються інтересами іншого. Так, національний інтерес в умовах глобалізації інколи підміняється гуманітарними інтересами або й інтересами «міжнародного співтовариства». Щодо визначення категорії «національний інтерес».

Історичний досвід і реальна практика переконливо свідчать, що успішному розвиткові будь-якої країни найбільшою мірою сприяє саме така політика, яка ґрунтується на національному інтересі.

Національний інтерес – це, по суті, інтегральне вираження інтересів усіх членів суспільства, що реалізується через політичну систему та поєднує інтереси кожної людини, інтереси національних, соціальних, політичних груп з інтересами держави.

Доволі цікавим є розуміння сутності національних інтересів американськими дослідниками Ч. Лерчем і А Саїдом, які вважають, що їх ціннісне наповнення ґрунтується на п'яти видах «добра»: 1) добро окремих громадян; 2) добро суспільства у цілому; 3) добро держави; 4) добро соціально зацікавлених груп у державі; 5) добро уряду і його членів.

Національний інтерес – категорія абстрактна та суб’єктивна, оскільки її параметри визначаються картиною світу та системою цінностей, що домінує в певному суспільстві та державі. Як зазначав М. Комін, «національний інтерес є інтерес нації як двоєдності суверенної територіальної держави та громадянського суспільства». Що стосується державного інтересу, то він «не тільки пов’язаний з поняттям національного інтересу, але в значній мірі визначає його смислову структуру».

В науковій літературі наводяться різні визначення поняття «національний інтерес». Узагальнюючи їх, зазначимо:

По-перше, категорія «інтерес» не існує сама по собі і є частиною тріади: цінності, інтереси і цілі. Отже, стосовно особи – цінності, інтереси і цілі особи; стосовно держави – це національні інтереси, національні цінності, національні цілі; стосовно світового співтовариства – цінності, інтереси і цілі світового співтовариства.

По-друге, пропонуємо національні інтереси визначати як інтегральний вираз інтересів більшості членів суспільства, держави, що є похідними від загальновизнаних базових цінностей і реалізуються через національно-правову систему відповідної держави

законодавчою, виконавчою та судовою гілками влади.

По-третє, суть національних інтересів пропонуємо визначити як необхідність в забезпеченні необмеженого в часі безпечного існування держави в якості самостійного суб'єкта, постійного зростання усіх складових могутності країни – політичної, економічної, військової, наукової тощо, а також стійкого розвитку особи, суспільства. При цьому в якості незмінного постійного змісту національного інтересу необхідно виділити задачу забезпечення безпеки держави, основний обов'язок якої – безпека, розвиток особи і суспільства.

*Українські національні інтереси* – це життєво важливі матеріальні, інтелектуальні і духовні цінності українського народу як носія суверенітету й єдиного джерела влади в Україні, визначальні потреби суспільства і держави, реалізація яких гарантує державний суверенітет країни та її прогресивний розвиток. У цьому розумінні національні інтереси є найважливішими завданнями внутрішньої і зовнішньої політики.

За своєю спрямованістю національні інтереси зорієнтовані на забезпечення виживання та прогресивний розвиток і певною мірою лідерства особи, суспільства, держави. Тільки крізь призму їх реалізації та захисту можуть і повинні розглядатися проблеми створення системи національної безпеки, її головна мета, цілі, завдання, принципи функціонування, усі внутрішні параметри.

Серед основних складників національних інтересів можна виділити три найважливіших (рис. 5.1).

Рис. 5.1 – Складові національних інтересів

Основні складники національних інтересів впливають на стан нації, можливості та перспективи її розвитку і, таким чином, на розуміння та визначення національних інтересів. Відповідно до цього, у розумінні сутності національних інтересів країни велике значення має геополітичне та геостратегічне уявлення про її місце і роль у світі.

Геополітичні реалії, які віддзеркалюють посилення взаємозалежності всіх суб'єктів міжнародних відносин, об'єктивно підвищують значення і роль загальнолюдського чинника в геополітичному просторі. Вищезазначене змушує Україну, як і інші держави світу, виробляти у зовнішній політиці такі правила поведінки, які були б адекватними сучасній геополітичній ситуації. Проте ця обставина аж ніяк не означає зневажання чи приниження ролі національних інтересів, так само як і відмову від боротьби за їх реалізацію. Без урахування культурно-історичних традицій і національних цінностей розуміння міжнародних відносин не

може бути повним.

У загальному вигляді національні інтереси України – це усвідомлені суспільством і виражені в Конституції України та інших нормативно-правових актах конституційного рівня у вигляді програмних цільових настанов життєво важливі потреби існування та розвитку природи, людини, соціальної групи, суспільства, держави. Із цього погляду національні інтереси – це фундаментальні цінності народу. Саме тому Законом України «Про національну безпеку України» 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».

На сучасному етапі розвитку Українська держава зіткнулася із загрозами та викликами, які потребують негайного вирішення, найбільш актуальними з яких є:

– військова агресія, участь регулярних військ, радників, інструкторів і найманців у бойових діях на території України;

– розвідувально-підривна і диверсійна діяльність, дії, спрямовані на розпалювання міжетнічної, міжконфесійної, соціальної ворожнечі і ненависті, сепаратизму і тероризму, створення і всебічна підтримка, зокрема військова, маріонеткових квазідержавних утворень на тимчасово окупованій території частин Донецької,Луганської та Запорізької областей;

– нарощування військових угруповань біля кордонів України та на тимчасово окупованій території країни, у тому числі й перспектива розміщення на півострові Крим тактичної ядерної зброї;

– інформаційно-психологічна війна, приниження української мови і культури, фальшування української історії, формування російськими засобами масової комунікації альтернативної до дійсності викривленої інформаційної картини світу.

У цьому контексті для України першочерговими стратегічними завданнями державної політики національної безпеки є відновлення територіальної цілісності країни та сукупності демократичних інститутів на усій її території, консолідація української політичної нації, формування загальнонаціональної ідентичності, єдності всіх громадян України та усіх її регіонів, реінтеграція тимчасово окупованих територій після їх звільнення.

Суттєвою характеристикою національних інтересів є їх усвідомленість. Усвідомлення всезагальності національних інтересів і необхідності їх узгодженої реалізації перетворює останні в найважливіший орієнтир поточної діяльності держави.

Зауважимо, що поняття «національні інтереси» відбиває внутрішній суспільний консенсус, який об'єднує в єдине ціле різних в усіх відношеннях людей. Набуваючи в міру поступального розвитку нації все більш універсального для неї сенсу, легітимні політичні механізми формування національних інтересів стають осьовими елементами національної ідеї – системи цінностей, що визначають архетипні риси і невід'ємні характеристики національної спільноти та відбивають культурну спадкоємність в її духовній історії.

Отже, національні інтереси, незважаючи на розвиток глобалізаційних процесів, посилення взаємозалежності країн унаслідок загострення глобальних проблем, зростання ролі інтеграційних об'єднань та їх впливу на внутрішню політику держав, продовжують відігравати вирішальну роль у формуванні державної політики, визначенні стратегії їх діяльності. Отже, захист національних інтересів є домінантною основою забезпечення національної безпеки країни, що, своєю чергою, передбачає необхідність глибокого аналізу та врахування геополітичного фактору і визначення на цій підставі стратегії держави.

### *5.3 Інтереси особи, суспільства та держави в інформаційній сфері*

Інформація, яка охоплює всі сфери життєдіяльності суспільства, створює умови

інформаційної нерівності, коли розподіляється відповідно до соціально-статусних, ресурсних та матеріальних чинників, а така нерівність значною мірою зумовлює виникнення інформаційних ризиків, порушення інформаційної безпеки. Це, зокрема, стосується негативних впливів окремих інформаційних ресурсів маніпулятивного характеру, вторгнення в особистісний інформаційний простір, кібернетичної злочинності та інших порушень інформаційних прав людини. Таким чином, інформаційна безпека людини, суспільства й держави в усіх її аспектах є найважливішою світовою цінністю інформаційної епохи.

Розвиток інформаційного суспільства – це не лише матеріалізація технологічних досягнень в інформаційній сфері, а передусім прогрес самої соціальної структури людської спільноти, котра прагне до все повнішого задоволення своїх потреб у цій царині. Втім, розбудова інформаційного суспільства ще більшою мірою зумовлена еволюцією людини як носія соціальних цінностей, розвитком творчих потенцій особи, її здатності до критичного мислення, зростанням індивідуалізації, обсягів особистих та громадянських прав і свобод, демократичних основ організації суспільного життя, формуванням інформаційної культури.

Національні інтереси в інформаційній сфері значною мірою зумовлені наявністю відповідних загроз. Зміст цих загроз визначається чинниками шкідливого впливу на об’єкти національних інтересів в інформаційній сфері, до яких належать інформація, інформаційна інфраструктура, правовий статус суб’єкта в інформаційній сфері.

Національні інтереси в інформаційній сфері можна визначити як природну потребу людини, суспільства й держави в такому стані цієї сфери, який забезпечує їх стабільне існування, функціонування та сталий розвиток. Отже, весь комплекс питань, пов’язаних із формуванням системи національної безпеки, є її головною метою, завданнями, принципами та механізмами функціонування, тому має розглядатися виключно в контексті реалізації та захисту національних інтересів.

Деякі фахівці, проводячи класифікацію національних інтересів, пропонують їх певну ієрархію. Так, американські теоретики Р. Яргер та Дж. Барбер визначають національні інтереси за чотирма категоріями: (захист країни; економічний прогрес; гармонійний розвій суспільства; забезпечення продуктивної участі країни у світовому розподілі праці) та трьома рівнями пріоритетності (важливості, вагомості):

- життєво важливі (їх недотримання одразу спричинить загрозу засадничим національним інтересам);
- важливі (їх недотримання може викликати серйозні загрози найвагомішим національним інтересам);
- периферійні (їх недотримання може завдати значної матеріальної та іншої шкоди без прямої загрози найважливішим національним інтересам).

Окремі дослідники обстоюють також позицію, за якою для формування стратегії національної безпеки потрібна побудова ієрархії пріоритетів національних інтересів держави, яка, на їхню думку, дасть змогу уникнути невідповідності між декларованою метою та засобами її матеріалізації. Доцільність розроблення такої ієрархії, її законодавчого закріплення вбачається досить сумнівною, адже пріоритети національних інтересів в інформаційній сфері вельми варіативні в часі, зумовлюються оперативною обстановкою та іншими чинниками. Крім того, кожен окремий випадок потребує вироблення відповідної тактики й застосування специфічних засобів реалізації.

Наприкінці XX ст. відомий український філософ та безпекознавець Б. Пархонський зазначав, що стратегічні національні інтереси формуються відповідно до вибраного суспільством і державою курсу розвитку на тривалий період. Проте під впливом зміни історичних умов вони можуть модифікуватися. Як прогнозував учений, у XXI ст. ситуація змінюватиметься вельми динамічно, оскільки економічний та технологічний розвиток усе

більшою мірою визначатиметься інтелектуальним та духовним чинниками, що може радикально змінити геополітичну ситуацію.

Отже, ефективність реалізації визначених у Доктрині інформаційної безпеки України національних інтересів в інформаційній сфері значною мірою зумовлюється законодавчим визначенням національних цінностей, що потребує подальшого розроблення національних (державних) інтересів. Національні цінності та інтереси формують національні цілі .

Зміст Доктрини інформаційної безпеки України стосується лише національних інтересів в інформаційній сфері. Таким чином, законодавчого визначення потребують передусім національні цінності в інформаційній сфері, а вся наведена вище тріада має стати чітким орієнтиром формування здійснення та вдосконалення відповідної державної політики.

Американські військові дослідники Ярґер Річард та Джордж Барбер, розглядаючи цю тріаду в системі забезпечення національної безпеки держави, визначають національні цінності як найменш рухомий і найстабільніший елемент системи. Цінності формуються під час історичного процесу, розвитку матеріальної та духовної культури суспільства, відповідають геополітичному спрямуванню країни.

Національні інтереси – це елемент порівняно динамічний, що формується на основі національних цінностей під впливом довгострокових тенденцій суспільного розвитку. Національні цілі – це найбільш рухливий елемент.

Б. Гогвуд та Л. Ган національні цінності розглядають як переконання, мораль, стандарти та більш специфічні норми, котрі впливають на процес вироблення політики на всіх рівнях (індивідуальному, груповому, організаційному та суспільному) через спрямування та стримування поведінки та дій учасників процесу творення політики, впливаючи на їхнє сприйняття бажаного кінцевого стану (кінцевих цінностей) та прийнятних засобів (інструментальних цінностей) для його досягнення.

До цього твердження слід додати важливу засторогу відомого соціолога М. Вебера стосовно того, що кожна історична епоха має свою систему цінностей, тобто це категорія є принципово історичною.

До національних цінностей в інформаційній сфері відносять систему духовних та матеріальних цінностей людини, суспільства й держави, котрим притаманні виразні ознаки, зокрема світоглядні, соціально-економічні, культурні, демографічні, географічні. Ця система становить правовий та філософсько-етичний базис подальшої еволюції суспільства й держави, сприяє формуванню національної мети, що стоїть перед державою в інформаційній сфері. Таким чином, з огляду на сутність і, відповідно, вагомість національних цінностей в інформаційній сфері як найбільш специфічного сегменту системи вони потребують особливого захисту.

До національних цінностей в інформаційній сфері з огляду на сучасний стан державотворення в Україні слід віднести матеріальний добробут населення, зокрема на основі розвитку ІКТ; інформаційну захищеність людини, суспільства, держави; духовність; доступність віросповідання, запобігання релігійному фанатизму та екстремізму, неприпустимість використання релігії як психологічного чинника тероризму, розвиток традиційних українських релігійних напрямів; мову як основний ідентифікатор нації, засіб передачі інформації та знань, пам’ять поколінь; культуру інформаційних відносин; свободу інформації; захищеність інформаційних прав людини, доступ до інформації, нейтралізацію негативних інформаційних впливів.

Соціально-економічний складник інформаційної безпеки є засадничим у структурі національних цінностей в інформаційній сфері, тому є всі підстави стверджувати, що базова категорія економічної політики держави «матеріальний добробут» має стати такою ж складовою частиною інформаційної безпеки держави, тим паче національної безпеки України.

З огляду на зазначене можемо припустити, що критерієм ефективності забезпечення інформаційної безпеки має бути високий рівень безпеки за мінімуму відповідних затрат.

Запропонована вище схема взаємозв'язку національних цінностей, інтересів цілей і надбань в інформаційній сфері доводить думку про те, що національні цінності є головним критерієм оцінки негативного впливу на інформаційну безпеку держави. Їх недотримання, порушення, спотворення чи нехтування можуть істотно зашкодити стану захищеності людини, суспільства, держави, нації в інформаційній сфері.

Основними національними цілями в інформаційній сфері вбачаються такі:

– духовна безпека – усунення й недопущення деструктивних впливів на світоглядні позиції людей і суспільну свідомість, здійснюваних шляхом пропагування фальшивих цінностей, навіювання хибних пріоритетів, завдань і цілей окремим особам та суспільству загалом;

– військова безпека – упровадження інформаційних технологій у військову сферу, а також їх захист;

– економічна безпека – підвищення темпів розроблення та впровадження у суспільно-економічну сферу новітніх конкурентоспроможних інформаційно-комунікативних технологій;

– соціальна безпека – досягнення належного рівня інформаційної культури суспільства;

– екологічна безпека – формування загальнодержавної інформаційної системи постійного екологічного моніторингу;

– сприяння інтегруванню національної інформаційної інфраструктури у відповідну світову інфраструктуру;

– удосконалення й посилення захисту прав людини в інформаційній сфері;

– організація невідкладних заходів для створення високої репутації України в умовах інформаційної глобалізації, а також для формування відповідного позитивного іміджу.

Таким чином, національні цілі визначають національні надбання в інформаційній сфері. З огляду на потужний прогрес інформаційних технологій, їх істотний вплив на весь комплекс суспільних відносини та всі сфери життєдіяльності соціуму, зокрема економіку, оборону, охорону здоров'я, низка здобутків вітчизняної інформаційної галузі є безперечно національним надбанням. Зауважимо, що ці надбання слугуватимуть певним показником, індикатором ефективності реалізації національних цілей в інформаційній сфері.

### *5.4 Інформаційна безпека держави в умовах обмежень прав і свобод громадян у період воєнного стану*

Однією з відправних позицій оцінки обмежень прав людини є вимога юридичної визначеності – обмеження встановлюються законом, закон має бути доступним, а застосування обмежень на практиці припустиме лише за умови їх передбачуваності. В умовах правового режиму воєнного стану, через утворення нових владних суб'єктів і оперативну зміну розподілу повноважень, можливості застосування державного примусу на розсуд адміністрації збільшується, що за відсутності належного контролю створює передумови для можливих порушень прав людини.

У цьому контексті проблема правової визначеності повноважень відповідних суб'єктів, обсягів і процедур запроваджених обмежень прав людини постає дуже гостро. Ця проблема додатково посилюється в контексті обмеження інформаційних прав, які, по-перше, є різними за характером (як позитивні, так і негативні) та механізмами забезпечення, по-друге, нові інформаційні права ще не мають усталеного юридичного змісту, що ускладнює дотримання принципу пропорційності обмежень, і, по-третє, свобода інформації, є визнаним ООН критерієм здійснення усіх прав людини.

Тому обмеження інформаційних прав в сучасному інформаційному суспільстві безпосередньо впливає на можливості реалізації усіх інших прав людини. Ведення Україною захисту своїх територій від масштабної збройної агресії рф продемонструвало, що в цих складних умовах ефективна реалізація низки інформаційних прав, (зокрема доступу цивільного населення та Сил оборони до Інтернету і цифрових технологій, надійної комунікації), здатна істотно впливати на хід бойових дій, не тільки згуртовуючи і мотивуючи, а й сприяти виявленню та знищенню окупаційних військ, а також фіксації військових злочинів. Отже значення відповідності обмежень інформаційних прав людини засадам міжнародного права і принципам верховенства права, навіть в умовах воєнного стану, в правовій демократичній державі не може ні ігноруватися, ні применшуватися.

Конституційний Суд України тлумачить обмеження прав людини здебільшого як «звуження змісту та обсягу конституційних прав і свобод». Імовірно через особливості такого формулювання в українській науковій літературі обмеження прав людини часто-густо подаються в контексті зменшення можливостей особи щодо певного обсягу дій, обмеження її поведінки.

Обмеження позитивного права виявляється у звуженні його юридичних меж, а негативного – в законному розширенні меж втручання в це право з боку держави, що в повній мірі стосується обмежень інформаційних прав. При цьому, через специфіку методів державної діяльності якою обмежуються негативні інформаційні права (передусім, право на приватність), такі обмеження здебільшого залишаються прихованими від особи, права якої обмежуються, що на практиці ускладнює контроль їх легітимності і пропорційності.

Запровадження будь-яких обмежень прав людини має ґрунтуватися на відповідних уявленнях про їх допустимість.

Так, ст. 8 «Заходи правового режиму воєнного стану» Закону України «Про правовий режим воєнного стану» надає військовому командуванню та військовим адміністраціям (у разі їх утворення) повноваження запроваджувати низку заходів в межах допустимих тимчасових обмежень прав людини, зокрема інформаційних прав, закріплених ст. 31, 32, 34 Конституції України.

Серед цих заходів є такі, що можуть обмежувати право людини на свободу думки і слова, на вільне вираження своїх поглядів і переконань (позитивне право, яке ґрунтується на свободі дій) шляхом звуження можливостей і здійснення додаткового контролю інформаційної діяльності, а саме:

1) заборона проведення мирних зборів, мітингів, походів і демонстрацій, інших масових заходів (п. 8 ч. 1 ст. 8 Закону України «Про правовий режим воєнного стану»)

2) упорядкування інформаційної діяльності різних суб’єктів відповідно до умов воєнного часу, зокрема щодо використання їх матеріально-технічних можливостей (місцевих радіостанцій, телевізійних центрів, друкарень) для військових потреб і проведення роз’яснювальної роботи, а також можливість заборони передавання інформації через комп’ютерні мережі та використання приймально-передавальних радіостанцій особистого і колективного користування (п. 11, 12 ч. 1 ст. 8 Закону України «Про правовий режим воєнного стану»).

Прикладом безпосередньої реалізації і конкретизації обмежень інформаційних прав людини в межах цих заходів є встановлена військовим командуванням і офіційно оголошена тимчасова заборона використання автомобільних реєстраторів з метою протидії розголошенню критично важливої в воєнних умовах інформації.

Слід зауважити, що характер встановлення рамок допустимої інформаційної діяльності мають також додаткові заборони запроваджені Кримінальним кодексом України у зв’язку з удосконаленням правового регулювання в умовах воєнного стану, зокрема щодо

колабораціонизму (ст. 1111 Кримінального кодексу України) та несанкціонованого поширення інформації про дії Сил оборони (ст. 1142 Кримінального кодексу України).

Однак, в цьому разі, такі законодавчі новели є засобами кримінально-правової охорони і їх необхідно вважати не обмеженнями права людини на свободу вираження поглядів і переконань, а уточненням (фіксацією) юридичних меж цього права в умовах воєнного або надзвичайного стану, які і визначають рівний незмінний для всіх масштаб інформаційної свободи.

Обмеження прав людини негативного характеру, якими є право на повагу до приватного і сімейного життя та право на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції (ст. 31, 32 Конституції України), в наявних нормативних умовах вже не будуть такими явними і передбачуваними, оскільки межі і способи обмежень цих прав безпосередньо не випливають із системи заходів правового режиму воєнного стану, визначених Законом України «Про правовий режим воєнного стану».

Відповідно, якщо обмеження цих прав дійсно застосовуються як додаткові в умовах правового режиму воєнного стану, а не тільки залишаються можливими відповідно до переліку потенційно обмежуваних прав, оцінка їх правомірності може бути доволі неоднозначною.

Невизначеною також є ситуація щодо пропорційності обмеження нових неконституалізованих інформаційних прав, які наразі не мають визнаних юридичних меж, хоча очевидно можуть обмежуватися заходами правового режиму воєнного стану, як, приміром, ключове з «цифрових прав» – право на доступ до Інтернету.

## ПИТАННЯ ДЛЯ САМОПЕРЕВІРКИ

1. Формування яких життєво важливих інтересів відбувається протягом історичного становлення нації-держави як суб’єкта міжнародного права?
2. Надайте загальну характеристику національних інтересів у сфері інформаційної безпеки.
3. Охарактеризуйте національні інтереси як реалізацію природного права народу на самостійне існування.
4. На Вашу думку, що саме виступає певними концептуальними, ідеологічними основами, консолідуючими чинниками, важливими життєвими орієнтирами на шляху ефективного суспільного розвитку?
5. Обґрунтуйте взаємозв’язок національних цінностей, інтересів цілей і надбань в інформаційній сфері.
6. Визначте основні національні цілі в інформаційній сфері нашої держави.
7. Якою має бути інформаційна безпека держави в умовах обмежень прав і свобод громадян у період воєнного стану?

# ЛЕКЦІЯ 6
# НАЦІОНАЛЬНИЙ ІНФОРМАЦІЙНИЙ СУВЕРЕНІТЕТ ТА ДЕРЖАВНА ІНФОРМАЦІЙНА ПОЛІТИКА

**План викладу:**

6.1 Сутність поняття «суверенітет». Національний інформаційний суверенітет.

6.2 Інформаційний та електронний суверенітет: основні завдання забезпечення інформаційного суверенітету.

6.3 Державна політика, державна інформаційна політика, державна політика забезпечення інформаційної безпеки: сутність та співвідношення

6.4 Сучасні та потенційні проблемні питання правового забезпечення інформаційного суверенітету та можливі шляхи їх вирішення

6.5 Інформаційна безпека як глобальна проблема захисту інформації, інформаційного простору, інформаційного суверенітету країни та інформаційного забезпечення прийняття урядових рішень.

6.6 Проблеми забруднення інформаційного простору неправдивою інформацією.

## *6.1 Сутність поняття «суверенітет». Національний інформаційний суверенітет*

До формування поняття «інформаційний суверенітет» доцільно підходити, виходячи з того, що *суверенітет* - 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. 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 часі 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.

Більшість вітчизняних дослідників 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.

Відтак, 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.

Інформаційному суверенітету притаманні принципи: законності; принцип 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.

Для належного забезпечення державою інформаційного суверенітету необхідним є: 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.

### *6.2 Інформаційний та електронний суверенітет: основні завдання забезпечення інформаційного суверенітету*

Сучасне розуміння суверенітету держави відрізняється багатоманітністю та, крім правового або політикоекономічного аспектів, нерозривно пов'язане із сучасними інтеграційними процесами як самої держави, так і суспільства в цілому. Трансформація правового простору сьогодні має наддержавний характер, не обмежений територіальними кордонами, що, у свою чергу, обумовлюється не тільки існуванням міждержавних та наддержавних утворень, а й значним розширенням можливостей інтерактивної комунікації між різними суб'єктами права за допомогою новітніх інформаційних технологій та мережі Інтернет.

Інформаційний суверенітет передбачає проведення незалежної інформаційної політики, контроль за інформаційними мережевими потоками за умови забезпечення свободи слова, права на приватність та права населення на отримання достовірної інформації. Структура інформаційного суверенітету не відрізняється однорідністю.

*Цифрова складова*: раніше ідея цифрового суверенітету асоціювалася з політикою авторитарних держав, де шляхом жорсткого контролю за інформаційними технологіями ці політичні режими намагалися захиститися від впливів глобалізованого світу. Однак збільшення впливу цифрових технологій на політику держав дало підстави розглядати проблему цифрового суверенітету в аспекті складової суверенітету інформаційного, адже бурхливий розвиток ринку цифрових технологій суттєво вплинув на якість забезпечення національної та міжнародної безпеки в умовах уже сформованого єдиного інформаційного простору.

*Віртуальна складова*. Розуміння її сутності останнього пов'язане із суверенітетом у кіберпросторі. Підходи до розуміння сутності кіберпростору в аспекті питань суверенітету держави різняться. По-перше, це умовність кіберпростору, що виключає його юрисдикційність. З огляду на відкритість, доступність та повсюдність кіберпростору його слід розглядати як загальне надбання, що не підлягає суверенітету будь-якої держави або групи держав, на кшталт космічного простору. По друге, кіберпростір не є визначеним

місцем, це простір віртуальний, що знаходиться поза фізичним виміром і часом, проте водночас він може бути сферою застосування кіберсили, спроможної нести загрозу державному суверенітету.

Він не може бути відокремленим від суверенітету, остільки держави володіють суверенітетом над кіберінфраструктурою, що забезпечує його існування. Також має місце державна присутність у кіберпросторі за допомогою фінансової, банківської та інших систем. Вважаємо, що проблема віртуального суверенітету суттєво ускладнюється технічними можливостями забезпечення з боку держави. Але нездатність встановити всеохоплюючий контроль над віртуальною реальністю не означає нездатності утворювати власні ресурсні його складові та захищати свої суверенні права щодо державних об'єктів у кіберінфраструктурі.

*Медійна складова* в її класичному розумінні (радіо, телебачення друковані ЗМІ), мабуть, є однією з найбільш реалізованих у плані технічних можливостей забезпечення функціонування власної структури, її можливостей стосовно пошуку, фільтрації, блокування та розповсюдження інформації. Проте захист інформаційного суверенітету в цій сфері повинен базуватися на законодавчій основі та відображати напрацьовану стратегію розвитку.

Одним із важливих елементів інформаційного суверенітету є його *інтелектуальна складова*. Як така вона охоплює різні сторони інтелектуального життя та різних суб'єктів – носіїв інтелекту. В умовах єдиного інформаційного простору, коли інформація є товаром, а роль результатів інтелектуальної діяльності набула неабиякого значення для розвитку суспільства і держави, актуальними, на нашу думку, постають такі проблеми:

– проблема інтелектуального суверенітету держави, що прямо залежить від рівня її інтелектуального потенціалу;

– проблема інтелектуального суверенітету народу, пов'язана з освітою та її відповідністю сучасним науковим знанням;

– проблема інтелектуального суверенітету окремих соціальних груп та людини в аспекті створення належних умов для розвитку їхніх інтелектуальних можливостей взагалі та інтелектуальної еміграції зокрема.

– проблема підходів до розуміння меж та перспектив подальшої трансформації штучного інтелекту та тих наслідків, що можуть суттєво вплинути на майбутнє в цілому.

*Ідеологічна складова інформаційного суверенітету*. Цілі, завдання та функції будь-якої сучасної держави базуються на певних теоретичних, свідомісних конструкціях, ідеологічних настановах тощо. Україна не є виключенням. Вона чітко окреслила основи домінуючої державної ідеології в Основному законі. Це, передусім, ідеї розбудови демократичної, соціально-орієнтованої та правової держави, де усі люди є вільними і рівним у своїй гідності та правах, мають право на свободу думки і слова, на вільне вираження своїх поглядів і переконань, а народ виступає носієм суверенітету та єдиним джерелом влади.

*Культурологічна складова інформаційного суверенітету*. Будь-яка інтерпретація трансформаційних реалій розповсюдження інформації в сучасному світі в їхньому впливі на державний суверенітет не відкидає урахування культурологічних чинників суспільства, котрі ґрунтуються як на його цивілізаційній приналежності, так і на історичній спадщині та культурі. Можна стверджувати, що в Україні культурологічну складову суверенітету закріплено у преамбулі Основного Закону, де підтверджено європейську ідентичність Українського народу, а також у статтях, де зазначається розвиток історичної свідомості, традицій і культури, а також розвиток етнічної, культурної, мовної та релігійної самобутності всіх корінних народів і національних меншин України (ст. ст. 10-12, 35).

Невід'ємною складовою інформаційного суверенітету виступає *політичний імідж держави*. На наш погляд, іміджеву складову інформаційного суверенітету слід розуміти як цілеспрямовано або стихійно сформований образ держави на основі соціальнопсихологічних,

моральних та ціннісних аспектів розвитку суспільства, що відображає ефективність державних структур, легітимність державної влади, авторитет на міжнародній арені, ступінь відкритості та об'єктивності у взаємовідносинах із суспільством, можливість ефективного громадського контролю над політикою держави та рівень патріотизму її населення.

Іміджеву складову інформаційного суверенітету слід розуміти як цілеспрямовано або стихійно сформований образ держави на основі соціально-психологічних, моральних та ціннісних аспектів розвитку суспільства, що відображає ефективність державних структур, легітимність державної влади, авторитет на міжнародній арені, ступінь відкритості та об'єктивності у взаємовідносинах із суспільством, можливість ефективного громадського контролю над політикою держави та рівень патріотизму її населення.

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. Термін цифровий суверенітет вперше був популяризований у маніфестах конфіденційності, спрямованих на отримання більшого індивідуального контролю над особистою інформацією, що поширюється через соціальні мережі та в контексті споживачів Інтернету. Це допомогло стимулювати нещодавній Загальний регламент Європейського Союзу про захист даних (GDPR) та Рамку захисту конфіденційності США та ЄС.

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). 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.

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;
- розвиток власного контенту та технологічної інфраструктури;
- створення кіберозброєнь, проведення інформаційних спеціальних операцій та інформаційних війн;
- запобігання, виявлення і нейтралізація внутрішніх та зовнішніх інформаційних загроз;
- 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 тощо.

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

- наповнення національного інформаційного простору якісною інформацією, розвиток національного книговидання;
- наповнення вітчизняного сегмента Інтернету і впорядкування його діяльності;
- реалізація конституційних прав і свобод громадян, суспільства і держави на інформацію;
- формування та захист інтересів України у світовому інформаційному просторі й міжнародних інформаційних відносинах;
- створення потужних інформаційних потоків, що підтримуватимуть національну систему символів, установок, переконань та стереотипів, а також забезпечуватимуть їхню експансію у навколишній світ (за принципом «діяпротидія») тощо.

### *6.3 Державна політика, державна інформаційна політика, державна політика забезпечення інформаційної безпеки: сутність та співвідношення*

Державна політика є одним із важливих компонентів життєдіяльності суспільства, оскільки її заходи спрямовуються на поліпшення рівня проживання громадян та гарантування соціальної стабільності країни і її регіонів.

У наукових дослідженнях з державного управління представлено декілька підходів до визначення державної політики. Так, 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.

Тобто, 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).

Відповідно до Закону України «Про інформацію» *державна інформаційна політика* –

це сукупність основних напрямів і способів діяльності держави з одержання, використання, поширення та зберігання інформації.

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; розвиток національної інформаційної інфраструктури; 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, Ебанкінг, 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 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 соціальнопсихологічного 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.

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. Відповідно, діяльність із забезпечення інформаційної безпеки держави можна поділити на три основні напрями: державно-управлінський, техніко-технологічний та соціально-змістовний (Таблиця 6.1).

Таблиця 6.1

Напрями забезпечення інформаційної безпеки держави

| державно-управлінський | техніко-технологічний | соціально-змістовний |
|---|---|---|
| - реалізація державної політики інформаційної безпеки та забезпечення інформаційного суверенітету України.<br>- Законодавче визначення стратегічних напрямів забезпечення інформаційної безпеки та їх реалізація.<br>- Удосконалення державного регулювання розвитку інформаційної сфери, протидія її монополізації.<br>- Належне інформаційне забезпечення прийняття державно-управлінських рішень.<br>- Постійна відкрита інформаційна взаємодія між державною владою і громадянським суспільством (е-уряд, е-демократія).<br>- Забезпечення урядового зв'язку і Національної системи конфіденційного зв'язку.<br>- Участь у міжнародному співробітництві у сфері інформаційної безпеки.<br>- Протидія поширенню інформації, що містить заклики до зміни конституційного ладу та кордонів держави, | - Забезпечення інноваційного потенціалу країни через впровадження новітніх технологій в інформаційній сфері.<br>- Підтримка вітчизняних виробників засобів інформатизації та захисту інформації, створення передумов для підвищення їх конкурентоспроможності на світовому та національному ринках.<br>- Стандартизація, сертифікація і ліцензування засобів інформатизації та захисту інформації.<br>- Розвиток національного інформаційного простору, створення умов для його інтегрування у світовий інформаційний простір.<br>- Розвиток, ефективне використання та захист національної інформаційної інфраструктури.<br>- Розвиток, ефективне використання та захист інформаційних ресурсів, забезпечення вільного доступу до них, формування системи національних електронних ресурсів. | - Наповнення національного інформаційного простору якісним вітчизняним інформаційним продуктом, забезпечення потреб громадян у якісній, повній і достовірній інформації для їх життєдіяльності, освіти та розвитку.<br>- Поширення у світовому інформаційному просторі достовірної інформації про Україну, розвиток іномовлення.<br>- 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.<br>- Захист від маніпулювання інформацією та дезінформування, деструктивних впливів на свідомість, підсвідомість і психіку як індивіда, так і суспільства в цілому. |

| | | |
|---|---|---|
| міжнаціо-нальної та міжконфесійної ворожнечі.<br>- Запобігання та протидія інформаційній експансії інших держав, інформацій-ному тероризму, використан-ню інформаційної зброї.<br>- Ведення активної розвідувальної, контр-розвідувальної і оперативно-розшукової діяльності з метою забезпечення інформаційної безпеки. | - Управління вітчизняним сегментом мережі Інтернет. - Технічний та криптографічний захист інформації з обмеженим доступом (службової інформації та інших видів конфіденційної інформації, державної таємниці).<br>- Запобігання та протидія правопорушенням в інформаційній сфері, комп'ютерним злочинам. | - Забезпечення приватності життя громадян, захист персональних даних.<br>- Захист суспільної моралі, духовної, культурної та мовної самобутності.<br>- Запобігання та протидія поширенню інформації, що пропагує агресію, насильство, наркоманію, алкоголізм та інші негативні суспільні явища. |

***6.4 Сучасні та потенційні проблемні питання правового забезпечення інформаційного суверенітету та можливі шляхи їх вирішення***

Зростанням протягом останніх 5-10 років загроз, що стають наслідком стрімкої інформатизації у всьому світі, змушують держави більш уважно поставитись до власної безпеки на цьому напрямі. Все частіше навіть в роботах західних дослідників згадується необхідність побудови того, що умовно може бути названо «інформаційний суверенітет» (хоча західні дослідники частіше використовують поняття «кібермогутність», однак її принципові характеристики швидше відповідають саме проблематиці «інформаційного (кібер) суверенітету»). Прикметно, що на відміну від пострадянських досліджень в сфері інформаційної безпеки (які сконцентровані переважно навколо інформаційно-психологічних елементів) західні дослідники концентруються, передусім, на технологічній складовій.

Тим більше, що убезпеченість контентної складової все більше залежить від технічної. Це стало особливо очевидним після викривальних заяв Е. Сноудена щодо масштабів шпигунської діяльності АНБ США. При чому ця діяльність здійснювалась на всіх рівнях: починаючи від традиційного прослуховування розмов та збору персональних даних мільйонів громадян і закінчуючи створенням (за попередньою домовленістю з IT-корпораціями) спеціальних «бекдорів» в програмному забезпеченні та навіть в чіпах.

Дискусійним є питання щодо того, в якому саме форматі мають бути сформульовані засади «інформаційного суверенітету». Однак, практика нормативно-правового забезпечення питань національної безпеки в Україні (її стратегічних пріоритетів, а не повноважень конкретних відомств) багато в чому залишається декларативною та мало дієвою.

Крім того, «інформаційний суверенітет» є складним і поліаспектним явищем (яким власне є і більш традиційний суверенітет держави). Окремі його положення (які ще мають бути визначені) швидше за все вже частково закріплені у чинному нормативно-правовому полі. Відповідно буде вкрай складно створити новий окремий Закон України, який а) не буде конфліктувати із чинним законодавством і б) зможе його повноцінно врахувати. Тим більше, що крім окремих Законів України, вже спрямованих на досягнення елементів «інформаційного суверенітету», є певна множина різноманітних державних цільових програм, науково-дослідних робіт тощо, які виконуються в державі протягом тривалого часу.

Таким чином, фактично державна політика щодо забезпечення «інформаційного суверенітету» має бути визначена не стільки на рівні окремого Закону України, скільки Стратегії чи Плану Дій, який би міг узагальнити ключові напрями діяльності держави на цьому напрямі (зокрема, діяльність державних цільових програм чи національних проектів) та виявити ключові показники, які мають бути досягнуті.

Зважаючи на комплексність та системність цього документу, а також його потенційного

впливу на життя практично кожного громадянина, швидше за все він має пройти суттєве громадське обговорення, задля мінімізації можливого негативного сприйняття з боку суспільства.

Україна, як і більшість світових держав, стикається з об'єктивною загрозою деформування власного суверенітету в інформаційному (цифровому) просторі. Ціла низка потужних держав вкладають значні кошти у створення кіберозброєнь, проведення інформаційних спеціальних операцій та інформаційних війн. Все це суттєвим чином впливає на безпекове середовище, в якому Україна має проводити політику відповідно до власних національних інтересів.

Протягом 90-х років XX сторіччя в Україні було здійснено принаймні декілька спроб вирішити цю проблему на нормативно-правовому рівні. Було розроблено два проекти Закону України «Про інформаційний суверенітет та інформаційну безпеку України», однак жоден з них так і не дійшов до предметного обговорення та прийняття парламентом. Останні завдання щодо розробки такого закону відносяться до 2003 р., а «Доктрина інформаційної безпеки України» згадує проблему «інформаційного суверенітету» лише побіжно.

Водночас стрімке зростання залежності України (у всіх сферах життєдіяльності) від ефективності функціонування ключових інформаційних систем та убезпечення даних у таких системах від стороннього несанкціонованого доступу знов актуалізує проблему концептуалізації поняття «інформаційний суверенітет» та розробки відповідної державної політики щодо його забезпечення.

З огляду на зростання важливості «інформаційного суверенітету» для забезпечення безпеки держави, вбачається доцільним:

1. Активізувати в межах чинного бюджетного фінансування, а також актуальних на сьогоднішній день державних грантових наукових програм, наукові дослідження за темою «інформаційного суверенітету». До таких досліджень мають бути залучені, як молоді спеціалісти, так і фахівці наукових установ України, відомчих наукових дослідницьких структур Міноборони, СБУ, МВС, Держспецзв'язку та тих державних інституцій, на які покладено обов'язки забезпечення інформаційної безпеки держави та реалізації державної інформаційної політики.

2. Ключовими темами таких досліджень мають стати: загальна концепція інформаційного суверенітету держави; визначення балансу «контентної» та «технологічної» складової; основні складові кожного з запропонованих елементів; нормативно-правовий аналіз чинного законодавства щодо його відповідності проблематики забезпечення інформаційного суверенітету держави; формування переліку робіт (дослідницьких, конструкторських) виконання яких є пріоритетним для забезпечення інформаційної безпеки держави; формування граничних показників стану забезпечення інформаційної безпеки держави на різних рівнях.

3. Щодо проблеми уточнення в чинній нормативно-правовій базі поняття «інформаційний суверенітет», то воно має більш точно і об'єктивно відображати обидві (контенту та технологічну) компоненти цієї проблеми. Визначення доречно закріпити або у Законі України «Про інформацію» або у Законі України «Про інформаційний суверенітет», якщо буде прийнято рішення про його розробку та затвердження.

4. Розробка відповідного законодавства не може відбуватись поза участю суспільства та, передусім, приватного сектору. Інституційно оптимальним варіантом створення необхідного майданчику для дискусії є або Рада національної безпеки і оборони України або один з консультативно-дорадчих органів (міжвідомчі групи) при Президентові України.

### *6.5 Інформаційна безпека як глобальна проблема захисту інформації,*

***інформаційного простору, інформаційного суверенітету країни та інформаційного забезпечення прийняття урядових рішень.***

Інформаційна безпека виконує завдання, пов'язані з прогнозуванням і запобіганням можливим діям подібного роду, а також зводить до мінімуму можливий збиток.

Інформаційна безпека має декілька напрямів:

1) Формування системи заходів, які спрямовані на недопущення несанкціонованого доступу до інформації, несанкціонованої її модифікації або порушення цілісності.

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

Захист політичних, державних і громадських інтересів країни, захист загальних моральних цінностей, недопущення закликів до порушення територіальної цілісності, заборона інформації, яка включає ідеї війни, насилля, дискримінації та посягання на права людини. Об'єктами захисту інформації виступають: документи, програми ЕОМ, ноу-хау, бази даних, тексти, на яких зафіксована інформація інші матеріальні носії інформації, захист яких передбачений державними нормативними актами, внутрівідомчими постановами та розпорядженнями, іншими спеціальними документами.

Інформаційна безпека розглядається як глобальна проблема захисту інформації, захисту інформаційного простору та інформаційного суверенітету, а також як проблема інформаційного забезпечення прийняття урядових рішень. Визначеними нормами міжнародного права, які зафіксовані у документах ООН і ЮНЕСКО, у документах європейських міжнародних організацій, а також у нормативних актах окремих держав регулюється Інформаційна безпека.

Вирішення проблеми інформаційної безпеки має здійснюватися шляхом:

– творення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;

– підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційної безпеки, запобігання таким загрозам та забезпечення ліквідації їх наслідків;

– вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп’ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;

– розгортання та розвиток Національної системи конфіденційного зв’язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

Дії, які так або інакше загрожують збереженню, що допускають нанесення збитків інформаційній безпеці підрозділяються на певні категорії:

1) Дії, які здійснюють користувачі, авторизовані в системі. Ця категорія включає:

– зловмисні дії користувача з метою крадіжки або повного або часткового знищення даних, що є на сервері або робочій станції компанії;

– пошкодження наявних даних як результат прояву необережності, халатності у діях користувача.

– «Електронне» втручання - дії хакерів (незаконне проникнення в захищені комп'ютерні мережі, здійснення мережевих атак).

2) Спам. Якщо ще кілька років тому спам був всього лише незначним по масштабах, дратівливим чинником, то в даний час технології спаму представляють достатньо серйозну загрозу для забезпечення інформаційної безпеки:

– так, основним каналом для ефективного і швидкого розповсюдження спаму і інших

шкідливих програм в даний час стала електронна пошта;

– на перегляд спаму йде достатньо велика кількість часу, а подальше видалення численних повідомлень може викликати відчуття дискомфорту співробітників на психологічному рівні;

– спам може виступати одним з основних методів реалізації різних шахрайських схем, жертвами яких можуть ставати як приватні, так і юридичні особи;

– великий ризик видалення потрібної кореспонденції разом із спамом, що може привести до різного роду неприємним наслідкам; при цьому така небезпека зростає, якщо удаватися до використання недосконалих поштових фільтрів для виявлення і відсіювання спаму.

3) Комп’ютерні віруси. Так само, як і деякі інші шкідливі програми відносяться до окремої категорії способів електронної дії з подальшим нанесенням збитку. Дані засоби дії є реальною загрозою для ведення сучасного бізнесу, що має на меті широке використання комп'ютерних мереж, електронної пошти і Інтернету в цілому.

4) «Природні» загрози. В категорію «природних» загроз відносять різні зовнішні чинники, причиною втрати інформаційної безпеки може виступити крадіжка інформаційних носіїв, форс-мажорні обставини, неправильний спосіб зберігання інформації та ін.

В наш час інформація є як найдорожчим товаром, так і найдорожчою послугою, тому що використовується в усіх сферах людської діяльності. Важливим є безпека інформації, оскільки несанкціоноване використання інформації може призвести до великої катастрофи в суспільстві. Щоб не виникло ніяких проблем необхідно вживати заходів з забезпечення інформаційної безпеки, не лише теоретично, але й практично.

### *6.6 Проблеми забруднення інформаційного простору неправдивою інформацією*

Навмисне поширення брехні та супутні напади на свободу преси, верховенство права кидають виклик основним нормам та цінностям, від яких залежить інституційна легітимність та політична стабільність. В документі Єврокомісії зазначається, що «дезінформація руйнує довіру до установ, цифрових та традиційних засобів масової інформації, шкодить нашій демократії, перешкоджає громадянам приймати обґрунтовані рішення. Це може поляризувати дебати, створити або поглибити напругу в суспільстві та підірвати виборчі системи, а також мати більш широкий вплив на європейську безпеку. Погіршує свободу думок та вираження поглядів – основне право, що закріплене в Хартії основних прав Європейського Союзу».

Дезінформація є багатогранною проблемою, яка не має однієї першопричини і, отже, не має одного єдиного рішення. Деякі форми дезінформації, очевидно, були увімкнені розвитком конкретних цифрових ЗМІ, включаючи продукти та послуги платформ, але проблема стосується також деяких політичних акторів, ЗМІ та акторів громадянського суспільства. Проблеми дезінформації пов'язані з ширшими політичними, соціальними, громадянськими та медіапроблемами. Багато з цих основних питань передують переходу на цифрові медіа. Оскільки країни стикаються з ризиками, спричиненими різними формами дезінформації, перш за все важливо забезпечити оновлене та засноване на доказах розуміння масштабу, обсягу та точного характеру існуючих проблем та розробити можливі відповіді, які враховуватимуть що, оскільки проблеми дезінформації глибоко переплетені з цифровою екосистемою, технологіями, тактика та методи будуть продовжувати розвиватися.

На початку XXI ст. дослідники цифрової революції висунули припущення, що впровадження інформаційно-комунікаційних технологій (ІКТ) призведе до зменшення ролі держави. Інтернет 1990-х та початку 2000-х рр. видався найбільшим тріумфом неолібералізму: державне регулювання було мінімальним, а цифрові інновації та підприємництва створювали нові Інтернет-ринки, розширювали можливості зв’язків та

спільноти. Другим висновком, тогочасних дослідників, була оптимістична оцінка технічного прогресу та його впливу на політичне життя: нові засоби комунікації розширили доступ до новин, швидше та надійніше передавали їх, надавали ширші можливості для вільного висловлювання та публічного обговорення. Учасники цифрової епохи вбачили, що нова технологія за своєю суттю прагне зламати централізовану владу, і чим далі Інтернет буде поширюватися по всьому світі, тим більше він просуне свободу і буде загрожувати диктатурам.

На думку професора соціології та державного управління Принстонського університету Пола Старра (Paul Starr), таке розуміння наслідків цифрових інновацій для засобів масової інформації та демократії стало жертвою трьох помилок.

По-перше, оптимістичний наратив припускав, що злиття цифрової економіки буде не менше підтримувати вільну пресу, ніж доцифрова економіка. Сьогодні стало цілком зрозумілим, що онлайн-спілкування здатне поширювати дезінформацію та ненависть так само швидко і дешево, як і надійну інформацію та громадянський дискурс.

По-друге, можливості більш широкого індивідуального вибору у джерелах новин були подвійними, тому що, коли споживачам надається така можливість, люди схильні шукати джерела, що підтверджують їхні існуючі упередження, оцінки, та самостійно розподілялися на групи зі схожими поглядами, що посилювало групову поляризацію. Нова структура спілкування також створила нові засоби мікроцільової дезінформації таким чином, що журналісти та інші фахівці не можуть легко контролювати, а тим більше спростувати таку інформацію в реальному часі.

По-третє, цифрові провидці вбачили, що нова технологія розбиває усталені форми централізованої влади, вони помилково вважали, що особлива форма Інтернету, прийнята протягом 1990-х рр. була властивістю цієї технології та, отже, постійною, коли вона, фактично, залежала від конституційного вибору щодо розвитку Інтернету, і була відкрита для сил, які могли б принципово змінили її характер. В іншу епоху Інтернет розвивався б інакше, але в Сполучених Штатах, які домінували в прийнятті критичних рішеннях щодо технологій, державного регулювання та антимонопольного законодавства, а також державної власності, все це відступило, і ці обставини дозволили появу монополій платформ, бізнес-моделей та алгоритмів, які сприяли розповсюдженню дезінформації.

Відтак, на сьогодні наявність дезінформації в інформаційному просторі є серйозною загрозою та викликом основам демократії та функціонуванню основних інституцій країни. Зарубіжні дослідники намагаються не використовувати поняття «фейкової інформації», оскільки воно охоплює складні явища забруднення інформації, а також цей термін почали активно вживати політики у всьому світі для медіа, інформацію яких вони вважають невгодною, і цим самим підривають свободу та довіру до ЗМК.

Тому, чітко виокремлюють такі поняття як «дезінформація» («dis-information») – це інформація, яка є неправдивою та навмисно створена для заподіяння шкоди людині, соціальній групі, організації чи країні; «помилкова інформація» («mis-information») – неправдива інформація, яка не створена з метою заподіяння шкоди та шкідлива, зловмисна інформація («mal-information») – інформація, яка базується на реальних подіях та використовується для заподіяння шкоди людині, організації чи країні.

**ПИТАННЯ ДЛЯ САМОПЕРЕВІРКИ**

1. Охарактеризуйте сутнісне та змістовне наповнення понять «суверенітет» та «національний інформаційний суверенітет».
2. Які основні завдання забезпечення інформаційного суверенітету?
3. Інформаційний та електронний суверенітет: тотожність та відмінність понять.

4. Якими є складові державної інформаційної політики щодо забезпечення інформаційної безпеки країни безпека держави, суспільства та особи?
5. Вкажіть ознаки та властивості державної інформаційної політики, коротко їх охарактеризуйте.
6. Проаналізуйте сучасні та потенційні проблемні питання правового забезпечення інформаційного суверенітету.
7. Окресліть можливі шляхи вирішення правового забезпечення інформаційного суверенітету.
8. Обґрунтуйте тезу: «Інформаційна безпека як глобальна проблема захисту інформації, інформаційного простору, інформаційного суверенітету».
9. В чому полягають проблеми забруднення інформаційного простору неправдивою інформацією?

# ЛЕКЦІЯ 7
# ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

**План викладу:**

7.1 Сутність «загроз» інформаційній безпеці: види загроз та дестабілізуючі фактори.
7.2 Класифікація загроз інформаційної безпеки: правові підходи.
7.3 Джерела та засоби впливу загроз на інформаційну безпеку.
7.4 Механізми реагування на загрози інформаційній безпеці.
7.5 Політико-правовий аналіз загроз інформаційній безпеці України на сучасному етапі.
7.6 Внутрішні та зовнішні інформаційні загрози національній безпеці України та шляхи гарантування інформаційної безпеки країни.

## *7.1 Сутність «загроз» інформаційній безпеці: види загроз та дестабілізуючі фактори.*

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. 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 однією з цих компонентів. 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.

Проте, першочергово слід звернутись до нормативно-правових актів у цій сфері. У Законі України «Про національну безпеку України» від 21.06.2018 р. № 2469-VIII закріплено визначення «*загрози національній безпеці України*» – явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України. Вони, як і відповідні пріоритети державної політики у сферах національної безпеки і оборони, визначаються у Стратегії національної безпеки України, Стратегії воєнної безпеки України, Стратегії кібербезпеки України, інших документах з питань національної безпеки і оборони, які схвалюються Радою національної безпеки і оборони України і затверджуються указами Президента України.

Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. № 2163-VIII більше уваги приділяє питанню загроз у цій сфері. Зокрема, індикатори кіберзагроз визначаються як показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози.

*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. Тут розкриваються поняття кіберінцидентів та кібератак, кіберзлочинів (комп’ютерних злочинів), кібертероризму і кібершпигунства тощо.

У Доктрині інформаційної безпеки України», затвердженій Указом Президента України

№47/2017 від 25 лютого 2017 р., перелічено актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері:

– здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних сил України та інших військових формувань, провокування екстремістських проявів;

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

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

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

– інформаційне домінування держави-агресора на тимчасово окупованих територіях;

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

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

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

Як бачимо, автори Доктрини при виділенні загроз інформаційній безпеці держави використали той самий підхід, що й до визначення національних інтересів в інформаційній сфері, тобто наявні повторення, неповнота переліку, термінологічна невизначеність, донесення однієї думки за рахунок різних формулювань тощо. Наприклад, декілька разів використовується поняття «спеціальні інформаційні операції», при цьому в національному законодавстві це поняття не розкривається і стає незрозумілим, чому загрозою визнаються лише спеціальні інформаційні операції.

Крім того, при характеристиці першої загрози розробники Доктрини не вказали, від кого вона походить, при констатації наявності загрози, особливо у доктринальному документі, бажано чітко вказувати джерело її походження. Те саме стосується і формулювання загрози «поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій», не уточнюється, від кого походить ця загроза. У цілому ж закріплені у Доктрині положення щодо спеціальних інформаційних операції описують одну й ту саму загрозу – перманентну інформаційну війну РФ проти України, що здійснюється різними засобами як в українському національному інформаційному просторі, так і в глобальному.

Враховуючи те, що йдеться про загрози інформаційній безпеці держави, яка є складовою національної безпеки, то в умовах гібридної війни з РФ особи, відповідальні за виникнення вказаних загроз, вочевидь, мають нести і кримінальну відповідальність. Однак на практиці закріплення вказаних загроз у Доктрині інформаційної безпеки України не викликало належної реакції ані з боку громадянського суспільства, ані з боку державних органів.

На підставі вивчення положень Доктрини інформаційної безпеки України, закріплені у ній загрози інформаційної сфери можна класифікувати за джерелом походження на зовнішні та внутрішні.

*Зовнішні загрози*: проведення державою-агресором спеціальних інформаційних операцій проти України як на її території, так і поза її межами; інформаційна експансія та

інформаційне домінування держави-агресора.

*Внутрішні загрози* включають: недостатню розвиненість національної інформаційної інфраструктури; неефективність державної інформаційної політики; недосконалість законодавства; невизначеність стратегічного наративу; недостатній рівень медіа-культури суспільства; поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні.

Найбільш широко загрози інформаційним ресурсам розглядають як потенційно можливі випадки природного, технічного або антропогенного характеру, які можуть спричинити небажаний вплив на інформаційну систему, а також на інформацію, що зберігається в ній. Виникнення загрози, тобто віднаходження джерела актуалізації певних подій у загрози, характеризується таким елементом як уразливість. Саме за наявності вразливості як певної характеристики системи і відбувається активізація загроз. А самі загрози за своєю суттю, відповідно до теорії множин є невичерпними, а отже, й не можуть бути піддані повному описові у будь-якому дослідженні.

*Загроза* (англ. threat) – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків автоматизованій системі. Спробу реалізації загрози називають «атакою». *Загроза безпеці інформації* (англ. security threat) – загрози викрадення, зміни або знищення інформації. Вони бувають випадковими або навмисними.

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. До загроз інформаційній безпеці системи управління національною безпекою належать: розкриття інформаційних ресурсів; порушення їх цілісності; збій у роботі самого обладнання.

### *7.2 Класифікація загроз інформаційної безпеки: правові підходи*

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.

Розглядаючи загрози інформаційній безпеці держави, слід виокремити серед них загрози інтересам особи, суспільства та власне держави в інформаційній сфері. Крім того, загрози інформаційній безпеці групують за сферами діяльності держави. Через їх численність відповідно до загальної класифікації загроз національній безпеці виокремлюють загрози інформаційній безпеці за різними критеріями: за джерелами походження природного, техногенного та антропогенного походження; за повторюваністю вчинення; за ступенем гіпотетичної шкоди; за ймовірністю реалізації; за рівнем визначеності; за значенням; за

структурою впливу; за характером реалізації; за ставленням до них; за рівнем детермінізму.

Загрози інформаційній безпеці України ми розглядаємо як детермінуючі фактори, що зумовлюють і породжують негативні явища, які посягають на національні інтереси в інформаційній сфері, організацію та функціонування національного інформаційного простору загалом. Вони мають або можуть мати широкомасштабне значення, пов'язані з ризиками і небезпеками в інших сферах.

Так, у законодавстві України регламентовані загрози національній безпеці України на сучасному етапі розвитку нашого суспільства і держави існують у зовнішньополітичній сфері, у сфері державної безпеки, у воєнній сфері та сфері безпеки державного кордону України, у внутрішньополітичній сфері, в економічній сфері, у соціальній та гуманітарній сферах, у науково-технологічній сфері, у сфері цивільного захисту, в екологічній сфері, в інформаційній сфері.

Безпосередньо детермінують посягання на інформаційну безпеку, так само як і на державний суверенітет, територіальну цілісність держави України такі загрози, як претензії з боку інших держав світу, глобалізація світових відносин і зосередження важелів впливу на світові процеси в руках окремих осіб або груп, прояв сепаратизму і намагання автономізації за етнічною ознакою окремих регіонів України.

Усі інші загрози національній безпеці України можуть прямо і не створювати небезпеку посягання, але тією чи іншою мірою підривають ці фундаментальні цінності держави та суспільства. Слід підкреслити, що загрози інформаційній безпеці держав виходять за межі географічних їх кордонів, посягають на національний інформаційний простір, але можуть мати транскордонні чи глобальні негативні наслідки.

З метою запобігання і протидії існуючим та ймовірним загрозам інформаційній безпеці стратегічне завдання сучасної держави, з огляду на відповідні функції і завдання, полягає у створенні та функціонуванні механізму забезпечення інформаційної безпеки. Він передбачає послідовну системну діяльність, сукупність заходів і державно-правових інституцій, що покликані гарантувати безперешкодну реалізацію національних інтересів держави в інформаційній сфері, відповідних інтересів людини і суспільства, запобігання інформаційним конфліктам та оперативне їх подолання. Враховуючи активну глобалізацію інформаційно-комунікаційних мереж, важливо не тільки державам, а й міжнародним організаціям долучатися до співпраці у напрямі протидії різноманітним видам інформаційної агресії.

### *7.3 Джерела та засоби загроз на інформаційну безпеку*

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.

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.

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.

### *7.4 Механізм реагування на загрози інформаційній безпеці*

Забезпечення інформаційної безпеки ґрунтується на наступних принципах:

1. Принцип системності. Відповідно до якого, захисні заходи повинні бути спрямовані на ліквідацію інформаційних атак з боку зовнішніх та внутрішніх джерел, а також враховувати засоби захисту та канали закритого доступу. Засоби захисту повинні використовуватись адекватно можливим видам загроз та функціонувати у вигляді комплексного захисту, технічно доповнюючи один одного.

2. Принцип міцності. Встановлює, що правила забезпечення інформаційної безпеки повинні охоплювати всі зони безпеки, мати рівну надійність захисту та дозволяти визначати можливі загрози.

3. Принцип багаторівневого захисту. Орієнтований на створення меж захисту інформаційної системи, що складаються з послідовно розташованих зон безпеки, ключова з яких знаходиться всередині всієї системи.

4. Принцип безперервності. Відповідно до якого, функціонування системи інформаційної безпеки повинно бути безперервним.

5. Принцип розсудливості. Визначається в розумності застосування захисних заходів з потрібним ступенем безпеки. В основі даного принципу знаходиться доцільність високих матеріальних витрат та раціональність їх подальшого використання.

Останніми роками Україна зробила важливі кроки щодо регулювання інформаційної безпеки на нормативно-правовому рівні. Зокрема, 28 грудня 2021 року було затверджено Стратегію інформаційної безпеки, головною метою прийняття якої є посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина.

Ефективність сучасної зброї все більше визначається не стільки вогневою потужністю, скільки ступенем інформаційної забезпеченості. В змісті військових дій зросла значимість інформаційно-технічного протиборства. Переваги в ступені інформованості – неодмінна умова перемоги в повітряному, морському та сухопутному бою.

Ключовими заходами щодо забезпечення ефективної діяльності у сфері державного управління інформаційною безпекою є:

– розробка показників оцінки ефективності систем захисту інформаційної безпеки держави; моніторинг та ідентифікація появи дестабілізуючих факторів та загроз;
– організація проведення фундаментальних та прикладних наукових досліджень в галузі забезпечення інформаційної безпеки;
– розробка відповідної нормативно-правової бази;
– протистояння загрозі інформаційної війни.

Інформаційна безпека є важливою функцією держави, повинна передбачати, насамперед, формування відповідними державними органами політики організаційно-правових механізмів в галузі інформаційної безпеки. Важлива роль в даному напрямі належить державним органам, які відповідно до наданих повноважень в сферах своєї відповідальності повинні здійснювати організаційне, нормативно-правове, матеріально-технічне та фінансове забезпечення реалізації державної політики інформаційної безпеки.

З метою ефективного, планомірного та контрольованого забезпечення цілісної військової безпеки необхідно функціонування за єдиним сценарієм системи військової безпеки, що виражається в ефективній діяльності трьох компонентів: управлінського, силового та забезпечувального.

Система забезпечення безпеки повинна не тільки реагувати на загрози та виклики, але й володіти передбаченням можливих загроз. Основним чинником вимог до системи забезпечення військової безпеки є поєднання централізованого та децентралізованого управління засобами забезпечення інформаційної безпеки. Механізм забезпечення інформаційної безпеки є невід’ємною складовою в процесі реалізації національної безпеки (рис. 7.1).

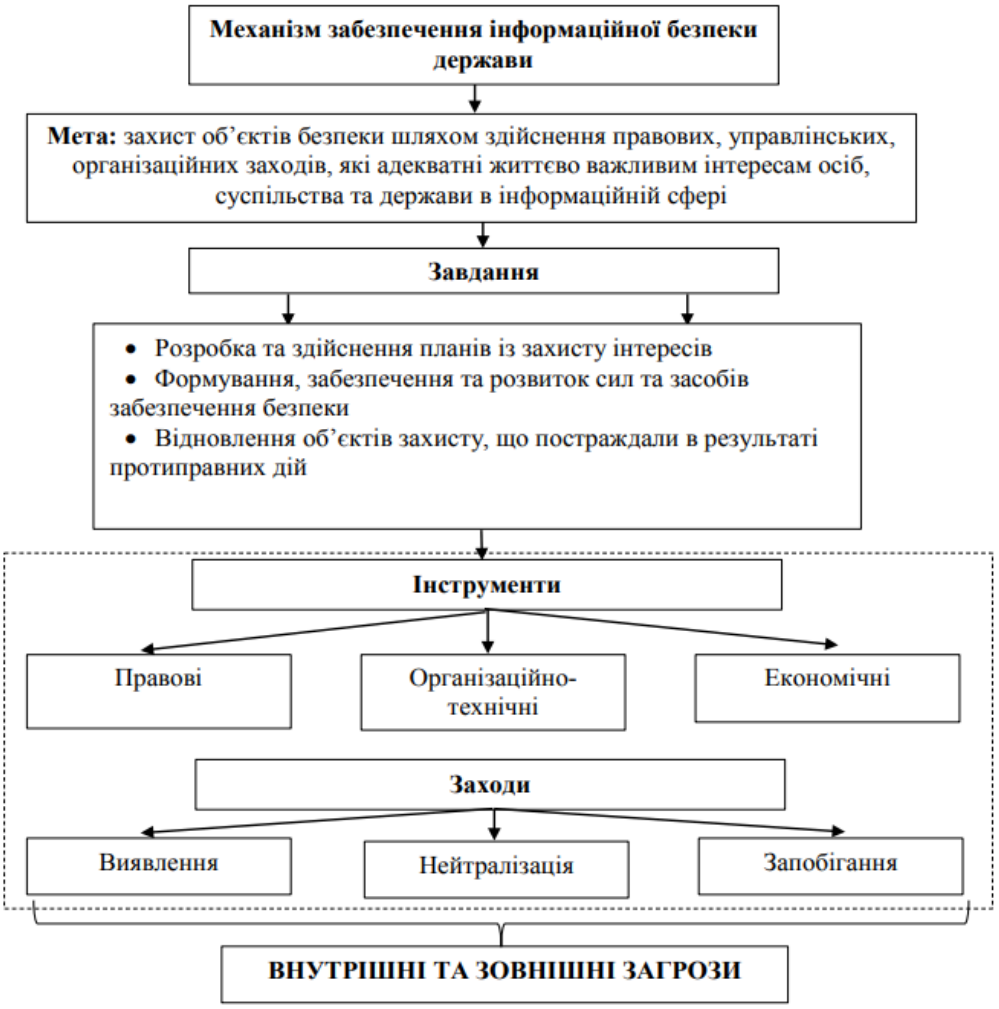



Рис.7.1 – Механізм забезпечення інформаційної безпеки.

Серед ключових напрямів, які має виконувати механізм забезпечення інформаційної безпеки варто відзначити наступні:

– виявлення внутрішніх та зовнішніх загроз інформаційній безпеці держави;
– визначення індикаторів інформаційної безпеки та їх порівняння нормативними показниками;
– формування та реалізація системи моніторингу, яка включає: спостереження, збір, обробку, збереження та аналіз інформації щодо стану інформаційної безпеки держави;
– розробка заходів, спрямованих на забезпечення стабільності інформаційної безпеки держави.

Структурні елементи інформаційної безпеки на міжнародному та внутрідержавному рівні включають:

– захист відомостей, що містять державну або комерційну таємницю;
– захист серверів державних установ та систем життєзабезпечення;
– захист безпеки даних як набір апаратних та програмних засобів, що забезпечують збереження інформації від неавторизованого доступу;
– інформаційно-психологічний блок, який передбачає реалізацію систем заходів, спрямованих на захист від цілеспрямованого впливу на суб'єкт нападу, його психологічний стан або імідж на міжнародній арені.

### *7.5 Політико-правовий аналіз загроз інформаційній безпеці України*

В умовах війни, коли країна стала об'єктом агресії і підпадає під значну низку інформаційних загроз, їх ліквідація вимагає вжиття певних організаційно-правових заходів. Стратегічна ціль забезпечення інформаційної безпеки як складової національної безпеки обумовлена національними інтересами України у внутрішньополітичній сфері, до яких відноситься збереження конституційного устрою, підтримка національної злагоди та єдність правового простору.

Головними напрямами вдосконалення системи забезпечення інформаційної безпеки є наступні:

- стратегічне стримування та ліквідація військових конфліктів, що можуть виникнути в результаті застосування інформаційних технологій;
- вдосконалення системи забезпечення інформаційної безпеки Збройних Сил України, військових формувань, включаючи в себе сили та засоби інформаційної протидії;
- прогнозування, виявлення та оцінка інформаційних загроз, включаючи загрози Збройним Силам України в інформаційній сфері.

Під час воєнного стану інформаційна зброя є достатньо потужним засобом ведення війни, оскільки її технічна інноваційність, потужність та непомітність є дуже небезпечними. Тому, інформаційна безпека України має ґрунтуватися на скоординованих діях державних установ та структур громадянського суспільства.

Відтак, одним з першочергових завдань держави є забезпечення захисту інформації, що в свою чергу є гарантією національної безпеки. В результаті цивілізаційного розвитку інформація стає повноцінним ресурсом. Забезпечення інформаційної безпеки на даний час є не менш важливим напрямом державної політики, чим підтримка економічної стійкості та високих соціальних стандартів.

Основними напрямами щодо реалізації та захисту національних інтересів на сучасному етапі розвитку України в інформаційній сфері є наступні:

– розробка та прийняття довгострокової програми із забезпечення виходу на рівень провідних країн світу в галузі створення систем інформатизації та управління, що ґрунтуються на новітніх інформаційних технологіях;

– забезпечення свободи отримання та розповсюдження інформації громадянами, іншими суб'єктами суспільних відносин в інтересах формування громадянського суспільства, демократичної правової держави, розвитку науки та культури;

– забезпечення надійного захисту інформаційного потенціалу України від неправомірного його використання; здійснення контролю за експортом з держави інтелектуальної продукції, а також інформаційних банків даних;

– організація ефективної системи підготовки та перепідготовки кадрів в галузі забезпечення інформаційної безпеки;

– розвиток взаємодії державних та комерційних систем інформаційного забезпечення з метою більш ефективного використання інформаційних ресурсів держави.

Проблематика внутрішньополітичних загроз національній безпеці України є предметом наукового та науково-практичного опрацювання з перших років Незалежності нашої держави. Відповідно до того, як змінювався безпековий порядок денний – від подолання наслідків системної кризи 90-х років XX ст. до протидії гібридним впливам на внутрішньополітичну ситуацію з боку РФ – еволюціонували і підходи науковців до визначення безпекових пріоритетів внутрішньої політики. Українські вчені й державні управлінці розглядають питання внутрішньополітичної безпеки у контексті сучасного бачення світових суспільних наук, зокрема – виходячи з пріоритету безпеки людини. А також – з урахуванням підходів, які застосовує у своїй безпековій політиці Європейський Союз.

Результатом роботи над стратегічним плануванням національної безпеки стало

рішення Ради національної безпеки і оборони України від 14 вересня 2020 р. «Про Стратегію національної безпеки України», уведене в дію Указом Президента. У Національному інституті стратегічних досліджень ведеться системна робота з дослідження внутрішньополітичних загроз національній безпеці. Зокрема, в аналітичних доповідях до щорічних Послань Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України» робиться регулярний огляд динаміки безпекового середовища, розглядаються нові фактори ризиків та пропонуються заходи, спрямовані на зниження загроз.

## ПИТАННЯ ДЛЯ САМОПЕРЕВІРКИ

1. Охарактеризуйте види загроз інформаційній безпеці.
2. Як на інформаційну безпеку країни впливають дестабілізуючі фактори?
3. Вкажіть правові підходи до класифікації загроз інформаційної безпеки.
4. Назвіть джерела та обґрунтуйте засоби впливу загроз на інформаційну безпеку.
5. Здійсніть політико-правовий аналіз загроз інформаційній безпеці України на сучасному етапі.
6. Визначте коло загроз інформаційній безпеці особи.
7. Оберіть одну із сфер діяльності держави та вкажіть інформаційні загрози.
8. Окресліть внутрішні та зовнішні інформаційні загрози національній безпеці України.
9. Яким, на Вашу думку, є шляхи гарантування інформаційної безпеки країни?

# ЛЕКЦІЯ 8
# БЕЗПЕКА ІНФОРМАЦІЙНОГО ПРОСТОРУ

**План викладу:**

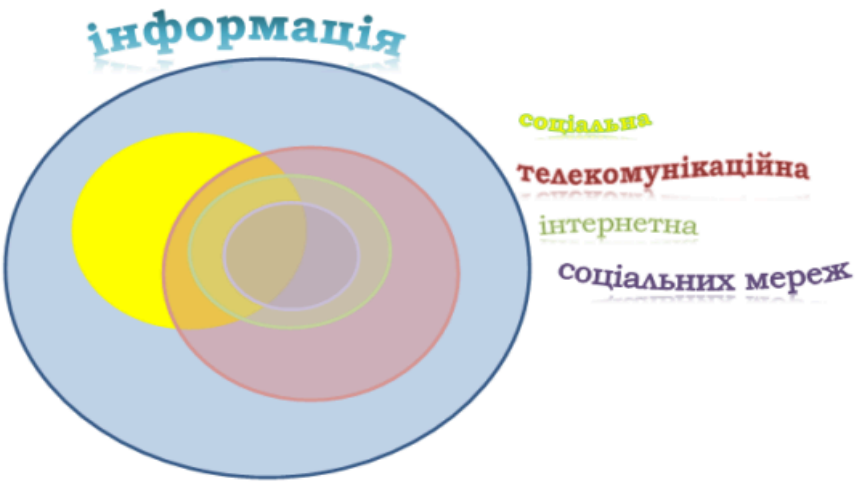
8.1 Інформаційний простір: підходи до визначення.
8.2 Ознаки, функції та структура інформаційного простору.
8.3 Суб'єкти та об'єкти управління в інформаційному просторі, їх класифікація.
8.4 Національний інформаційний простір. Особливості формування та сучасний стан національного інформаційного простору держави.
8.5 Проблемні питання правового реагування та трансформаційні процеси забезпечення національної та міжнародної інформаційної безпеки та можливі шляхи їх вирішення.
8.6 Інтеграція України до європейського інформаційного простору.

## *8.1 Інформаційний простір: підходи до визначення*

Термін «інформаційний простір» має багато тлумачень. Саме поняття складається з двох слів – інформація і простір, тлумачення яких є невизначеним, неоднозначним і в багатьох випадках залежить від контексту. Загальноприйнятого і однозначного визначення інформації немає, автори дають певні визначення в залежності від галузі використання.

Згідно із Закону України «Про інформацію», інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Вибір джерел інформації, формування персональних соціальних мереж, а саме – вибір сайтів, груп в службах соціальних мереж і т.і. означатиме вибір певного продукту або послуги (це важливо для бізнесу), вибір певного кандидата на виборах (це важливо в політичній сфері), вибір інформаційного поля, інформаційного середовища (важливо в умовах інформаційних війн).

Важливою частиною інформації, яку може отримати людина є соціальна інформація: сукупність відомостей, знань, даних, які формуються в суспільстві та використовуються індивідами, соціальними групами, організаціями для регулювання соціальної взаємодії, суспільних відносин та процесів. Соціальна інформація може отримується із взаємовідносин у реальному житті, і за допомогою телекомунікаційних систем (див. рис. 8.1).




**Взаємовідношення різних видів інформації, яку сприймає індивід**

Згідно із Digital 2020: Global Digital Overview типовий користувач Інтернету проводить там більше 40 відсотків денного часу, а на соціальні мережі витрачає приблизно 2 години 27 хвилин на день, тому можна вважати, що значущу долю інформації людина отримує за

допомогою телекомунікаційних засобів, включаючи Інтернет. Інформацію, отриману засобами телекомунікаційних систем, Інтернету, в тому числі з сайтів служб соціальних мереж, будемо називати телекомунікаційною інформацією (ТІ).

Дамо наступне визначення: «Телекомунікаційна інформація індивіда (інформація з телекомунікаційних систем, яку отримує індивід) – це відомості/знання про об’єкти, їх властивості і зв’язки, що отримуються індивідом засобами телекомунікаційних систем, мереж, в тому числі через Інтернет».

Вся сукупність інформації, яка може бути отримана телекомунікаційними засобами, створює певний простір, який назвемо телекомунікаційним інформаційним простором. Програмне забезпечення телекомунікаційних систем надає індивіду певний набір інструментів для виконання дій над інформацією. Наприклад, більшість служб соціальних мереж дозволяють виконувати зберігання інформації, її копіювання, розповсюдження (пересилання певним акаунтам, включаючи акаунти інших соціальних мереж).

В наукових дослідження в області інформаційних технологій використовуються наступні визначення інформаційного простору: «Сукупність понять та відносин між ними, які організовано у інформаційну систему, що описує діапазон можливих значень або смислів, які об'єкт може приймати за даними правилами та обставинами», «Тип інформаційної конструкції, у якій репрезентації інформаційних об'єктів розташовані у організованому просторі.

Інформаційний простір є динамічним, він швидко адаптується до викликів розвитку сучасного суспільства, стаючи на варті інтересів держави або, навпаки, впливаючи на неї.

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.

### *8.2 Ознаки, функції та структура інформаційного простору*

Інформаційний простір є динамічним середовищем, де фізичні об’єкти зазвичай мають чітко визначені фізичні межі, що можуть досягати часової інформаційної переваги, а простір є структурованим. З розвитком засобів та новітніх технологій передавання інформації суттєво змінюється зміст взаємодії під час спільної діяльності. Помітною стає конкуренція за досягнення інформаційної переваги, за володіння розвиненішим інформаційним ресурсом, що відкриває кращі можливості контролю над інформаційним ресурсом держави.

Інформаційний простір завжди захищений, в ньому є місця, що свідомо захищаються від чужого входження. Захист одночасно передбачає наявність слабких місць, служить їх детектором. 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.

Інформаційний простір є базовим для понять інформаційної війни та інформаційної зброї. Інформаційну війну можна визначати як несанкціоновану діяльність у чужому інформаційному просторі.

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.

Характерною рисою процесу формування єдиного інформаційного простору України є: створення технологій; технологічна структура інформатизації для забезпечення взаємодії виробників інформації і її споживачів.

Інформаційна інфраструктура суспільства – середовище, яке забезпечує можливість збору, передачі, зберігання, обробки й розповсюдження інформації та належить до складу технологічних й організаційних компонентів інформаційного простору.

Інформаційна інфраструктура суспільства утворюється сукупністю: інформаційних і телекомунікаційних систем та мереж зв’язку індустрії засобів інформатизації, телекомунікації і зв’язку; систем формування і забезпечення збереження інформаційних ресурсів; системи забезпечення доступу до інформаційно-телекомунікаційних систем, мереж зв’язку та інформаційних ресурсів; індустрії інформації та ринку інформаційних послуг; системи підготовки кадрів, проведення наукових досліджень; алгоритмів і програмних засобів, що забезпечують функціонування програмно-апаратних платформ тощо.

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 є сукупністю 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.

### *8.3 Суб’єкти та об’єкти управління в інформаційному просторі, їх класифікація*

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.

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.

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.

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). 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.

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, 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).

### *8.4 Національний інформаційний простір. Особливості формування та сучасний стан національного інформаційного простору держави*

Особливості формування та сучасний стан національного інформаційного простору України. У науці та законодавстві України представлено багато визначень національного інформаційного простору. 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;
- 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);

- важливу ознаку 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;

- сферу 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.

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.

Серед чинників, які перешкоджають розвитку та забезпеченню безпеки інформаційного простору України варто відзначити:

- 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.

Тож завданнями щодо розвитку інформаційного простору України є:

– 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 прийняття системних державних рішень, спрямованих на стимулювання створення національних інноваційних структур (центри наукових парків і технопарків) для розроблення конкурентоспроможних вітчизняних інформаційно-комунікаційних технологій;

– розробити на національному та місцевому рівні механізм ефективної громадської участі та громадського контролю за реалізацією пріоритету розбудови інформаційного суспільства;

– забезпечити баланс інтересів держави і світового співтовариства при входженні України в глобальний інформаційний простір та забезпечення її національного інформаційного суверенітету тощо.

### *8.5 Проблемні питання правового реагування та трансформаційні процеси забезпечення національної та міжнародної інформаційної безпеки та можливі шляхи їх вирішення*

У системі правового забезпечення національної безпеки України в інформаційній сфері нормативно-правова складова узгоджується з інституційними механізмами, що відчутно демонструє їхню єдність. Особливе місце та призначення у цій системі займають санкції. Найбільш суттєві порушення інформаційної безпеки знаходять свою реалізацію у спосіб встановлення санкцій у нормах права, а застосування – відповідно до рішення судів щодо притягнення до адміністративної або ж до кримінальної відповідальності у спосіб визначення у першому випадку – стягнень, у другому – покарання. В інших випадках санкції виконують функцію обмежень у реалізації прав учасників міжнародних і внутрішніх правових відносин за певних, передбачених спеціальним законом обставин. Таким спеціальним законом в Україні є Закон «Про санкції» №1644-VII від 14 серпня 2014 року.

Види передбачених спеціальним законом санкцій є різними і стосуються економічної, у тому числі зовнішньоекономічної, господарської, фінансової тощо діяльності, користування об’єктами права власності, використання активів, у тому числі фінансових, здійснення і реалізації угод, переміщення капіталів, товарів тощо, здійснення заходів контролю, у тому числі щодо проведення фінансових операцій.

Повноваження щодо запровадження санкцій належать Раді національної безпеки і оборони України за зверненням Верховної Ради України, Президента України, Кабінету Міністрів України, Служби безпеки України з прийняттям відповідного рішення, яке затверджується Указом Президента та потребує ухвалення Постановою Верховної Ради України лише у випадку застосування загальних санкцій.

Законом не проведено диференціації, чіткого розмежування підстав та видів санкцій, які можуть бути застосовані до суб’єктів, які вчинили дії на шкоду національній безпеці України. У правових відносинах у сфері національної безпеки загалом та у сфері інформаційної безпеки зокрема держава має виключні повноваження стосовно захисту своїх суверенних прав, у тому числі у спосіб упровадження загальних і персональних санкцій.

В «інформаційному суспільстві» створення, розповсюдження, використання, узагальнення та маніпулювання інформацією становить значну частину економічної, політичної та культурної діяльності. Економіка знань стає економічною копією цієї діяльності, оскільки добробут суспільства створюється через експлуатацію знань або розуміння суті речей та процесів. Люди, які мають засоби і можливості бути в інформаційному суспільстві отримують певні додаткові вигоди.

Узагальнюючи ознаки та тенденції, які характеризують інформаційно-правове поле, в умовах якого сьогодні формуються суспільні відносини з приводу інформації в українському суспільстві можна окреслити певні висновки:

– інформаційне суспільство в умовах воєнного стану – це така форма глобального соціального інформаційного простору, де з одночасною реалізацією ефективної інформаційної взаємодії людей, їх активного доступу до світових інформаційних ресурсів, задоволення потреб щодо інформаційних продуктів і послуг, існує і певна система вимушених під тиском війни державно-владних обмежень у поширенні інформації, що з одного боку захищає, а з другого – обмежує права та свободи громадян;

– Україні ще належить виконати значний обсяг роботи з осмислення і адаптації концепції «інформаційного суспільства» в українських реаліях війни, розроблення та реалізації Національної стратегії сучасного інформаційно-комунікаційного розвитку, а не «інформаційного суспільства».

– існує недооцінка інтелектуальної складової сфери інформаційно-комунікаційних технологій та переоцінка бізнесової складової, що реально призводить до відтоку інтелекту в сферу інформаційно-комунікаційних технологій інших країн, а тим більш під час дії воєнного стану та згідно аналітиці може набути ще більших і неконтрольованих розмірів вже після скасування заборони виїзду чоловіків за кордон, яка відбудеться після перемоги України над росією;

– визначено, що Інтернет є одним із найважливіших інструментів розвитку інформаційного суспільства;

– особливістю українського воєнного стану є тотальна всеукраїнська та міжнародна поінформованість як простих громадян, так і влади про перебіг воєнних дій;

– запровадження державного застосунку «Дія» під час воєнного стану, значно допомагає громадянам в умовах внутрішнього переміщення, знаходження за межами країни або навпаки на тимчасово окупованій території.

### *8.6 Інтеграція України до європейського інформаційного простору*

Україна вже давно обрала шлях до європейської інтеграції, який полягає не лише в економічній співпраці та вдосконаленні правових норм, а й у входженні України до інформаційного простору ЄС із метою обміну інформацією, забезпечення інформаційної безпеки й взаємного культурного збагачення, популяризації української культури, національних цінностей.

Особливо важливо співпрацювати та інтегрувати інформаційні простори України та ЄС зараз, під час повномасштабної війни, розпочатої РФ. Завдяки співпраці про Україну та її біль знає весь світ й активно допомагає українцям протистояти агресору, приймати біженців, надавати гуманітарну допомогу тощо. Розпочато прискорену процедуру вступу до ЄС, під час якої Україні доведеться прийняти низку умов та адаптувати низку процесів до формату ЄС.

У європейському інформаційному просторі існує потужна правова основа, що регламентує функціонування самого простору, використання інформаційних продуктів, захисту прав інтелектуальної власності, а також дотримання безпекових вимог. Правове забезпечення функціонування й відкритості державних інформаційних ресурсів є необхідною умовою інтеграції єдиного інформаційного простору України з європейським та світовим інформаційним простором.

Організаційна основа інформаційного простору стосується функціонування державних і недержавних органів формування інформаційної політики та забезпечення інформаційної безпеки, порядку функціонування інформації в ЗМІ й інших інформаційних джерелах, містить вимоги щодо достовірності інформації та, загалом, мало відрізняється від

організаційних засад сучасного українського інфопростору. Інформаційний простір як сукупність інформаційних процесів у суспільстві визначає політичний, економічний, соціальний, безпековий та культурний потенціал суспільства.

Цілі створення й розвитку єдиного інформаційного простору України:

– забезпечення прав громадян на інформацію відповідно до вимог Конституції України;

– створення та підтримання рівня інформаційного потенціалу, необхідного для сталого розвитку суспільства;

– підвищення узгодженості рішень центральних органів державної влади, облдержадміністрації й місцевого самоврядування;

– підвищення рівня правової свідомості громадян шляхом надання їм вільного доступу до нормативно-правових документів, що визначають їхні права, обов'язки та можливості;

– створення можливостей для громадян і громадських організацій контролювати діяльність органів центрального, місцевого та місцевого самоврядування;

– підвищення ділової й соціальної активності громадян шляхом зрівняння з державними органами можливості використання відкритої науково-технічної, соціально-економічної, суспільно-політичної інформації, а також інформаційних фондів у сфері освіти, культури тощо;

– інтеграція зі світовим інформаційним простором.

Інформаційний простір буде ефективним, якщо він буде відкритим для суспільства, що, зі свого боку, дасть змогу всебічно та системно реалізовувати узгоджені інтереси громадян, суспільства та держави. Ефективний інформаційний простір може бути створений і почне розвиватися на основі відповідної інформаційної політики держави, що забезпечить поступовий рух країни до побудови інформаційного суспільства.

Цей рух має ґрунтуватися на новітніх інформаційних, комп'ютерних, телекомунікаційних та комунікаційних технологіях. Їх розвиток відкриває інформаційні мережі, особливо інтернет, що надає принципово нові можливості для міжнародного обміну інформацією.

Створення та розвиток єдиного інформаційного простору України і, зокрема, відповідних державних інформаційних ресурсів є міжгалузевою та міжрегіональною проблемою. Вона потребує виконання складних організаційних і технологічних завдань, значних витрат та не може бути розв'язана відразу. Це потребує комплексного розгляду соціально-економічних, правових та політичних аспектів комп'ютеризації суспільства, повного використання організаційного, технологічного, технічного й правотворчого досвіду, набутого в розвитку інформаційних просторів провідних країн.

Створення та розвиток єдиного інформаційного простору України – це, передусім, забезпечення швидкого доступу до наявних інформаційних ресурсів і робота над їх включенням до єдиного інформаційного простору. Новостворені інформаційні ресурси, що входять до єдиного інформаційного простору, мають бути законно доступними для органів державної влади, суб'єктів господарювання та громадян.

Основою впровадження нових інформаційних технологій можуть бути чинні й розроблені інформаційно-управлінські системи органів державної влади (центрального та місцевого самоврядування), відомчі й міжвідомчі територіально розосереджені системи та мережі збору, обробки й розповсюдження інформації.

Відтак першочерговим питанням інтеграції в європейський інформаційний простір є адаптація та гармонізація українського законодавства в інформаційній сфері з відповідними нормативно-правовими актами ЄС. Наприклад, європейське законодавство ставить високі вимоги до достовірності інформації й протидії дезінформації.

Європейський інформаційний простір має низку особливостей, що містять більш

посилені вимоги до якості та безпеки використання інформаційних продуктів. У зв'язку з цим виникає проблема можливостей входу інформаційного продукту України на європейські інфоресурси. На сьогодні для України запущено прискорену процедуру євроінтеграції. Тому існує потреба у вдосконаленні нормативно-правового та організаційного забезпечення функціонування українського інформаційного простору для більш легкого входження в європейський простір.

**ПИТАННЯ ДЛЯ САМОПЕРЕВІРКИ**

1. Які підходи до визначення інформаційного простору Ви знаєте?
2. Охарактеризуйте ознаки, функції та структуру інформаційного простору.
3. Окресліть коло суб'єктів та об'єктів управління в інформаційному просторі, здійсніть їх класифікацію.
4. Яким є сутнісне та змістовне наповнення поняття «національний інформаційний простір»?
5. Охарактеризуйте особливості формування національного інформаційного простору держави.
6. На Вашу думку, яким є сучасний стан національного інформаційного простору держави? Обґрунтуйте свою відповідь.
7. Які проблемні питання правового реагування забезпечення національної та міжнародної інформаційної безпеки потребують невідкладного вирішення?
8. Окресліть трансформаційні процеси забезпечення національної та міжнародної інформаційної безпеки
9. Вкажіть можливі шляхи забезпечення національної інформаційної безпеки.
10. Якими мають бути невідкладні кроки для інтеграції України до європейського інформаційного простору?

# ЛЕКЦІЯ 9
# ІНФОРМАЦІЙНІ ВІЙНИ ЯК ДЖЕРЕЛО ЗАГРОЗ БЕЗПЕЦІ ДЕРЖАВИ

**План викладу:**

9.1 Сутність понять «інформаційний вплив», «інформаційна операція», «інформаційна війна», «інформаційна зброя».

9.2 Об’єкти інформаційного впливу. Інформаційно-психологічна протидія, контроль каналів передачі інформації, система моніторингу та прогнозування негативних інформаційно-психологічних впливів.

9.3 Принципи, логіка, моделі, різновиди інформаційної війни. Засоби, методи і технології інформаційних воєн.

9.4 Інструменти інформаційно-психологічних протиборств.

9.5 Відповідальність за порушення інформаційної безпеки держави.

9.6 Способи та форми ведення інформаційної боротьби. Методологія оцінки ефективності інформаційної боротьби.

## *9.1 Сутність поняття «інформаційний вплив», «інформаційна операція», «інформаційна війна», «інформаційна зброя»*

Інформаційне суспільство проходить через значні зміни під впливом інформаційних технологій та інформаційної революції. Інформаційний вплив став значною проблемою для сучасної людини, оскільки він впливає на формування, розвиток та функціонування особистості. У сучасному суспільстві відбуваються зміни, що призводять до трансформацій у різних сферах життя людини, зокрема, у професійних відносинах, характері праці, комунікації та когнітивних функціях. Актуальний спосіб життя вимагає від людини постійного прискорення темпу та взаємодії зі світом за посередництвом інформаційно-комунікативних технологій. А це призводить до того, що люди в інформаційному суспільстві споживають і продукують велику кількість інформації.

Інформаційно-психологічний вплив (далі - ІПВ) - вплив на свідомість особи і населення з метою внесення змін у їх поведінку та (або) світогляд. Базовими методами ІПВ є переконання і навіювання.

Переконання звернене до власного критичного сприйняття дійсності. Воно має власні алгоритми впливу:

логіка переконання повинна бути доступною інтелекту об'єкта впливу;

переконання необхідно здійснювати, спираючись на факти, відомі об'єкту;

переконуюча інформація повинна містити узагальнюючі пропозиції;

переконання має складатися з логічно несуперечливих тез;

факти, що повідомляються, повинні бути відповідним чином емоційно забарвлені.

Навіювання навпаки спрямовано на суб'єктів, що некритично сприймають інформацію. Його особливостями є:

цілеспрямованість і плановість застосування;

конкретність визначення об'єкта навіювання (селективний вплив на визначені групи населення, що враховує основні соціально-психологічні, національні й інші особливості цих груп);

некритичне сприйняття інформації об'єктом навіювання (навіювання засновано на ефекті сприйняття переданої інформації як інструкції до дії без її логічного аналізу);

визначеність, конкретність поведінки, що ініціюється (об'єкту необхідно дати інструкцію щодо здійснення конкретних його реакцій і вчинків, що відповідають меті впливу).

Як явище інформаційна війна існує в певній формі з давніх часів. Саме здійснення

інформаційних впливів як інформаційної зброї було зафіксовано літописцями на теренах України ще за Київської Русі. Використовувались різні методи, такі як приховування інформації, подача її частково, у певному ракурсі, перебільшення наслідків. Інформаційна війна прийшла до нас не з часом приходу інформаційного суспільства, а з давньої історії.

Типовими прикладами первісних інформаційних війн можна вважати сакральну боротьбу із силами природи, тваринами а також внутрішньо- та міжплемінні конфлікти, що супроводжувалися першими інформаційними атаками – залякуванням, дезінформацією, приховуванням, демонстрацією тощо. Згодом, як форму інформаційнопсихологічного впливу, почали використовувалися страхітливе бойове розфарбовування воїнів, люті бойові кличі, спеціальні шумові (удари списами або мечами по щитах) та візуальні (використання вогненних валів) ефекти, чутки, тощо.

Поступово своєрідне мистецтво управління психічними станами, думками і вчинками людей удосконалювалося. Воно стало таємною зброєю жерців, шаманів, воєначальників і використовувалося для управління широкими масами людей, для ведення воєнних дій.

У 2012 році офіційне визначення «інформаційна війна» вперше з'явилося в Україні. Згідно Указу Президента України «Про Стратегічний оборонний бюлетень України» (який втратив чинність), згідно якого «інформаційна війна, є форма протиборства між суб'єктами (державами, блоками, партіями тощо), що передбачає інформаційний вплив на населення з використанням засобів масової інформації, комп'ютерних мереж тощо з метою формування відповідної суспільної думки, підриву морального духу як усього суспільства, так і окремих його інституцій».

Інформаційна війна є формою організації інформаційної взаємодії, яка є найбільш ефективною при досягненні політичних цілей, і вимагає постійного інформаційного підкріплення. Інформаційна війна – найвищий рівень інформаційного протиборства, спрямований на розв'язання суспільно-політичних, ідеологічних, а також національних, територіальних та інших конфліктних ситуацій між державами, народами, націями, класами й соціальними групами, транснаціональними корпораціями шляхом широкомасштабної реалізації способів і методів інформаційного насильства (інформаційної зброї).

Інформаційна війна може включати в себе: збір тактичної інформації; гарантування безпеки власних інформаційних ресурсів; поширення пропаганди або дезінформації, щоб деморалізувати війська та населення ворога; підрив якості і інформації супротивника і попередження можливості збору інформації супротивником.

Інформаційна війна ведеться шляхом застосування інформаційно-психологічних операцій (ІПСО). Інформаційно-психологічна операція – це комплекс узгоджених та взаємопов'язаних заходів маніпулювання інформацією, що здійснюються за загальним планом з метою досягнення та утримання переваги шляхом психологічного впливу на противника. Інформаційно-психологічні операції є комунікативними технологіями, що спрямовані на внесення змін у поведінку індивіда за допомогою модифікації його моделі світу, що здійснюється шляхом внесення змін у інформаційні потоки.

Основна мета інформаційно-психологічної операції – створення та постійне підтримання напруги (в політичній, економічній та соціальній сферах) у суспільстві держави-противника, запуск деструктивних процесів, які поступово вражатимуть та руйнуватимуть державу зсередини. Головна ціль інформаційно-психологічних операцій – це дестабілізація суспільного життя, розпад зсередини, які в свою чергу підготовлюватимуть ґрунт для успішного здійснення політичних, економічних та воєнних дій. Головне завдання інформаційно-пропагандистських акцій у процесі проведення ІПСО полягає в тому, щоб вплинути на духовну сферу – суспільну думку та настрої, які панують в суспільстві, ціннісні орієнтації, погляди, соціально-психологічний клімат, посіяти страх та невпевненість перед

майбутнім, викликати недовіру до органів державної влади та державного управління, створити атмосферу незадоволення, посіяти тривогу, сприяти виникненню опозиційних груп та стимулювати антиурядову діяльність.

Для проведення інформаційно-психологічної операції застосовуються заходи впливу на визначені групи людей за допомогою ЗМІ, різного роду друкованої, аудіо- чи відеопродукції, а також шляхом особистого спілкування, щоб викликати у них такі настрої чи поведінку, які забезпечували б досягнення політичних та воєнних цілей. Головними об'єктами впливу вважаються лідери політичних партій, громадських організацій, релігійних общин, найбільш впливові представники бізнесу, військової еліти та творчої інтелігенції. Такі заходи можуть застосовуватися щодо особового складу військових сил, робітників, селян, державних службовців.

*Інформаційна зброя* – це комплекс технічних та інших засобів і технологій, призначених для встановлення контролю над інформаційними ресурсами потенційного супротивника; втручання в роботу його систем управління та інформаційних мереж, систем зв'язку з метою порушення їх працездатності аж до повного виведення з ладу, вилучення, спотворення даних, що містяться в них, або спрямованого введення спеціальної інформації; поширення потрібної інформації та дезінформації в системі формування громадської думки та ухвалення рішень.

Інформаційна зброя здебільшого використовується для дезорганізації систем управління супротивника, передбачає дії на його елементи озброєння, критично важливі інформаційні технології і ресурси, а також захист від аналогічних дій відповідних елементів власної інформаційної структури. При цьому інформаційна зброя не заступає відомі типи озброєння, а лише створює потрібне тло, що знижує потребу в традиційних видах зброї.

Інформаційна зброя відрізняється від звичайного озброєння керованістю, прихованістю, універсальністю, економічністю та тривалістю. Крім того, різні види інформаційної зброї впливають на людську психіку, управлінські та радіоелектронні системи, а також на програмно-технічне оснащення, використовуючи при цьому найбільш відповідні методи впливу.

### *9.2 Об'єкти інформаційного впливу. Інформаційно-психологічна протидія, контроль каналів передачі інформації, система моніторингу та прогнозування негативних інформаційно-психологічних впливів*

Важлива особливість інформаційно-психологічного впливу на індивідуальну свідомість полягає в тому, що людина може не помічати його і не усвідомлювати як загрозу. Поведінкою особи керує її мозок, свідомість. Усе, що спонукає людину до діяльності, має проходити через її мислення. Отже, ІПВ з метою зміни поведінки особистості в бажаному напрямку має домогтися відповідної зміни в її свідомості.

Небезпечний ІПВ на індивідуальну свідомість може призвести до двох видів взаємозалежних змін:

- зміни психіки, психічного здоров'я людини. Оскільки у випадку застосування інформаційного впливу складно визначити межі норми і патології, показником змін може бути втрата адекватності щодо відображення світу у свідомості й індивідуальному ставленні до світу. Можна говорити про деградацію особистості, якщо форми відображення дійсності спрощуються, реакції грубішають і здійснюється перехід від вищих потреб (у самоактуалізації, соціальному визнанні) до нижчих (фізіологічних, побутових);

- зміни в цінностях, життєвих позиціях, орієнтирах, світогляді особистості. Такі зміни спричиняють антисоціальні вчинки і становлять небезпеку вже для всього суспільства і держави.

Для реалізації інформаційно-психологічного впливу на індивідуальну, групову і масову свідомість використовуються наступні джерела, канали поширення і технології (засоби):

засоби масової інформації і спеціальні засоби інформаційно-пропагандистської спрямованості;

глобальні комп'ютерні мережі і програмні засоби швидкого поширення в мережі пропагандистських інформаційних матеріалів;

засоби, що нелегально модифікують інформаційне середовище, на підставі якої людина приймає рішення;

засоби створення віртуальної реальності;

слухи;

засоби підпорогового психосемантичного впливу;

засоби генерування акустичних і електромагнітних полів.

Засоби масової інформації і спеціальні засоби інформаційно-пропагандистської спрямованості. ЗМІ найбільш ефективні для надання інформаційно-психологічного впливу на великі маси людей, що дозволяє розглядати їх як складову частину стратегічних сил інформаційної війни. Використання різних технологій схованого впливу за допомогою звуку і відеозображень на свідомість і підсвідомість людини дозволяє говорити про відповідність подібних засобів по наслідках їхнього застосування.

Самою небезпечною рисою ЗМІ, вважають багато фахівців, є їхня здатність подавати інформацію таким чином, щоб за видимою об'єктивністю у великої маси людей формувалася віртуальна картина реальності. Однак як тільки людина починає сумніватися у віртуальній картині світу, ефективність інформаційно-психологічного впливу різко падає. Ці сумніви можуть бути підтримані технологіями контрпропаганди, також реалізовані за допомогою ЗМІ.

Дієвість ЗМІ як джерела інформаційно-психологічного впливу обумовлена насамперед створенням глобальних систем віщання. Маючи цілком мирне і гуманне застосування в повсякденному житті, вони мають можливість безперешкодно довести сигнал до будь-якої точки світу. Для багатьох регіонів може виявитися, що дане джерело інформації є єдино доступним. Саме володіння державою системами супутникового радіо- і телемовлення можливо буде служити стримуючим чи, навпаки, підсилюючим фактором розв'язання інформаційних воєн.

Сила і результативність інформаційно-психологічного впливу, здійснюваних за допомогою ЗМІ і, насамперед, телебачення, посилюються сильним психологічним ефектом сумісної участі до подій, коли людина занурюється в них «тут і зараз». Цей своєрідний ефект, що одержав назву «ефект CNN», оцінюється багатьма як головна умова ефективності інформаційно-психологічного впливу за допомогою ЗМІ.

До спеціалізованих засобів інформаційно-пропагандистської спрямованості відносяться мобільні радіомовні і телевізійні центри, пропагандистські пересувні гучномовці, плакати, листівки. Технологія їх застосування відпрацьований і подальший розвиток пов'язаний насамперед з методами схованого впливу на підсвідомість людини.

Засоби, що нелегально модифікують інформаційне середовище, на підставі якого людина приймає рішення. Діяльність людини значною мірою спирається на можливості інформаційно-керуючих систем. Для вирішення практичних задач людина намагається зосередити в одному місці якнайбільше інформації для прийняття більш обґрунтованих рішень. При всіх перевагах сучасних комп'ютеризованих систем підтримки прийняття рішень вони мають цілком очевидний недолік — людина приймає рішення на основі тієї інформації, яку надає йому система і вірогідність якої в більшості випадків вона оперативно перевірити не здатна. Посадова особа, що приймає рішення, цілком покладається на ту інформацію, яка

видається йому на монітор, тому внесення навмисних змін в інформаційні масиви і повідомлення спричиняє неправильні рішення.

В даний час у багатьох країнах ведеться розробка спеціалізованих засобів впливу на інформацію в інформаційно-керуючих системах. По результату, який при цьому досягається, ці засоби еквівалентні найдужчим технологіям інформаційно-психологічного впливу.

Засоби створення віртуальної реальності. Потужність мережних технологій збільшується багаторазово завдяки новим технологіям мультимедіа і віртуальній реальності. Віртуальна реальність як імітація дійсності може розглядатися як психологічний інструмент впливу на свідомість і підсвідомість людини. Вона втягує її в нові форми існування й значною мірою може формувати особистість. Можуть виникати і нові форми опосередкованого соціального контролю, засновані на замаскованому маніпулюванні свідомістю, м'якому придушенні психіки, зміні структури особистості.

Соціально-психологічні наслідки розвитку технологій віртуальної реальності, як і взагалі сучасних символічних візуальних систем, у контексті безпеки особистості і суспільства можуть бути негативні. Подібні технології дозволяють з максимальною ефективністю робити інформаційно-психологічний вплив. Вони часто використовуються для підвищення наочності подачі інформації, наприклад у програмах новин. Подібні технології можуть використовуватися для створення будь-якої реальної ситуації, сполучаючи елементи реального відеозображення й елементи, створені комп'ютерною графікою.

Слухи відіграють важливу роль у конфліктах різного роду: міжгрупових, міжнаціональних, міжнародних. Їхня значимість пов'язана з тим, що в у багатьох випадках можливості впливу конфліктуючих сторін одна на одну істотно обмежені як законодавчими рамками, так і суспільною думкою. Крім того, часто результат конфлікту зважується в процесі легітимізації найбільш розповсюдженої в суспільстві точки зору (вибори, референдуми). При цьому зростає значимість тих прийомів інформаційно-психологічного впливу, які пов'язані зі зміною уявлень про конфлікт у більшості в напрямку, вигідному для однієї з конфліктуючих сторін. Подібні зміни здійснюються за допомогою спеціально підібраних відомостей, розповсюджуваних як каналами ЗМІ, так і каналами неформальної комунікації. Саме останніми передаються слухи, які стають серйозною зброєю в політичному чи ідеологічному зіткненні. У порівнянні з використанням ЗМІ використання неформальної комунікації навіть переважніше, оскільки відсутні відомості про їхнього автора. Це зменшує підозри в політичній ангажованості слуху і сприяє тим самим його більшій ефективності.

### *9.3 Принципи, логіка, моделі, різновиди інформаційної війни. Засоби, методи і технології інформаційних воєн.*

Основна мета інформаційної війни є маніпулювання свідомістю суспільства, вплинути на дію противника проти його інтересів, змушення її повного контролю. Завданням такої інформаційно- психологічної війни є знищення соціуму, це як вірус, що знищує та руйнує організм. Інформаційна війна має низку відмінностей від звичайної війни, а саме є її безконтактність, що направлена на фізичне придушення супротивника. Оскільки, інформаційна війна безпосередньо не пов’язана із кровопролиттям та руйнуваннями, досить часто призводить до певного ігнорування та безпечності у ставленні до неї, на початках навіть до переоцінки її впливу на руйнування суспільної психології.

Наслідком інформаційно-психологічної війни є погіршення владно-громадських відносин, що призводять до активізації дій громадянського суспільства проти власних урядів.

Методами інформаційної війни є пропаганда, шпигунство (шпіонаж), диверсії – головне проникнення усередину системи противника, підрив його цілей, поглядів та зміни світосприйняття.

Пропаганда – зумисне фальшиве поширення викривленої інформації та фактів для впливу на масову аудиторію, її емоційний та психологічний стан; зміну суспільної думки в інтересах пропагандиста. Пропаганду можна класифікувати за двома принципами: джерелом повідомлення або ж природою повідомлення.

Шпигунство (шпіонаж) – передавання або збирання з метою передавання іноземній державі, іноземній організації або їх представникам відомостей, що становлять державну таємницю, якщо ці дії вчинені іноземцем або особою без громадянства.

Диверсії – акт зруйнування або пошкодження об'єктів військового, державного значення агентами ворожих країн або народними месниками у тилу окупантів, або військова операція, здійснювана для відвернення уваги противника від місця, де готується головний удар.

Існують такі форми інформаційної війни:

- командно-управлінська, метою якої є знищення каналів зв'язку між командуванням і виконавцями;
- розвідувальна, що передбачає збір важливої і захист власної інформації;
- психологічна, а саме: пропаганда, інформаційна обробка населення, деморалізація;
- хакерська, тобто диверсійні дії та атаки проти ворога шляхом створення спеціальних програм;
- економічна – інформаційна блокада та інформаційний імперіалізм;
- електронна, спрямована проти засобів електронних комунікацій – радіозв'язку, радарів, комп'ютерних мереж;
- кібервійна.

В інформаційній (інформаційно-психологічній) війні інформаційна боротьба здійснюється ворогуючими сторонами у формі проведення таємних інформаційно-психологічних операцій з використанням інформаційної зброї. У процесі проведення інформаційно-психологічної війни держава керується наступними принципами:

1. Використання принципу інформаційної асиметрії, трансформування інформаційного простору супротивника в цілях створення та маскування у його інформаційних об'єктах нових асиметричних рис, вразливих для асиметричної зброї.

2. Прихованість та анонімність оперування інформаційно-психологічними впливами, можливість проведення їх «під чужим прапором» і з будь-якої точки інформаційного простору.

3. «Плавність» переключення інформаційних впливів, регульована в широких межах інтенсивність та тривалість їхньої реалізації: від організації інформаційних «шоків», «ударів», «блокад» до в'ялопротікаючих, латентних, розтягнутих на роки мікродозованих впливів.

4. Багатоаспектність та багатооб'єктність впливу з високою інтенсивністю координації у часі та просторі. Зростаюча пронизаність усіх сфер життя суспільства інформаційними системами та технологіями дає можливість вибудувати інформаційні впливи по прийнятому (з можливістю внесення коректив в реальному часі) алгоритму. Такі впливи здійснюються на різноманітні сфери, процеси, країни, об'єкти, групи, персони одночасно, в потрібній послідовності та під різними кутами зору, що, в свою чергу, дозволяє оптимізувати отримання необхідного кінцевого результату та витрати на його досягнення.

5. Здатність малими інформаційними впливами отримати значні кінцеві результати.

6. Інформатизація як головний резерв посилення ефективності силових (воєнних) акцій.

7. Поширення хаосу у сферах, що піддаються інформаційно-психологічному впливу.

Основним засобом проведення інформаційних війн є інформаційна зброя. Інформаційна зброя має низку особливостей та відмінностей від інших видів зброї. До них

відносяться:

1. Керованість. Інформаційна зброя здійснює вплив на об’єкт у заданий час та у встановлених масштабах.

2. Прихованість. Досить складно визначити момент початку дії та встановити джерело.

3. Універсальність. Можливість ураження різних об’єктів у досить широкому діапазоні.

4. Низька вартість створення та висока ефективність застосування.

5. Доступність. Легке поширення та високий рівень контролю за процесом виконання.

6. Тривалість. Можливість довгострокового застосування інформаційної зброї без втрати ефективності її застосування.

7. Можливість використання у мирний час та раптовість застосування у разі воєнних дій. Всі ці особливості роблять інформаційну зброю надзвичайно небезпечною. Її досить легко замаскувати, наприклад під засоби захисту програмного забезпечення.

Основна небезпека використання інформаційної зброї при веденні інформаційного протиборства полягає в тому, що з’являється можливість вести наступальні дії під маскою анонімності і навіть без офіційного оголошення війни.

Виділяють такі основні види інформаційної зброї:

1. Вплив на людську психіку. До цього типу інформаційної зброї відносяться методи, способи та засоби впливу на психічний стан людини з метою зміни чи підриву цього стану.

2. Дезінформування систем прийняття рішень. До цього типу відносяться методи на групові та індивідуальні системи прийняття рішень, з метою вибору рішення, вигідного дезінформатору.

До основних засобів ведення протиборства зброєю такого типу відносяться засоби інформації, телекомунікаційні системи, засоби зв’язку. Принципова відмінність інформаційного протистояння від звичайної війни полягає в тому, що інформаційне протиборство певною мірою регулюється законодавством. Єдина мета інформаційної зброї – завдання інформаційних систем супротивника найбільшої шкоди. Досягнення цієї мети противники реалізують практично певні завдання.

Що стосується сфери законодавства з проблеми, то можна зробити висновок, що у зв’язку із встановленням інформаційного простору та розвитком інформаційних технологій, структура українського законодавства включає в себе малу кількість нормативно-правових актів.

З розвитком даного сектора база офіційних документів буде поповнюватися, що допоможе покращити контроль за процесом регулювання проведення інформаційного протиборства.

Цілісність сучасного світу забезпечується в основному за рахунок інтенсивного інформаційного обміну. Інформаційна зброя здатна призупинити глобальні інформаційні потоки, що може призвести до глобальної кризи. Для того, щоб розібратися в питанні застосування інформаційної зброї, необхідно виявити сферу її застосування. Найбільш широкодоступною областю є світові інформаційні мережі. Світові інформаційні мережі – це сукупність електронно-обчислювальних машин, що пов’язані між собою каналами телекомунікації. Такі інформаційні мережі дозволяють користувачам обмінюватися інформацією, спільно використовувати необхідні інформаційні ресурси.

Інформаційна війна передбачає різні форми конфлікту, в якій відбуваються прямі атаки на інформаційні системи для впливу на знання або припущення противника. Інформаційна війна може проводитися як частина більшого і більш повного набору військових дій. Таким чином, під загрозою інформаційної війни розуміється намір певних сил скористатися разючими можливостями, прихованими в комп'ютерах, на неозорому кіберпросторі, щоб

вести «безконтактну» війну, в якій кількість жертв (у прямому значенні слова) зведено до мінімуму.

Громадянська інформаційна війна може бути розв'язана терористами, наркотичними картелями, підпільними торговцями зброєю масового ураження. Військові завжди намагалися впливати на інформацію, яку потребував ворог для ефективного управління своїми силами. Зазвичай це робилося за допомогою маневрів і відволікаючих дій. Оскільки ці стратегії впливали на інформацію, що отримує ворог, побічно шляхом сприйняття, вони й атакували інформацію ворога побічно. Тобто, для того, щоб хитрість була ефективною, ворог повинен був зробити три речі: спостерігати обманні дії; порахувати обман правдою; діяти після обману відповідно до цілей того, хто обманює.

Проте, сучасні засоби виконання інформаційних функцій зробили інформацію вразливою до прямого доступу і маніпуляції з нею. Сучасні технології дозволяють противнику змінити або створити інформацію без попереднього отримання фактів та їх інтерпретації. Ось короткий список характеристик сучасних інформаційних систем, що призводить до появи подібної уразливості: концентроване зберігання інформації, швидкість доступу, повсюдна передача інформації, і великі можливості інформаційних систем виконувати свої функції автономно. Механізми захисту можуть зменшити, але не до нуля цю уразливість.

### 9.4 *Інструменти інформаційно-психологічних протиборств*

Початок 21 сторіччя показує, що протиріччя, кількість яких збільшується, вирішується в більшості випадків нетрадиційними методами збройних протистоянь, а з використанням сучасних інформаційних технологій. Тобто переможець у протистоянні визначається за результатом проведення спеціальних операцій, що проводяться у інформаційному просторі, які, у свою чергу, розділяються на інформаційно-кібернетичні операції, що спрямовуються на технічну складову соціотехнічної системи та інформаційно-психологічні операції, що спрямовуються на соціальну складову соціотехнічної системи.

Використовуючи сучасні технології, постійно працюючи у соціальних мережах, отримуючи інформацію з тих чи інших сайтів і таким чином, опосередковано від власних думок і бажань створюється власна інформаційна модель, яка відображає уподобання, пріоритети тощо. Голова Apple відзначає: «Здається, що жодна інформація не є надто особистою чи надто приватною, щоб її не можна було відстежувати, монетизувати і агрегувати, щоб отримати вичерпний огляд всього вашого життя. Підсумок цього – те, що ви більше не клієнт, ви – продукт».

Відповідно проведення ІПО організовуються і проводяться з метою перетворення «суб’єкта-клієнта» на «об’єкт-продукт» інформаційної взаємодії. Відповідно, для досягнення головної мети інформаційного протиборства потрібно вирішити такі задачі.

1) Створення напруги і хаосу, шляхом маніпулювання свідомістю соціуму соціотехнічної системи.

2) Ініціації внутрішніх конфліктів.

3) Зниження рівня інформаційного забезпечення (своєчасності і об’єктивності подання інформації), як органів влади так і безпосередньо населення, з метою зниження керованості процесів життєдіяльності соціуму, підриву довіри до влади тощо.

4) Підрив ефективності функціонування суб’єкта інформаційної взаємодії, в тому числі на міжнародній арені.

5) Нанесення ризиків об’єктам критичної інфраструктури.

Для отримання перемоги у конкурентному інформаційному середовищі потрібно забезпечити максимально можливе охоплення соціуму, а також практично реалізувати прямі чи опосередковані контакти з окремими його елементами. Важливим є те що для рішення наведених задач протиборчим сторонам потрібно мати відповідні ресурси. В першу чергу ці ресурси мають забезпечувати можливість проведення спеціальних ІПО. При цьому потрібно зауважити, що протиборчі сторони мають свої ресурси, процеси, що відбуваються в системах організації і реалізації спеціальних ІПО, внутрішні і зовнішні об'єктно-суб'єктні відносини тощо. Узагальнено можна сказати, що це стан економіки, технологічний стан протиборчої сторони, рівень інформатизації суспільства тощо.

Можна виділити такі основні етапи підготовки та здійснення інформаційно-психологічної операції:

-планування;

-формулювання робочих цілей;

-аналіз об'єкта впливу;

-аналіз конкретних видів, форм, методів інформаційно-психологічного впливу;

-планування контенту інформаційно-психологічного впливу;

-вибір відповідних джерел впливу;

-визначення обмежень та умов здійснення інформаційно-психологічного впливу;

проведення підготовленої інформаційно-психологічної операції;

-аналіз відгуків об'єкта впливу;

-оцінювання ефективності проведення ІПО;

-коригування (за потреби) умов та обмежень здійснення ІПО;

-завершення ІПО.

Очевидно, що наведена алгоритмізація процесу проведення ІПО вимагає побудови організованої системи проведення інформаційного протиборства.

Елементи системи інформаційного протиборства виконують такі операції:

Підготовка інформаційно-психологічної операції: планування операції, формулювання цілей операції, аналіз об'єкта впливу.

Вибір джерела впливу: вибір та підготовка відповідних інформаційних каналів для реалізації ІПО, визначення обмежень та умов здійснення впливу.

Формування контенту та коментарів: формування контенту інформаційно-психологічного впливу та його інформаційного супроводу у вигляді коментарів.

Вибір об'єкта впливу: сегментація і вибір частини соціуму на який відбувається інформаційний вплив.

Аналіз реакції об'єкта впливу: аналіз відгуків об'єкта впливу.

Оцінювання ефективності впливу: оцінювання ефективності реалізованого впливу.

Корегування ІПО: на основі результатів аналізу відгуків об'єкта впливу, а також оцінки ефективності, відбувається корегування умов і обмежень, а також контенту спеціальної інформаційної операції.

### *9.5 Відповідальність за порушення інформаційної безпеки держави*

Законом України «Про захист персональних даних», що поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, персональні дані віднесено до об'єкту захисту. Статтею 5 цього Закону персональні дані за режимом доступу віднесено до інформації з обмеженим доступом. При цьому, згідно з нормами статті 24 Закону України «Про захист персональних даних» володільці, розпорядники персональних даних та треті особи зобов'язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, у тому числі

незаконного знищення чи доступу до персональних даних.

Таким чином, оскільки законодавством персональні дані віднесено до інформації з обмеженим доступом, а також встановлено вимогу щодо їх захисту, то згідно до вимог статті 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» така інформація *(інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом)* повинна оброблятися в автоматизованій *(інформаційній, телекомунікаційній та інформаційно-телекомунікаційній)* системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством. Статтею 9 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

За порушення вимог законодавства передбачена відповідальність:

1. Кодекс України про адміністративні правопорушення:

Стаття 188-31. *Невиконання законних вимог посадових осіб органів Державної служби спеціального зв'язку та захисту інформації України*

Невиконання законних вимог посадових осіб органів Державної служби спеціального зв'язку та захисту інформації України щодо усунення порушень законодавства про криптографічний та технічний захист інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, та законодавства у сфері надання послуг електронного цифрового підпису, а також створення інших перешкод для виконання покладених на них обов'язків - тягнуть за собою накладення штрафу на посадових осіб від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян.

Ті самі дії, вчинені повторно протягом року після накладення адміністративного стягнення, - тягнуть за собою накладення штрафу на посадових осіб від ста до ста п'ятдесяти неоподатковуваних мінімумів доходів громадян.

Стаття 188-39. *Порушення законодавства у сфері захисту персональних даних*

Неповідомлення або несвоєчасне повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних або про зміну відомостей, які підлягають повідомленню згідно із законом, повідомлення неповних чи недостовірних відомостей - тягнуть за собою накладення штрафу на громадян від ста до двохсот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян - суб’єктів підприємницької діяльності - від двохсот до чотирьохсот неоподатковуваних мінімумів доходів громадян.

Невиконання законних вимог (приписів) Уповноваженого Верховної Ради України з прав людини або визначених ним посадових осіб секретаріату Уповноваженого Верховної Ради України з прав людини щодо запобігання або усунення порушень законодавства про захист персональних даних - тягнуть за собою накладення штрафу на громадян від двохсот до трьохсот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян - суб’єктів підприємницької діяльності - від трьохсот до однієї тисячі неоподатковуваних мінімумів доходів громадян.

Повторне протягом року вчинення порушення з числа передбачених частинами першою або другою цієї статті, за яке особу вже було піддано адміністративному стягненню, - тягне за собою накладення штрафу на громадян від трьохсот до п’ятисот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян - суб’єктів підприємницької діяльності - від п’ятисот до двох тисяч неоподатковуваних мінімумів доходів громадян.

Недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення

прав суб’єкта персональних даних, - тягне за собою накладення штрафу на громадян від ста до п’ятисот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян - суб’єктів підприємницької діяльності - від трьохсот до однієї тисячі неоподатковуваних мінімумів доходів громадян.

Повторне протягом року вчинення порушення, передбаченого частиною четвертою цієї статті, за яке особу вже було піддано адміністративному стягненню, - тягне за собою накладення штрафу від однієї тисячі до двох тисяч неоподатковуваних мінімумів доходів громадян.

Стаття 188-40. *Невиконання законних вимог Уповноваженого Верховної Ради України з прав людини*

Невиконання законних вимог Уповноваженого Верховної Ради України з прав людини або представників Уповноваженого Верховної Ради України з прав людини - тягне за собою накладення штрафу на посадових осіб, громадян - суб'єктів підприємницької діяльності від ста до двохсот неоподатковуваних мінімумів доходів громадян.

2. Кримінальний кодекс України:

Стаття 182. *Порушення недоторканності приватного життя*

1. Незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації, крім випадків, передбачених іншими статтями цього Кодексу, - караються штрафом від п'ятисот до однієї тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або арештом на строк до шести місяців, або обмеженням волі на строк до трьох років.

2. Ті самі дії, вчинені повторно, або якщо вони заподіяли істотну шкоду охоронюваним законом правам, свободам та інтересам особи, - караються арештом на строк від трьох до шести місяців або обмеженням волі на строк від трьох до п'яти років, або позбавленням волі на той самий строк.

Примітка. Істотною шкодою у цій статті, якщо вона полягає у заподіянні матеріальних збитків, вважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян.

Стаття 361. *Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку*

1. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, - карається штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, - караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи.

Стаття 361-2. *Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації*

1. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства, - караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до двох років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, - караються позбавленням волі на строк від двох до п'яти років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи.

Стаття 362. *Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї*

1. Несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, - караються штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років з конфіскацією програмних або технічних засобів, за допомогою яких було вчинено несанкціоновані зміна, знищення або блокування інформації, які є власністю винної особи.

2. Несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації, - караються позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк та з конфіскацією програмних чи технічних засобів, за допомогою яких було здійснено несанкціоновані перехоплення або копіювання інформації, які є власністю винної особи.

3. Дії, передбачені частиною першою або другою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, - караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років та з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані дії з інформацією, які є власністю винної особи.

Стаття 363. *Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється*

Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію, - караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк.

Відповідальність за порушення законодавства про державну таємницю:

Посадові особи і громадяни винні у порушенні обов'язків щодо збереження державної таємниці, розголошенні державної таємниці, недотриманні обмежень щодо передачі державної таємниці, несуть відповідальність згідно з законодавством.

Стаття 422. ККУ: Розголошення відомостей військового характеру, що становлять державну таємницю, за відсутності ознак державної зради – карається позбавленням волі на строк від двох до п'яти років.

При сучасному високому технічному оснащенні армій розвинених держав засобами радіоелектронної боротьби важливе значення набуває така властивість зв’язку, як її безпека.

Безпека характеризує спроможність зв’язку забезпечити зберігання в таємниці від противника змісту переданих (прийнятих) повідомлень і протистояти введенню хибної інформації.

В оперативній ланці управління інформація з управління військами повинна передаватися з гарантованою стійкістю засекречування, а в тактичній ланці, де інформація старіє значно швидше, вона може передаватися і з тимчасовою стійкістю засекречування, зберігаючи високу оперативність управління.

Для передавання повідомлень відкритими каналами зв’язку повинні використовуватися засоби попереднього шифрування й кодування, а в тактичній ланці управління - з використанням документів прихованого управління військами. Ці ж засоби служать і для приховування від обслуговуючого особового складу змісту документів які передаються відкритими каналами зв’язку.

### *9.6 Способи та форми ведення інформаційної боротьби. Методологія оцінки ефективності інформаційної боротьби*

Мета інформаційної боротьби в широкому розумінні – забезпечення воєнно–політичних, економічних і військових інтересів країни за рахунок досягнення й утримання інформаційної переваги на найбільш важливих (чутливих, уразливих) в конкретних умовах напрямах. Вона не може бути досягнутою на всіх напрямах інформаційної боротьби. Навіть найрозвиненіша в інформаційному значенні країна, якою сьогодні є США, не спроможна забезпечити абсолютну перевагу в інформаційній боротьбі. Тому дуже важливим є пошук і виявлення найбільш уразливих, з погляду інформаційного впливу місць, найбільш значущих для досягнення мети як у себе, так і в протидіючої сторони, та концентрація зусиль (сил і засобів інформаційної боротьби) з метою інформаційного захисту своїх військ і населення від інформаційного впливу протидіючої сторони.

Метою інформаційної боротьби у вузькому розумінні – створення сприятливих умов для успішного проведення операцій і бойових дій, ефективного застосування своїх військ (сил), озброєння і військової техніки, а також зниження ефективності застосування військ (сил) і зброї противника через захоплення й утримання інформаційної переваги над противником під час підготовки й у ході воєнних (бойових) дій опосередкованим введенням протидіючої сторони в поле свого управління на інформаційному рівні. Цю мету можна досягти, забезпечуючи перевагу над протидіючою стороною у розв’язанні взаємопов’язаних комплексів завдань. Комплекси завдань інформаційної боротьби:

цілеспрямоване добування інформації про поточну ситуацію з жорсткими вимогами до її своєчасності, якості, обсягу й темпу відновлення та оцінка на її основі стратегічної, оперативно–тактичної, тактичної, політичної (воєнно–політичної, воєнної, економічної, соціальної тощо) обстановки;

цілеспрямований і комплексний вплив на свідомість та підсвідомість населення й особового складу, на інформаційні ресурси на всіх фазах їх виробництва, розповсюдження і

використання, а також на інші складові інформаційного середовища протидіючої сторони в інтересах нав'язування їй бажаних рішень і управління її поведінкою;

захист власних інформаційних ресурсів та інших складових інформаційного середовища, у тому числі на рівні свідомості та підсвідомості людини від впливу на них протидіючою стороною.

Взаємопов'язаність наведених комплексів завдань інформаційної боротьби виявляється в тому, що грамотне вирішення завдань першого і третього комплексів неможливе без знань про те, яким чином протидіюча сторона вирішує завдання другого комплексу, а ефективне вирішення завдань другого комплексу неможливо без знань про сили, засоби, методи, алгоритми вирішення протидіючою стороною завдань першого і третього комплексів, а також про її знання (інформаційне уявлення) про проблемну ситуацію.

Сутність інформаційної боротьби схематично показано на рис. 9.1

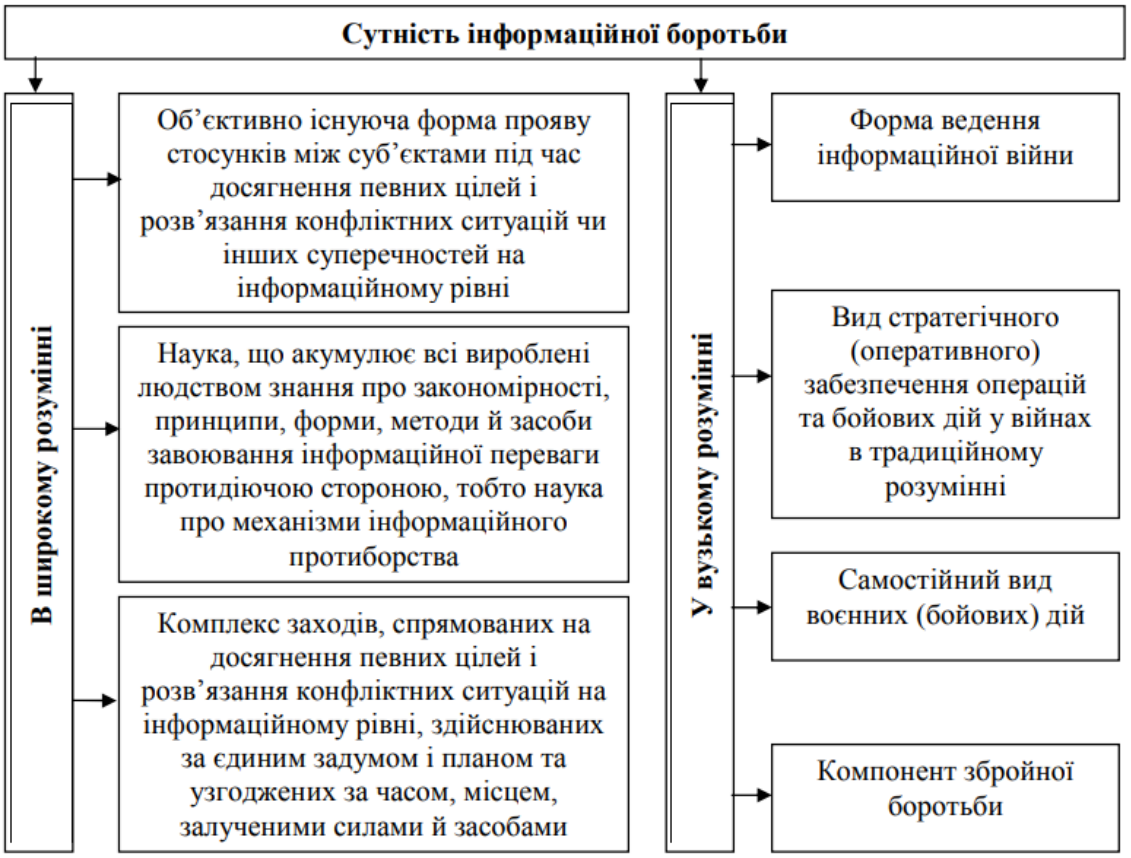



Рис. 9.1 – Сутність інформаційної боротьби

Специфікою інформаційної боротьби є те, що вона виступає як самостійний вид, так і як складовий елемент будь–якого іншого різновиду боротьби (збройної, ідеологічної, економічної тощо). Вона ведеться постійно – як за мирного, так і за воєнного часу. Масштаби інформаційної боротьби такі грандіозні, що її підготовка й організація не можуть бути спонтанними. Вона повинна мати плановий, систематичний характер.

За мирного часу інформаційна боротьба має прихований характер. Основний зміст її – ведення розвідувальних і політико–психологічних дій стосовно противника, а також здійснення заходів щодо забезпечення своєї інформаційної безпеки. Зростаючу роль на цьому етапі відіграють засоби спеціального програмно–математичного впливу на інформаційний ресурс технічних систем противника.

У цей період можуть також вирішуватися питання створення, розвитку, підтримання в потрібних ступенях бойової готовності та відпрацювання планів ефективного бойового

використання інформаційних ресурсів своїх військ (сил), а також своєчасного й достовірного викриття і нейтралізації інформаційного впливу протидіючої сторони. У загрозливий період до наведених завдань додаються й такі, що виконуються в інтересах забезпечення потрібної ефективності запланованих операцій (бойових дій). У повному обсязі розгортається інфраструктура системи керування запланованого для бойових дій угруповання військ (сил) з урахуванням забезпечення її максимальної скритності. У цей період ведення інформаційної боротьби має особливості, основні з яких показано на рис. 9.2

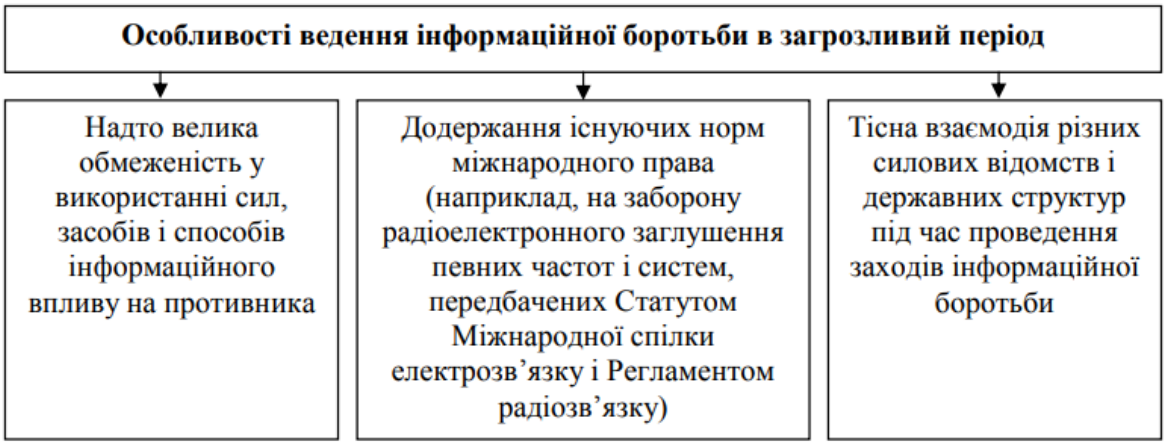



Рис. 9.2 – Особливості ведення інформаційної боротьби в загрозливий період

З початком воєнних дій сили й засоби інформаційної боротьби виконують завдання, основні з яких наведено на рис. 9.3

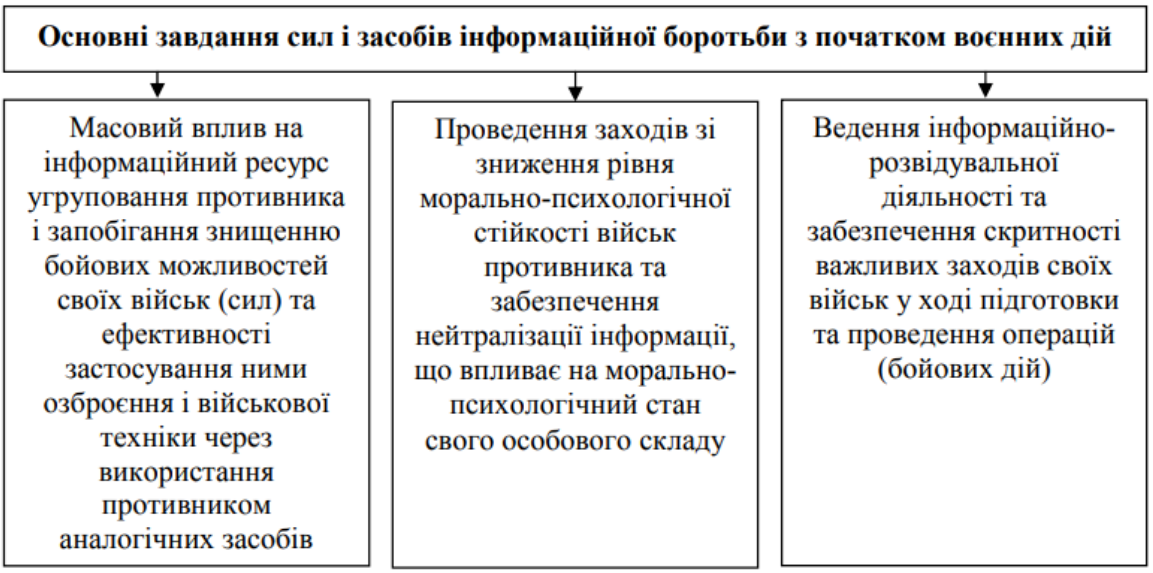



Рис. 9.3 – Основні завдання сил і засобів інформаційної боротьби з початком воєнних дій

Під час проведення заходів інформаційної боротьби у визначений період надзвичайно важливо не допустити випадкового впливу своїх засобів на об'єкти своєї інформаційної інфраструктури. Невід'ємними компонентами інформаційної боротьби, як і збройної, є оцінка обстановки, захист і напад, які за своєю взаємопов'язаною сукупністю становлять її триєдину сутність. Оскільки інформаційна боротьба, аналогічно збройній, має цілеспрямований характер і підпорядкована цілям і завданням операцій і бойових дій, то її складовою є управління військами (силами) і засобами інформаційної боротьби.

Основні форми ведення інформаційної боротьби:

*Інформаційний вплив* – це організоване застосування сил і засобів інформаційної

боротьби для розв'язання завдань завоювання (підтримання) інформаційної переваги над стороною, що протистоїть.

*Інформаційна атака* є сукупністю активних інформаційних впливів сил і засобів окремих підрозділів на елемент або групу елементів інформаційних систем сторони, що протистоїть, з метою виконання поодиноких тактичних завдань інформаційної боротьби.

*Інформаційна битва* – це сукупність різних інформаційних впливів і атак, що об'єднані спільним задумом, проводяться спеціально виділеними силами й засобами і спрямовані на виконання одного оперативного завдання інформаційної боротьби.

*Інформаційна операція* – сукупність узгоджених за метою, завданням, місцем та часом інформаційних впливів, атак і битв, що проводяться за єдиним задумом і планом для виконання завдань інформаційної боротьби на стратегічному чи оперативному напрямах.

Для досягнення мети інформаційного впливу, атак, битв і операцій застосовується уся сукупність способів інформаційної боротьби.

Під способом інформаційної боротьби розуміється порядок та заходи застосування сил і засобів для захоплення й утримання інформаційної переваги над противником під час підготовки та в ході бойових дій. Спосіб інформаційної боротьби охоплює вид і послідовність інформаційного впливу на противника, об'єкти впливу, склад сил і засобів, що виділяються для ведення інформаційної боротьби, та їх оперативну побудову (бойовий порядок).

Зміст способу відзначається великою різноманітністю, пов’язаною з тим, що одна й та сама інформація може формуватися й доводитись до органів керування за допомогою різних сил і засобів.

Способи інформаційної боротьби поділяються на три основні категорії: силові, інтелектуальні та комбіновані (цей розподіл має більш методичне значення, оскільки на реалізацію рефлексивного управління протидіючою стороною можуть бути спрямовані способи різних категорій). До силових належать способи, що полягають в ураженні об'єктів інформаційної боротьби різними видами зброї (звичайної, радіоелектронної, інформаційної).

Застосування силових способів дає змогу досягнути інформаційної переваги в обсязі інформації, потрібної для виконання завдань керування військами (силами). Інтелектуальні способи мають на меті реалізацію рефлексивного керування противником. Їх застосування дозволяє досягнути інформаційної переваги за допомогою інформації, яка використовується для керування військами (силами).

До комбінованих належать способи, що забезпечують досягнення інформаційної переваги як в обсязі, так і в якості інформації про обстановку. В інформаційній боротьбі (за аналогією зі збройною) можна виокремити дві основні групи способів — наступальну й оборонну.

Наступальними можна вважати такі способи, як блокування, відволікання, сковування, виснаження, інсценування, дезінтеграція, умиротворення, залякування, провокування, переобтяження, навіювання і тиск, а оборонними – деблокування й ототожнення. Запорукою успіху інформаційної боротьби є максимальна можливість та одночасність застосування всіх її форм і способів.

Оцінка ефективності інформаційної боротьби – визначення ступеня відповідності результатів інформаційної боротьби її меті (цілі).

Метод оцінки ефективності інформаційної боротьби – це сукупність способів, прийомів визначення кількісних значень показників інформованості протидіючих сторін та розрахунку ступеня інформаційної переваги однієї з них над іншою у відповідності до мети інформаційної боротьби. В основу методу може бути покладене математичне моделювання процесу забезпечення інформацією органів управління протидіючих сторін.

Методика оцінки ефективності інформаційної боротьби включає ряд взаємозв’язаних

етапів оцінки ефективності інформаційної боротьби:

- формування інформаційного кадастру органів керування протиборчих сторін;
- оцінку характеристик інформації про обстановку, що поступає в органи керування, Її селекцію і класифікацію;
- порівняльну оцінку величини показника інформованості органів керування своїми силами і засобами і силами і засобами противника.

## ПИТАННЯ ДЛЯ САМОПЕРЕВІРКИ

1. Охарактеризуйте сутність понять «інформаційний вплив», «інформаційна операція», «інформаційна війна», «інформаційна зброя».
2. Вкажіть об’єкти інформаційного впливу.
3. Які канали передачі інформації Ви знаєте та хто повинен здійснювати їх контроль?
4. Обґрунтуйте необхідність прогнозування негативних інформаційно-психологічних впливів.
5. Які характерні особливості має інформаційно-психологічна протидія?
6. Назвіть засоби, методи і технології ведення інформаційних воєн.
7. Які різновиди інформаційної війни Ви знаєте?
8. Які інструменти інформаційно-психологічних протиборств є найдієвішими в умовах воєнного стану?
9. Яка відповідальність, відповідно до законодавства, настає за порушення інформаційної безпеки держави?
10. Окресліть способи та форми ведення інформаційної боротьби.
11. Охарактеризуйте складові методології оцінки ефективності інформаційної боротьби.

# ЛЕКЦІЯ 10
# НОРМАТИВНО-ПРАВОВЕ ТА ІНСТИТУЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

**План викладу:**

10.1 Система та державна політика забезпечення інформаційної безпеки України: основні загрози національній безпеці.

10.2 Мета функціонування, завдання та основні функції системи забезпечення інформаційної безпеки України.

10.3 Політика інформаційної безпеки та її реалізація в законодавстві.

10.4 Особливості адміністративно-правового забезпечення інформаційної гігієни в умовах сучасної України.

10.5 Інституційне забезпечення інформаційної безпеки України.

10.6 Реальні та потенційні загрози інформаційній безпеці України.

## *10.1 Система та державна політика забезпечення інформаційної безпеки України: основні загрози національній безпеці*

Зростання залежності сучасного суспільства від стійкого функціонування інформаційної інфраструктури робить реалізацію національних інтересів України в інформаційній сфері важливим фактором національної безпеки. Тож для України нині необхідним кроком на шляху до інформаційного майбутнього є розроблення цілісної гнучкої динамічної державної політики у сфері забезпечення інформаційної безпеки, яка враховуватиме багатоаспектність явища інформаційної безпеки, перспективні тенденції змін інформаційного простору, особливості геополітичного становища, економічного стану країни і знайде своє відображення у суспільній свідомості.

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, Ебанкінг, 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).

Державна політика 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 соціальнопсихологічного характеру.

Основною метою державної політики у сфері забезпечення інформаційної безпеки при цьому є управління реальними та потенційними загрозами з метою створення необхідних умов для задоволення інформаційних потреб людини та громадянина, а також реалізації національних інтересів.

Державна політика у сфері забезпечення інформаційної безпеки України – це діяльність державно-правових інституцій щодо управління реальними та потенційними загрозами та небезпеками з метою задоволення інформаційних потреб людини та громадянина, а також реалізації національних інтересів, тож державна інформаційна політика та державна політика у сфері забезпечення інформаційної безпеки співвідносяться як ціле та частина. Отже, інформаційна безпека забезпечується проведенням єдиної державної політики в інформаційній сфері, системою заходів економічного, політичного й організаційного характеру, які є адекватними загрозам національній безпеці, а також можливостям держави щодо здійснення управління відповідними ризиками.

Система забезпечення інформаційної безпеки є інструментом реалізації державної політики у сфері забезпечення інформаційної безпеки. Головне призначення цієї системи полягає у досягненні цілей національної безпеки в інформаційній сфері, а отже, її основною функцією є забезпечення збалансованого існування інтересів особи, суспільства і держави в інформаційній сфері. Державна політика у сфері забезпечення інформаційної безпеки має три основних вектори: захист інформаційних прав і свобод людини, захист державної безпеки в інформаційній сфері та захист національного інформаційного ринку, економічних інтересів держави в інформаційній сфері, національних виробників інформаційної продукції.

Предметом інформаційної політики держави слід вважати:

– тенденції і закономірності розвитку інформаційної сфери, суспільних інформаційних відносин та інформаційних процесів, а також засоби й методи їх аналізу та прогнозування;

– дослідження впливу ЗМІ та засобів масової комунікації на свідомість мас, суспільство в цілому (зокрема, і громадянське) та державу разом із механізмами цього впливу.

Для глибшого аналізу інформаційної політики держави визначимо ті родові ознаки й форми, що їм відповідають, які стануть основою класифікації її конкретних проявів. На підставі цього можна виділити важливі для групування ознаки (підстави).

1. Суб’єктний зміст інформаційної політики держави – об’єднує види й відповідні форми інформаційної політики залежно від її суб’єкта й, отже, від того, чиї інтереси відображатимуться у най найбільшою мірою: міжнародна інформаційна політика (рівень держав); партійна (пов’язана з лобіюванням); інформаційна політика спільнот (груп) різного рівня: національна, класова, елітарна тощо.

2. Часовий вимір розглядуваної політики − ознака, за якою види і відповідні форми цієї політики групуються залежно від тривалості політичного процесу, а також від завдань і цілей цієї політики, що вміщуються в певному часовому відрізку: колишня, сучасна і майбутня; тактична, стратегічна, довгострокова, короткострокова, оперативна тощо.

3. Територіально-просторовий вимір такої політики – ознака, за якою види і відповідні форми цієї політики об’єднуються залежно від території її поширення (чи просторової зони). За цією ознакою можна виокремити такі різновиди інформаційної політики: локальна;

субрегіональна; регіональна; глобальна.

4. Спрямованість інформаційної політики держави щодо громадського прогресу − підстава групування видів, напрямів і відповідних форм цієї політики за ступенем (мірою) відповідності її змісту інтересам прогресу суспільства. За цією ознакою розрізняють реакційну, консервативну та прогресивну політики.

5. Методи провадження розглядуваної політики − підстава групування видів, напрямів і відповідних форм цієї політики за способами її реалізації.

Інформація відіграє дедалі вагомішу роль в управлінні суспільством і всіма життєвими сферами. Водночас у процесі формування інформаційного суспільства відкритість інформації для громадян стає дедалі важливішою обставиною, а інформація, у свою чергу, перетворюється на неодмінний атрибут управління в цілому. За тим самим принципом інформаційне управління стає невід'ємною складовою інформаційного суспільства.

В інформаційній політиці держави можна виокремити дві головні складові – техніко-технологічну та гуманітарну. Перша із них стосується: вирішення завдань щодо подальшого перетворення суспільства на дійсно інформаційне; розроблення нових інформаційно-комунікаційних технологій і їх використання; створення відповідної конкурентоспроможної інфраструктури. До гуманітарної складової розглядуваної політики держави належать зміст і якість інформації, використовувані в ній поняття, вплив цієї політики на політичні, соціальні та інші процеси в суспільстві тощо. Через це гуманітарну складову державної інформаційної політики доречно визнати визначальною (рис. 10.1).

Рис.10.1 – Модель вдосконалення державної інформаційної політики

***10.2 Мета функціонування, завдання та основні функції системи забезпечення інформаційної безпеки України***

Ефективність системи управління національними інформаційними ресурсами та їхнім захистом значною мірою визначає загальний рівень національної безпеки, а будь-які недоліки

в структурі й функціонуванні системи управління цими процесами призводять до непоправних збитків суспільству й державі.

Визначальним елементом створення будь-якої системи є її мета. Отже, очевидним є розгляд даного компоненту і при створенні системи забезпечення інформаційної безпеки України. Мета функціонування системи забезпечення інформаційної безпеки полягає:

1) в організації управління системою інформаційної безпеки через ефективне функціонування самої системи її забезпечення;

2) у створенні необхідних економічних і соціокультурних умов та правових і організаційних механізмів формування, розвитку і забезпечення ефективного використання національних інформаційних ресурсів в усіх сферах життя і діяльності громадянина, суспільства й держави.

Для досягнення поставленої мети на систему забезпечення інформаційної безпеки покладаються певні завдання. Головним завданням системи забезпечення інформаційної безпеки України є створення умов для організації управління системою інформаційної безпеки. До основних завдань системи забезпечення інформаційної безпеки відносять:

– забезпечення інформаційної безпеки усіх складових елементів системи управління НБ;

– забезпечення інформаційно-аналітичного потенціалу країни;

– реалізація державної політики інформаційної безпеки в рамках реалізації політики національної безпеки;

– ведення активної розвідувальної, контррозвідувальної і оперативно-розшукової діяльності з метою забезпечення інформаційної безпеки через здобуття необхідної інформації для відпрацювання стратегічних, тактичних і оперативних рішень у сфері управління інформаційною безпекою та вироблення механізмів їх реалізації;

– виявлення, попередження і припинення розвідувальної та іншої, спрямованої на нанесення шкоди інформаційній безпеці України, діяльності спеціальних служб, а також окремих осіб чи організацій;

– виявлення, попередження і припинення інформаційного тероризму та іншої діяльності, спрямованої на підрив функціонування системи управління НБ;

– моніторинг (спостереження, оцінка та прогноз) стану інформаційної безпеки у зв'язку із впливом загроз та небезпек як зсередини, так і ззовні системи управління НБ;

– протидія технічному проникненню до інформаційних систем об'єктів інформаційної безпеки з метою вчинення злочинів, проведення диверсійно-терористичної та розвідувальної діяльності;

– запобігання можливої протиправної та іншої негативної діяльності суб'єктів системи забезпечення національної безпеки зсередини системи їй на шкоду;

– забезпечення збереження державної таємниці;

– організація демократичного цивільного контролю за функціонуванням системи управління НБ тощо.

Відповідно до окресленої мети і завдань доцільно визначити функції системи забезпечення інформаційної безпеки України.

Під функціями системи забезпечення інформаційної безпеки розуміється здійснення суб'єктами системи забезпечення інформаційної безпеки України діяльності зі створення умов для оптимального управління системою інформаційної безпеки. До основних функцій СЗІБ належать: розробка й прийняття політичних рішень, законодавчих і нормативно-правових актів щодо забезпечення системи управління національними інформаційними ресурсами та удосконалення механізмів реалізації правових норм чинного законодавства; визначення та здійснення повноважень системою управління НБ щодо оперативного управління (володіння, розпорядження, користування) державними інформаційними ресурсами. А також, розробка та

реалізація організаційних заходів і нормативно-методичного забезпечення відомчих і регіональних структур у сфері формування та використання інформаційних ресурсів за умови координації діяльності згаданих структур; розробка і реалізація фінансово-економічних засад регулювання процесів формування та використання інформаційних ресурсів; здійснення державної реєстрації інформаційних ресурсів, забезпечення повноти створення первинних і похідних інформаційних ресурсів на засадах використання інформації, що виникає (створюється) у процесі діяльності об'єктів інформаційної безпеки.

Крім того, введення технологічно та методологічно єдиних засад формування інформаційних ресурсів за результатами діяльності структурних компонентів системи управління НБ (крім інформаційних ресурсів, що мають відомості, віднесені до державної таємниці та до іншої інформації з обмеженим доступом); забезпечення ефективного використання інформаційних ресурсів у діяльності об'єктів інформаційної безпеки; оптимізація державної політики інформатизації щодо забезпечення науково-технічних, виробничо-технологічних і організаційно-економічних умов створення та застосування інформаційних технологій, інших елементів інформаційної інфраструктури для формування, розвитку й ефективного використання інформаційних ресурсів і сприяння доступу об'єктів інформаційної безпеки до світових інформаційних ресурсів, глобальних інформаційних систем.

Перелік основних функцій СЗІБ також охоплює: забезпечення функціонування ефективно діючої комплексної системи захисту інформаційних ресурсів системи управління НБ; забезпечення захисту системи управління НБ від хибної, спотвореної та недостовірної інформації; забезпечення розробки та застосування правових, організаційних і економічних механізмів стосовно форм та засобів обігу інформаційних ресурсів України (ринку інформації, інформаційних технологій, засобів обробки інформації та інформаційних послуг); регулювання інформаційного співробітництва, спрямованого на забезпечення рівноправного і взаємовигідного використання національних інформаційних ресурсів у процесі міжнародного обміну; здійснення єдиної державної політики наукової підтримки системи управління формуванням, розвитком і використанням національних інформаційних ресурсів; кадрове забезпечення функціонування системи управління НБ національними інформаційними ресурсами; організаційно-управлінське та адміністративно-правове забезпечення функціонування системи управління НБ; інформаційно-аналітичне забезпечення прийняття управлінських рішень у сфері управління інформаційними ресурсами; контроль за встановленим порядком і правилами формування, розвитку і використання інформаційних ресурсів; нагляд за додержанням законодавства у сфері формування, розвитку, використання інформаційних ресурсів та здійснення правосуддя у сфері суспільних інформаційних відносин.

### *10.3 Політика інформаційної безпеки та її реалізація в законодавстві*

Зважаючи на особливі умови і ведення проти нашої держави агресивної інформаційної війни не лише на її території, але й у світі, забезпечення реалізації Стратегії інформаційної безпеки можливе лише за умови належної координації заходів, здійснюваних усіма державними органами.

Участь у забезпеченні захисту українського інформаційного простору від пропагандистської аудіовізуальної та друкованої продукції держави-агресора, розробленні пріоритетів і стимулів розвитку українського кіно, телевізійного контенту, книгодрукування, зокрема, щодо висвітлення героїчного спротиву українського народу російській агресії також беруть Міністерство культури України, Національна рада України з питань телебачення і радіомовлення, Державний комітет телебачення і радіомовлення України відповідно до їх

компетенції.

Їх перелік схематично зображено на рис.10.3.

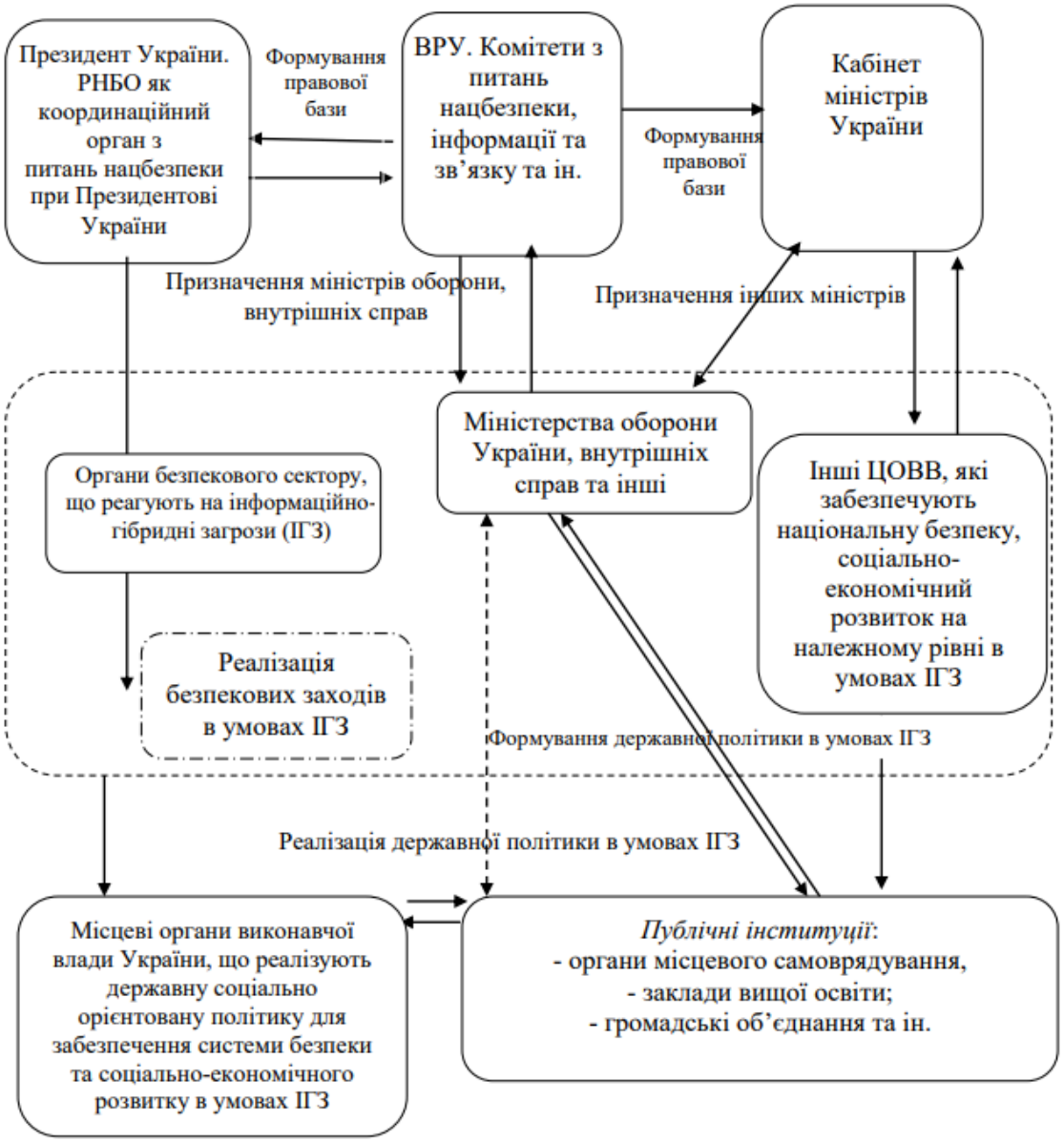



Рис. 10.3 – Суб'єкти реалізації державної інформаційної політики

До головних завдань системи забезпечення інформаційної безпеки належать:

прогнозування ризиків реалізації державної внутрішньої і зовнішньої політики, міждержавних та державних програм і проектів;

виявлення внутрішніх і зовнішніх потенційних і реальних загроз;

розроблення і впровадження адекватних заходів і засобів реагування на виклики як історичного походження, так і сучасного цивілізаційного розвитку;

нейтралізація або послаблення дії проявів гібридної війни та інших загроз національній безпеці України.

Системний і комплексний підхід до вирішення цих завдань має відповідним чином визначати спрямування державної політики у сфері забезпечення інформаційної безпеки нашої держави. У процесі реалізації державної політики у сфері безпеки необхідно звернути увагу на: розроблення й реалізацію комплексних заходів щодо запобігання, нейтралізації й випередження негативних інформаційно-психологічних впливів на суспільство і державу; підготовку суспільства до активної інформаційної протидії; входження національного

інформаційного поля у світовий інформаційний простір; удосконалення системи масової інформації й комунікації; формування системи підготовки кадрів для інформаційно-психологічної протидії; духовну консолідацію суспільства і віднайдення всіма верствами населення нової соціальної ідентичності. За сучасних умов інформаційна безпека має визнаватися основою інформаційної складової частини усіх сфер забезпечення національної безпеки.

Систему забезпечення інформаційної безпеки в інтернет просторі формує:

1) сукупність нормативно-правових актів, до якої входить Конституція України, закони України, підзаконні нормативні акти, що стосуються даної сфери;

2) діяльність державних органів, уповноважених законом на проведення роботи із забезпечення інформаційної безпеки в інтернет просторі;

3) діяльність користувача інтернет простору.

Найвищу юридичну силу має Конституція України, яка гарантує людині основні її права та свободи, їх неухильне дотримання з боку держави. Одним із таких прав є право на доступ до інформації: кожний має право вільно збирати, зберігати, використовувати і поширювати інформацію. Це право також закріплено у ЗУ «Про інформацію», «Про доступ до публічної інформації», «Про звернення громадян», «Про захист персональних даних», «Про захист інформації в інформаційно-телекомунікаційних системах», Постанова КМУ «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», а також підзаконні нормативно-правові акти, що стосуються доступу до інформації – це інструкції, програми, галузеві стандарти, спрямовані на реалізацію права на доступ до інформації.

Однак вітчизняні нормативно-правові акти, що стосуються забезпечення інформаційної безпеки в інтернет просторі, не відповідають перш за все вимогам часу (через стрімкий розвиток інформаційних технологій, вони не можуть ефективно регулювати відносини, що виникають у цій сфері).

Забезпечення інформаційної безпеки є визначальним напрямом державної політики, від якого залежатиме існування суверенної і незалежної держави, її національна безпека, соціально-економічний розвиток та відповідне місце у світовому співтоваристві. Державна інформаційна політика на сучасному етапі має вирішувати завдання, що передбачають гармонійне забезпечення інформаційної безпеки держави, особи і суспільства з одночасним виокремленням нагальних пріоритетів, до яких варто віднести створення/відновлення основних точок захисту системи національної безпеки в інформаційній сфері, ефективної системи інформаційної безпеки держави, перегляд списку нових інформаційних загроз, усунення наявних із визначенням ступеня можливих наслідків та рівнів їх інтенсивності.

### *10.4 Особливості адміністративно-правового забезпечення інформаційної гігієни в умовах сучасної України*

Діяльність державних органів, уповноважених законом на проведення роботи із забезпечення інформаційної безпеки в інтернет просторі, спрямована на моніторинг інтернет простору з метою забезпечення безпеки людини та держави у сфері комп’ютерних технологій. Ці органи та їх посадові особи наділені всіма правами, необхідними для якісного виконання покладених на них обов’язків. Сюди можемо віднести:

1) Міністерство цифрової трансформації України, основним завданням якого є діджиталізація країни, забезпечення безпеки персональних даних кожного користувача інтернету;

2) силові відомства: СБУ, МВС, зокрема підрозділи кіберполіції, їх діяльність спрямована на реалізацію державної політики у сфері протидіїкіберзлочинності.

Предметом розгляду правового забезпечення інформаційної безпеки є не тільки сама діяльність, але й елементи, включені до системного подання цієї діяльності, тобто повна схема кооперації діяльностей учасників взаємодії при здійсненні такої діяльності – це:

- правозастосовна діяльність органів державної виконавчої влади на які покладено завдання із забезпечення інформаційної безпеки, які виконують її основні функції;
- діяльність суб'єктів діяльності із забезпечення інформаційної безпеки, яка залучається до системи діяльності органів державної влади на які покладено завдання із забезпечення інформаційної безпеки;
- правотворча діяльність з питань формування та реалізації інформаційної політики щодо забезпечення інформаційної безпеки;
- діяльність фахівців, які виконують забезпечувальні (ресурсні) функції із забезпечення інформаційної безпеки;
- діяльність адміністрації органів державної виконавчої влади на які покладено завдання із забезпечення інформаційної безпеки з організовування, керівництва та управління діяльністю їх органів та підрозділів на різних рівнях системи.

Діяльність держави, спрямована на правове забезпечення інформаційної безпеки в інтернет просторі, об'єднує у собі як правотворчу, так і правозастосовну діяльність. Правотворча діяльність у цій сфері – це діяльність, спрямована на формування нормативно-правової бази такого рівня, який дозволяв би максимально ефективно використовувати інтернет простір, гарантуючи правовий захист людини і держави. Правозастосовна діяльність полягає в забезпеченні ефективної реалізації державної політики у сфері забезпечення інформаційної безпеки.

Тому, для забезпечення інформаційної безпеки ... необхідно визначити ряд основних завдань з реалізації державної інформаційної політики та забезпечення інформаційної безпеки України, таких як:

забезпечення постійного об'єктивного моніторингу інформаційного простору (внутрішнього і зовнішнього), систематичний аналіз результатів моніторингу;

чітке визначення єдиного загально-державного стратегічного наративу та особливостей його трактування різними державними інституціями України;

створення механізмів унеможливлення відхилення від наративу при здійсненні інформаційної діяльності різними державними інституціями;

скоординована діяльність в інформаційному просторі всіх державних інституцій України;

реалізація принципів та методології стратегічних комунікацій всіма державними інституціями, які здійснюють інформаційну діяльність;

виявлення, оцінювання та прогнозування наслідків загроз національним інтересам та національній безпеці України в інформаційній сфері;

протидія інформаційним впливам на населення України ...;

захист об'єктів критичної інформаційної інфраструктури України (зокрема від кібератак);

підвищення медіаграмотності населення України.

Отже, якісне виконання завдань допоможе зробити систему забезпечення інформаційної безпеки в інтернет просторі справді ефективною, адже окрім моніторингу та виявлення інформаційних загроз, з'явиться реальна можливість протидіяти цим інформаційним загрозам.

Протидія інформаційним загрозам повинна являти собою чітку та послідовну державну політику в усіх сферах життєдіяльності суспільства та держави, її мета – підвищення, а іноді й формування, у населення основ медіаграмотності. З цього приводу

варто нагадати загальнонаціональний проект з медіагрмамотності «Фільтр». Проект реалізовується у трьох напрямках: посилення комунікації з боку держави, розвиток медіаосвіти, стимулювання відповідального та безпечного медіасередовища.

Його мета – посилення усвідомленого ставлення населення до споживаної інформації. Вкрай важливим цей проект є для вчителів загальноосвітніх навчальних закладів, адже загальнонаціональний карантин та перехід на дистанційну форму навчання (на тривалий час) показав, що рівень їх медіаграмотності, а відповідно й інформаційної безпеки, є вкрай низьким. Поряд із позитивними зрушеннями в сфері забезпечення інформаційної безпеки ми все ж спостерігаємо і ті тенденції інтернет простору, які несуть небезпеку як людині, так і державі. «Однією з небезпечних тенденцій, що склалася в сучасних умовах інформатизації суспільства, є випереджальний розвиток форм, способів, технологій і методик впливу на свідомість або підсвідомість, психічний стан людини порівняно з темпами формування й удосконалення методів та інструментів протидії відповідним деструктивним психологічним впливам».

### *10.5 Інституційне забезпечення інформаційної безпеки України*

Дослідження інституційного забезпечення інформаційної безпеки доцільно розпочати з деталізації та систематизації категоріального апарату, зокрема понять «інститут», «інституції», «інституційне забезпечення». Аналіз наукових підходів до визначення категорій «інститут» та «інституція» дає змогу зробити висновок про однорідність їх економічного змісту та відмінність ступеня системності. Інституцію правомірно розглядати як систему, тоді як інститут – базовий неділимий елемент інституції.

Призначення інституцій у суспільстві полягає в тому, щоб зменшити невизначеність через встановлення постійної структури людської взаємодії. Формою прояву інституцій є інститути. Сутнісними характеристиками цієї категорії можуть виступати як юридичні норми, так і порядок встановлення зв'язків між ними, «що надає можливість упорядкувати (регламентувати) стосунки між суб'єктами права з метою надання їм стійкого характеру, для чого і створюються відповідні організаційні структури та органи контролю».

Інституційне забезпечення слід визначити як процес формування інституцій (формальні та неформальні норми, які впливають на поведінку суб'єктів) та інститутів (юридичні норми), які консолідовано у формі організацій (підприємства, інфраструктура, державні органи), законів (нормативно-правові акти) та правил (економічні закони ринкової економіки) у процесі еволюції ринкового механізму.

*Інституційне забезпечення інформаційної безпеки* – це сукупність державних і недержавних інституцій, які забезпечують створення нормативно-правових, організаційних та економічних умов, необхідних для формування та реалізації ефективної державної політики у сфері інформаційної безпеки. У складі інституційного забезпечення інформаційної безпеки виділяють дві складові: інституційно-правове та інституційно-організаційне забезпечення.

Система нормативно-правових актів, що регулюють питання інформаційної безпеки включає: Конституцію України, Закон України «Про національну безпеку України», Закон України «Про Концепцію Національної програми інформатизації», Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», Стратегію інформаційної безпеки, Стратегію кібербезпеки України, Концепцію розвитку цифрової економіки та суспільства України на 2018-2020 роки, Концепцію розвитку цифрових компетентностей, Міжнародні стандарти серії ISO/IEC 27000, нормативні документи в галузі технічного захисту інформації (НД ТЗІ) та державні стандарти України стосовно створення і функціонування КСЗІ, інші нормативно-правові акти, що регулюють відносини у сфері інформаційної безпеки.

До 2021 року інституційно-правове забезпечення інформаційної безпеки зводилося до опосередкованого розгляду окремих її аспектів або стосувалося системи технічного захисту інформації. Так, Конституцією України ст. 17, поряд із захистом суверенітету державної цілісності України, передбачено «забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу». В Законі України «Про національну безпеку України» визначені напрями державної політики щодо забезпечення інформаційної безпеки, кібербезпеки, а в Концепції Національної програми інформатизації інформаційна безпека визнається невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки.

Ухвалена Урядом у вересні 2021 року Стратегія інформаційної безпеки є концептуальною основою забезпечення інформаційної безпеки. Стратегією визначені методологічні аспекти забезпечення інформаційної безпеки України, упередження появи та мінімізації загроз національній безпеці в інформаційній сфері, захисту прав громадян на інформацію та захист персональних даних. Цей документ окреслив вектори державної регуляторної політики у зазначеній сфері та стане базисом для формування ґрунтовного інституційно-правового забезпечення інформаційної безпеки.

Інституційно-організаційне забезпечення пропонується розглядати як систему організацій (органів влади), які забезпечують формування та реалізацію державної політики у сфері інформаційної безпеки. Органами державної влади, на які покладено функції формування та реалізації державної політики у сфері інформаційної безпеки слід визначити: Президента України, Верховну Раду України, Кабінет Міністрів України, Міністерство оборони України, Міністерство культури та інформаційної політики України, Міністерство цифрової трансформації, Державну службу спеціального зв'язку та захисту інформації, Державний комітет телебачення і радіомовлення України, Раду національної безпеки і оборони України, Департамент кіберполіції Національної поліції України, інші центральні органи виконавчої влади та органи сектору безпеки і оборони України, місцеві органи виконавчої влади та органи місцевого самоврядування.

Зокрема, у Положенні «Про Міністерство культури та інформаційної політики» визначено, що Міністерство забезпечує формування та реалізує державну політику у сферах культури, державної мовної політики, популяризації України у світі, державного іномовлення, інформаційного суверенітету України та інформаційної безпеки.

Міністерство цифрової трансформації, забезпечуючи формування та реалізацію державної політики у сфері цифровізації, цифрової економіки, цифрових інновацій, електронного урядування та електронної демократії, розвитку інформаційного суспільства, є невід'ємним елементом інституційно-організаційного забезпечення інформаційної безпеки.

Основними завданнями Державної служби спеціального зв'язку та захисту інформації як центрального органу виконавчої влади зі спеціальним статусом, згідно з чинним законодавством, є реалізація державної політики у сфері захисту державних інформаційних ресурсів у мережах передачі даних, забезпечення функціонування Державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, криптографічного та технічного захисту інформації.

Базуючись на системному підході, який передбачає розгляд та дослідження будь-яких систем з позиції мети їх функціонування, суб'єктів, які приймають участь у її забезпеченні, об'єктів, які функціонують у певній сфері діяльності, та на яких направлено інструменти впливу, архітектоніка інституційного забезпечення інформаційної безпеки представлена на (рис. 10.4).

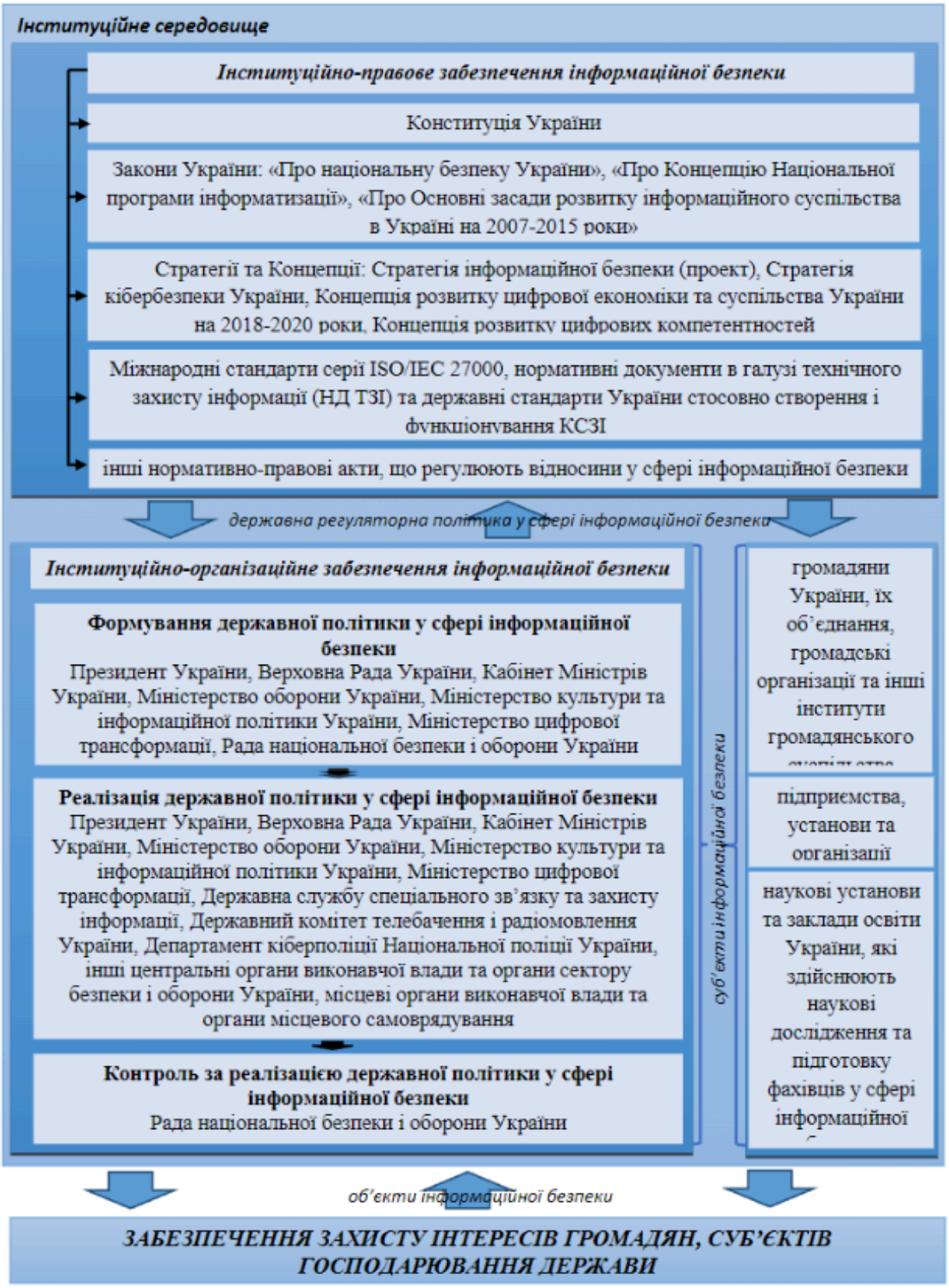



**Рис. Інституційне забезпечення інформаційної безпеки України**

Рада національної безпеки і оборони України як координаційний орган при Президентові України уповноважена приймати рішення щодо визначення концептуальних підходів та напрямів забезпечення національної безпеки в цілому та, в тому числі, в інформаційній сфері з урахуванням масштабу потенційних та реальних загроз національним інтересам України. Реалізацію державної політики в сфері протидії кіберзлочинності як невід'ємної складової державної політики у сфері інформаційної безпеки здійснює Департамент кіберполіції Національної поліції України.

Водночас, у чинному законодавстві не визначений спеціально уповноважений центральний орган виконавчої влади у сфері інформаційної безпеки України. Центральним органом виконавчої влади зі спеціальним статусом у сфері захисту інформації визначено Державну службу спеціального зв'язку та захисту інформації. Особливий статус має Рада національної безпеки і оборони України, оскільки є єдиним органом, який має повноваження координувати та контролювати діяльність органів виконавчої влади з реалізації політики інформаційної безпеки України та вносити Президенту України пропозиції щодо її уточнення та ресурсного забезпечення. Відсутність чіткої координації, розподілу функціональних обов'язків серед перелічених органів державної влади знижує рівень ефективності державної політики у сфері інформаційної безпеки.

Таким чином, інституційно-правове та інституційно-організаційне забезпечення інформаційної безпеки з урахуванням взаємозв'язків між суб'єктами (система державних і недержавних інституцій, а також громадян України) становлять інституційне середовище інформаційної безпеки, від ефективності функціонування якого буде залежати рівень забезпечення захисту інтересів громадян, суб'єктів господарювання та держави в цілому як соціальних об'єктів інформаційної безпеки.

На сьогоднішні проблема інституційно-організаційного забезпечення інформаційної безпеки в Україні полягає у відсутності спеціально уповноваженого органу, що суперечить сучасним тенденціям організації регуляторних процесів. Адже відсутність чіткої координації, розподілу функціональних обов'язків серед органів державної влади знижує рівень ефективності державної політики у сфері інформаційної безпеки.

Відмічаючи важливість та значення ухваленої Урядом Стратегії інформаційної безпеки, проблема недостатньої розробленості нормативно-правової бази у сфері інформаційної безпеки залишається актуальною та потребує розв'язання.

Таким чином, удосконалення інституційного забезпечення інформаційної безпеки вимагає комплексного підходу і передбачає впровадження якісних змін в інституційно-організаційному та інституційно-правовому забезпеченні.

### *10.6 Реальні та потенційні загрози інформаційній безпеці України*

На Україну чинять значний вплив інформаційні загрози (традиційні та нетрадиційні), а також проти неї ведеться інформаційно-гібридна війна. До традиційних загроз належать існуючі століттями військові загрози з використанням армій. Із розвитком людства й технологій ці загрози продовжують розвиватися й удосконалюватися, розрізняючись лише у формах та методах застосування зброї. Наразі вони набули глобального та більш загрозливого характеру через появою ядерної, хімічної та інших видів зброї масового знищення, наявних у розпорядження тих чи інших держав. До нетрадиційних загроз належать міжнародний тероризм, релігійний екстремізм, незаконний обіг наркотиків, торгівля людьми, контрабанда зброї, піратство, екологічні злочини та інші злочини транснаціонального характеру.

Сьогодні нетрадиційні загрози переважають над традиційними. Це пояснюється двома причинами, а саме: забороною на їх ведення та надмірними витратами на них. Властивістю багатовимірності повною мірою володіють гібридні конфлікти некласичного характеру з участю у бойових діях збройних формувань недержавних суб'єктів, серед яких міжнародний тероризм, для якого характерна розмита національна та ідеологічна приналежність. Протистояння армій є надзвичайно затратним і зумовлює непоправні втратами як людського, і матеріального характеру. Їм на зміну приходять війни нового типу – гібридного. Можна з упевненістю констатувати, що процеси глобалізації підвищили ефективність нетрадиційних загроз системі безпеці.

Технології інформаційно-гібридних війн, засновані на маніпулятивному управлінні

суспільно-політичною свідомістю і поведінкою громадян, є виключно небезпечними: їхнє головне завдання – розділити і поляризувати суспільство, сегментизувати його, змусивши фрагменти ненавидіти один одного, органи державної влади, для того, щоб потім зіштовхнути населення між собою, або, щоб вони ініціювали боротьбу зі знищення існуючої влади.

Метою технологій інформаційно-гібридних війн є об'єднати агресію людей в єдиний потік і направити його проти чинної державної влади. Глобальні соціальні платформи (Facebook, Twitter, YouTube тощо) є світовими монополістами у своїх форматах подання інформації чи дезінформації. Формати функціонування зазначених мереж не тільки передбачають контроль за інформацією, що проходить через них, володіючи можливістю і правом «банити» будь-які акаунти, але також вбудовування у трафік будь-яких інформаційних матеріалів без попередження про це користувачів.

Інформаційно-гібридна війна проти населення України, що триває, переслідує лише одну мету: погіршити місце нашої держави на міжнародній арені, зганьбивши українську націю і, зрештою, поширивши серед неї песимізм щодо свого майбутнього і недовіру до системи державного управління. Проти України також ведеться «когнітивна війна» (від слова cognitio – сприйняття, пізнання) як один із компонентів інформаційно-гібридних війн. «Когнітивна війна» передбачає вплив на свідомість людей та контроль над нею. Свідомість населення можна контролювати не тільки через засоби масової інформації, а також в Інтернет-просторі, шляхом поширення вигідної інформації/дезінформації.

На територію України поширює дію низка міжнародних неурядових організацій. Окремі з них мають на меті вплив на свідомість переважно молоді, формуючи в її частини відчуттів недовіри до чинної державної влади, що зумовлює зниження рівня інтелектуальної безпеки країни. Інформаційно-гібридна війна проти України ведеться з 90-х рр. минулого століття, тобто з моменту набуття республікою незалежності. Цю війну можна розділити на два етапи:

1) мирний період, що відзначається латентним впливом інформаційних загроз на систему безпеки нашої держави (часові межі цього етапу припадають на 1991 р. – 2011 р.);

2) воєнний період (2014 р. – по теперішній час), що характеризується активністю терористичних та інших груп, які використовують протиборчі сили для реалізації певних суспільно-політичних цілей.

Якщо провести хронологічний аналіз виявів інформаційно-гібридних загроз проти України (починаючи з 90-х років XX ст. і по теперішній час), то можна дійти висновку, що характер та методи терористичних дій та інформаційних вкидів зазнали поступальних змін (і в джерелі походження, і в масштабах). Їх основу, як і раніше, становлять фізичне усунення неугодних осіб та інфраструктурних об’єктів. Особливе занепокоєння викликає тенденції збільшення терористичних актів або спроб вчинення аналогічних діянь в останні роки, про що свідчать статистичні дані силового блоку. Беручи до уваги цю обставину, можна припустити, що тенденція зростання інформаційно-гібридних терористичних та екстремістських загроз зберігає присутність терористичних війн.

На сьогодні вони викликають стурбованість у багатьох країнах світу, включаючи й Україну, через проблему участі їхніх громадян у складі міжнародних терористичних угруповань у збройних конфліктах гарячих «місць» – Афганістану, Сирії, Іраку та інших. Ця тенденція зберігається й сьогодні, активно проявляючись у «терористичних війнах». Певну тривогу викликає питання щодо виявлення та відстеження коштів, спрямованих на фінансування тероризму, що загрожує інформаційній безпеці країни. Це пояснюється тим, що поки що не вдається повністю перекрити канали фінансування тероризму й екстремізму.

Ще однією складовою інформаційно-гібридних війн є кібервійни. Адже на сучасному етапі активна боротьба між світовими та регіональними спільнотами розгорнулася у

кіберпросторі. Сьогодні наявність високотехнологічного потенціалу в передових країнах дає їм можливість із використанням даного простору проводити підривні акції, що міцно утвердилися як «кібервійни». Такі війни, на жаль, набули значного поширення проти України. Як відомо, протягом останніх років російським хакерським атакам були піддані сайти вітчизняних урядових відомств (Міністерства освіти і науки України, Посольства України у Франції, Митної служби України та ін.).

Сьогодні створений ІГІЛ («кіберхаліфат») становить загрозу не тільки для України, а й усьому світу. У 2016 році це хакерське угруповання та ще десятки інших об'єдналися під загальною назвою «Об'єднаний кіберхаліфат» (United Cyber Caliphate, або UCC), до яких зараховують усіх кіберзлочинців, які діють від імені терористів ІГІЛ. Крім того, проти України ведуться «мігрантські війни». Починаючи з 80-х років минулого століття, наша держава відчувала наплив афганських біженців-мігрантів через ускладнення обстановки в північних прикордонних провінціях Афганістану, які продовжується й досі.

Сьогодні варто також говорити про імігрантські війни, що пов'язують зі збільшенням міграційних процесів за кордон України, у тому числі міграції її громадян до Республіки Польща, Німеччини та ін. Основою цього є проблема нелегальної міграції, з якою ведеться боротьба на міжнародному рівні. Тому будь-які негативні моменти (депортація громадян, урегулювання порядку перебування мігрантів та інші питання), що викликають невдоволення в іноземних країнах, подаються як «мігрантські війни».

Складності ситуації додає повномасштабна агресія проти України. Україною вже докладаються зусилля для позитивного вирішення питань нелегальної міграції, але війна триває. Відтак, державна міграційна політика є пріоритетним завданням для нашої країни, оскільки до значного відтоку трудових мігрантів-українців додалися вимушені переселенці з зон ведення активних бойових дій і окупованих територій. Крім того, зважаючи на все, процеси трудової міграції в найближчому майбутньому будуть значно посилені.

Це має під собою об'єктивне та суб'єктивне підґрунтя, оскільки досі не врегульовані прикордонні питання між Україною та Республікою Польща, що періодично зумовлюють необґрунтовані затримки під час перетину кордону. Таким чином, можна констатувати, що Україна схильна до інформаційно-гібридних загроз, які будуть з'являтися і в подальшому.

Організація розумного моніторингу Інтернет-активності та посилення контрпропаганди як способів протидії інформаційно-гібридним війнам є актуальним і своєчасним напрямком реалізації інформаційної політики України. На наше переконання, у цьому контексті слід забезпечити розвиток її інституційної системи публічного управління шляхом:

1. Створення власної інформаційної контргібридної пропагандистської структури, орієнтованої на конкретну аудиторію українського населення, яке не може протистояти інформаційним загрозам, у т.ч. з боку рф. Ця вітчизняна структура має розробляти технології протидії ворожій пропаганді на українське суспільство з використанням сучасних інформаційних технологій. На нашу думку, створення аналогічних контргібридних структур для України є перспективним і важливим вектором її інституційного розвитку в найближчому майбутньому. Аналогом такої інформаційної контргібридної пропагандистської структури для України визнається Бюро протидії гібридній війні, що функціонує в США.

2. Налагодження дієвої взаємодії України з іншими міжнародними та регіональними організаціями, а саме: Європейським центром з протидії гібридним загрозам, Парламентською Асамблею Ради Європи, Центром передового досвіду стратегічних комунікацій (StratCom) та ін.

Одночасно мають реалізовуватися заходи щодо належного забезпечення інформаційної безпеки України й іншими публічними інституціями – НУО, НКО. Вони мають залучатися до

реального формування та контролю за державною інформаційною політикою України. Зокрема, під час розробки Концепції інформаційної безпеки України. Крім того, уважаємо, що в цій концепції інформаційно-гібридна війна має бути визначена як одна із загроз інформаційній безпеці нашої країни.

У продовження також відзначимо, що розвиток вітчизняної інституційної системи публічного управління в умовах інформаційно-гібридних війнах має бути забезпечений шляхом створення Державного унітарного підприємства «Центр технічного захисту інформації, сертифікації та експертизи».

На наше переконання, такий центр має протидіяти іноземній технічній розвідці. Діяльність цієї організації рекомендуємо регламентувати в межах:

1) постанови Уряду України «Про положення про вимоги, умови та правила захисту інформації від іноземної технічної розвідки»;

2) державної програма забезпечення інформаційної безпеки України на період до 2030 року.

Підкреслимо, що реалізація таких правових документів повинна відзначатися використанням у повній мірі методу «інформаційно-правового домінування», що передбачає наявність позицій щодо максимально результативної взаємодії з міжнародними організаціями під час протистояння інформаційно-гібридним війнам, особливо кіберзагрозам з огляду на масштаби їхнього значного поширення.

Сьогодні основними учасниками кібервійн може бути визнано найбільш розвинені в технологічному відношенні країни: рф, Китай, Індію, Іран, Північну Корею та ін., які мають передову кіберзброю. Наприклад, найвідомішим фактом вважається американська хакерська атака на іранські ядерні об’єкти з використанням вірусу «Stuxnet», який вивів з ладу центрифуги зі збагачення урану.

Кібервійни відрізняються тим, що вони дають можливість досягти бажаного ефекту, установлюючи контроль над країною-об’єктом без кровопролиття, тобто із застосуванням новітньої технології. Кібероперації першої групи в основному спрямовані на добування закритої інформації військового, економічного та політичного характеру, тому до них віднесено кібершпигунство, економічне шпигунство, промислове шпигунство, політичне шпигунство та ін. З цією метою використовуються різні віруси-шпигуни, шкідливі програмні забезпечення, звукові атаки та ін.

На нашу думку, Україна може протидіяти кібервійнам у двох напрямках, а саме:

1. Удосконалення власної нормативно-правової бази, включаючи канал двостороннього та багатостороннього співробітництва із зарубіжними країнами.

2. Створення відповідних організаційних і технічних структур щодо захисту важливої інформації. З метою протидії кібервійнам із використанням Інтернету, соціальних мереж на вітчизняних теренах створено Кіберполіцію як департамент Національної поліції України.

Його завданням є боротьба з кіберзлочинами, тобто протидія хакерській діяльності, термінації міжнародних дзвінків стільникових компаній, вербування українців до терористичних груп у цифровому світі та ін. У контексті вдосконалення заходів щодо протидії «кібервійнам» Україна бере участь у міжнародних форумах, конференціях та інших науково-практичних заходах.

Крім того, у межах двостороннього та багатостороннього співробітництва України з іншими державами також здійснюється низка заходів. Практично у всіх підписаних чи підписуваних нормативно-правових документів передбачається співробітництво сторін у сфері боротьби з кіберзлочинами.

Багатосторонній формат співпраці з протидії кібервійнам передбачає спільну боротьбу в рамках міжнародних та регіональних організацій за прикладом ООН, ОБСЄ, СНД, ПАРЄ та

ін. В останні роки Україна стала поступово перетворюватися на одну з сприятливих політичних площин щодо обговорення та розгляду проблем боротьби із терористичними й інформаційно-гібридними війнами. Висловлюємо переконання, що створений Центр по боротьбі з тероризмом в Україні при МВС надасть додатковий позитивний імпульс для розробки заходів з протидії таким війнам.

Відтак, спеціальним службам та правоохоронним органам першорядне значення має бути приділено питанням забезпечення інформаційної безпеки українських громадян.

**ПИТАННЯ ДЛЯ САМОПЕРЕВІРКИ**

1. Охарактеризуйте державну політику забезпечення інформаційної безпеки України на сучасному етапі розвитку.
2. На Вашу думку, якою повинна бути система забезпечення інформаційної безпеки України?
3. Окресліть основні загрози національній безпеці України.
4. Вкажіть мету функціонування, завдання та основні функції системи забезпечення інформаційної безпеки України.
5. Яким чином реалізується політика інформаційної безпеки в законодавстві?
6. В чому полягають особливості адміністративно-правового забезпечення інформаційної гігієни в умовах сучасної України?
7. Охарактеризуйте інституційне забезпечення інформаційної безпеки України.
8. Якими, на Вашу думку, є реальні та потенційні загрози інформаційній безпеці України в умовах воєнного стану?
9. В чому полягають особливості розбудови системи інформаційної безпеки країни?

# ЛЕКЦІЯ 11
# ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ: ОСОБЛИВОСТІ, МОДЕЛІ, МЕХАНІЗМИ

**План викладу:**

11.1 Особливості забезпечення інформаційної безпеки України в різних сферах суспільного життя.
11.2 Політика інформаційної безпеки організації.
11.3 Інформаційна безпека України у сфері прав і свобод людини.
11.4 Моделі системного впливу на інформаційну безпеку Української держави.
11.5 Недержавна система інформаційної безпеки як інституційний механізм її забезпечення.

## *11.1 Особливості забезпечення інформаційної безпеки України в різних сферах суспільного життя*

Держава має розвивати свою політику у сфері забезпечення реалізації інформаційної безпеки України за наступними напрямками:

1) ідеологічний. М.О. Кириченко підкреслює, що ідеологія інформаційного суспільства як фактор динамічного розвитку і безпеки сучасної України в XXI столітті є сукупністю інформаційних, організаційних, матеріально-технічних, кадрових ресурсів, призначених для вирішення будь-яких задач інноваційного науково-технічного розвитку як окремої особистості, так і держави. Сучасний стан динамічного розвитку України та її національної безпеки, справедливо вказує науковець, є результатом взаємодії цілого ряду факторів, що впливають на формування та розвиток ідеології інформаційного суспільства. В її числі помітне місце належить освіті, науці, культурі, інтелігенції (національній еліті) України. Накопичення інноваційного та інтелектуального (наукового) потенціалу та міра його реалізації визначається якістю знань, ефективністю використання освітнього потенціалу у практичній діяльності та прагненням до формування ідеології інформаційного суспільства, яка б захищала на рівні держави потреби кожної особистості і формувалася як «ідеологія для всіх». Така позиція у багатьох аспектах віднайшла свій прояв у чинній нині Стратегії інформаційної безпеки, в якій значна увага приділяється просвітництву, громадянській та медійній культурі, національній ідентичності тощо. Отже, враховуючи вище викладене, можемо дійти висновку про те, що ідеологія сучасної державної політики з реалізації інформаційної безпеки в Україні має враховувати цілу низку умов і факторів та, звичайно ж, не зводиться виключно до протистояння конкретному ворогу (у даний час це російська федерація, яка активно веде інформаційну війну проти України). В основі цієї ідеології мають бути як національні та громадянські, так і абсолютні (або всезагальні) цінності та принципи. Україна має прагнути сформувати і розвивати стійку і адаптивну інформаційну систему із широкими можливостями, яка здатна ефективно протистояти і національним, і глобальним загрозам. Ключовою ідеєю протидії зазначеним загрозам мають стати не стільки заборони і різного роду обмеження з метою відгородитися, закритися від усього, що є чи здається ворожим, небезпечним, незрозумілим, скільки високоефективна контрпропаганда та просвітницька робота, спрямована на виховання медійно грамотних людей, з високим рівнем інформаційної та громадянської культури, правової та національної свідомості, здатних критично ставитися до отриманої інформації та ідентифікувати відповідні загрози. Тож по-справжньому ефективний механізм забезпечення інформаційної безпеки не може спиратися на ізоляціонізм;

2) нормативно-правовий. У чинні Стратегії інформаційної безпеки України визначено, що однією із проблем, що негативно позначаються на цій безпеці є недосконалість регулювання відносин у сфері інформаційної діяльності та захисту професійної діяльності журналістів. У Стратегії відмічається, що регулювання відносин у сфері інформаційної

діяльності не відповідає сучасним викликам та загрозам. Це перешкоджає розвитку українського медіаринку, ускладнює ведення бізнесу у цій сфері, зберігає залежність засобів масової інформації від їх власників, не забезпечує додержання професійних стандартів діяльності журналістів. Актуальною проблемою є непоодинокі випадки втручання в професійну організаційно-творчу діяльність засобів масової інформації та в індивідуальну професійну творчу діяльність журналістів, інші посягання на свободу інформаційної діяльності, зокрема перешкоджання їх професійній діяльності, погрози, насильство щодо них, посягання на їх життя та власність. Зазначене позбавляє журналістів можливості належним чином інформувати суспільство про суспільно важливі події та явища. З огляду на вище викладене, вважаємо, що розвиваючи свою політику щодо забезпечення інформаційної політики, держава повинна: своєчасно оновлювати нормативно-правове підґрунтя механізму забезпечення інформаційної безпеки в Україні, приводячи його у відповідність до перспектив подальшого розвитку та актуальних викликів і загроз; забезпечити гармонійне поєднання прав і свобод людини та громадянина в інформаційній сфері з національними інтересами у ній; створити нормативно-правові засади для ефективного просвітництва населення, підвищення їх медійної грамотності, правової культури та свідомості; забезпечити сприятливі нормативно-правові умови для розвитку економічної активності населення у інформаційній сфері; удосконалити матеріально-правові та процедурні засади контролю в інформаційній сфері, своєчасного виявлення та оцінювання ризиків; забезпечити сприятливе нормативно-праве середовище для взаємодії публічної влади всіх рівні із громадськістю з питань інформації та інформаційної діяльності;

3) організаційно-управлінський. Управлінська діяльність – це вид свідомо здійснюваної людської діяльності, спрямованої на ефективне функціонування здійснюваних робіт (індивідуально чи колективно) з досягнення тих чи інших цілей, вирішення відповідних завдань, виконання функцій. Сутнісний зміст управлінської діяльності полягає у ефективній організації функціонування підпорядкованої або керованої системи задля належного виконання її завдань та функцій. У розрізі досліджуваної проблематики організаційно управлінський напрямок розвитку досліджуваної політики повинен передбачати: вдосконалення системи суб’єктів забезпечення інформаційної безпеки; поліпшення якості кадрового забезпечення суб’єктів, які займаються забезпеченням інформаційної безпеки; покращення механізмів контролю за інформаційною діяльністю; вдосконалення механізмів координації діяльності суб’єктів із забезпечення інформаційної безпеки. Координація являє собою – метод управління, суттю якого є встановлення між суб’єктами та об’єктами державного управління горизонтальних зв’язків, тобто поєднання двох і більше однорівневих з точки зору визначеного критерію дій, що забезпечують досягнення запланованого результату. Координаційні відносини розрізняються за видами: узгодження, предметно-технологічна взаємодія, ієрархічна або складна взаємодія. А.В. Шегда відмічає, що координація забезпечує узгодженість у часі й просторі дій органів управління та посадових осіб, а також між системою в цілому і зовнішнім середовищем. Вона, тобто координація, відіграє в управлінні роль, яку образно можна порівняти з роллю диригента в оркестрі. Саме завдяки їй забезпечується динамізм системи, створюється гармонія взаємозв'язків підрозділів, здійснюється маневр матеріальними та трудовими ресурсами всередині системи залежно від специфіки завдань;

4) культурно-освітній. Даний напрям державної політики у досліджуваній сфері стосується проведення роботи щодо підвищення медійної грамотності населення і культури поводженні в інформаційному середовищі. Також важливим питанням, яке має вирішуватися за цим напрямком зазначеної політики, є утвердження національної ідентичності;

5) налагодження ефективної, системної та систематичної внутрішньодержавної

взаємодії та міжнародної співпраці з питань інформації та інформаційної безпеки;

6) інноваційний. Даний аспект державної політики передбачає стимулювання інновацій та забезпечення всебічного розвитку й захисту національної інформаційної інфраструктури, зокрема її телекомунікаційної складової, як сукупності різноманітних інформаційних (автоматизованих) систем, інформаційних ресурсів, телекомунікаційних (електронних комунікаційних) мереж, засобів комунікацій і управління інформаційними потоками, а також організаційно-технічних структур, механізмів, що забезпечують їх функціонування.

Наведений перелік звісно ж не є виключним і цілком може бути доповнений іншими напрямками розвитку зазначеної політики, втім переконані, що ті, які були нами запропоновані вище, мають доволі актуальний характер і цілком узгоджуються із цілями та завданнями чинної Стратегії інформаційної безпеки.

### *11.2 Політика інформаційної безпеки організації*

Забезпечення власної інформаційної безпеки в організаціях, як правило, є невід'ємною частиною загальної системи управління, необхідної для досягнення статутних цілей та завдань. Значимість систематичної цілеспрямованої діяльності щодо забезпечення інформаційної безпеки стає тим більш високою, чим вище ступінь автоматизації бізнес-процесів, і чим більше «інтелектуальна складова» в його кінцевому продукті, тобто чим більшою мірою успішність діяльності залежить від наявності та збереження певної інформації (технологій, ноу-хау, комерційних баз даних, маркетингової інформації, результатів наукових досліджень тощо), забезпечення її конфіденційності та доступності для власників і користувачів.

Значимість забезпечення інформаційної безпеки в деяких випадках може визначатися наявністю в загальній системі інформаційних потоків організації відомостей, що становлять не тільки комерційну, а й державну таємницю, а також інші види конфіденційної інформації (відомості, що становлять банківську таємницю, лікарську таємницю, інтелектуальну власність компаній-партнерів тощо). З одного боку, суб'єкти повинні протистояти впливу внутрішніх та зовнішніх інформаційних загроз, які дестабілізують систему, а з іншого, не допустити створення інформаційних загроз для елементів зовнішнього середовища.

Розбалансування і збої в інформаційній системі здатні завдати істотного економічного збитку. Однак створення ідеальної системи, безумовно здатної протистояти повному набору загроз вимагає істотних витрат, тому формування економічно виправданої системи оцінки ризиків інформаційної безпеки в умовах впливу дестабілізаційних факторів на рівні суб'єкта господарювання є вкрай важливим.

Політика інформаційної безпеки є комплексом документів, що відображають всі основні вимоги до забезпечення захисту інформації та напрямки роботи організації в цій сфері. При побудові політики безпеки можна умовно виділити три її основні рівні: верхній, середній і нижній.

Верхній рівень політики інформаційної безпеки організації служить: для формулювання і демонстрації ставлення керівництва до питань інформаційної безпеки та відображення загальних цілей організації в цій галузі;·є основою для розробки індивідуальних політик безпеки (на більш низьких рівнях), правил та інструкцій, що регулюють окремі питання та засобом інформування персоналу про основні завдання та пріоритети у сфері інформаційної безпеки.

Політики інформаційної безпеки середнього рівня визначають ставлення організації (керівництва) до певних аспектів його діяльності та функціонування інформ організації аційних систем: ставлення і вимоги (більш детально в порівнянні з політикою верхнього

рівня) до окремих інформаційних потоків та інформаційних систем, обслуговуючим різні сфери діяльності, ступінь їх важливості та конфіденційності, а також вимоги до надійності (наприклад, відносно фінансової інформації, а також інформаційних систем і персоналу, які відносяться до неї); відношення і вимоги до певних інформаційних та телекомунікаційних технологій, методів і підходів до обробки інформації і побудови інформаційних систем; відношення і вимоги до співробітників як до учасників процесів обробки інформації, від яких безпосередньо залежить ефективність багатьох процесів і захищеність інформаційних ресурсів, а також основні напрями і методи впливу на персонал з метою підвищення інформаційної безпеки.

Політики безпеки на найнижчому рівні відносяться до окремих елементів інформаційних систем і ділянок обробки та зберігання інформації і описують конкретні процедури і документи, пов'язані із забезпеченням інформаційної безпеки.

Розробка політики безпеки передбачає здійснення низки попередніх кроків:

оцінку особистих (суб'єктивних) відносин до ризиків організації її власників і менеджерів, відповідальних за функціонування і результативність роботи в цілому або окремі напрями його діяльності;

аналіз потенційно вразливих інформаційних об'єктів;

виявлення загроз для значущих інформаційних об'єктів (відомостей, інформаційних систем, процесів обробки інформації) і оцінку відповідних ризиків.

Здійснення попередніх кроків (аналізу) дозволяє визначити, наскільки інформаційна безпека в цілому важлива для стійкого здійснення основної діяльності організації, її інформаційної безпеки. На основі аналізу оцінок менеджерів і власників визначаються конкретні напрямки роботи щодо забезпечення інформаційної безпеки.

Таким чином, політика інформаційної безпеки (практично на всіх рівнях) в частині роботи з такими даними буде заснована на загальних строго формалізованих правилах, процедурах і вимогах (таких, як використання сертифікованого обладнання та програмного забезпечення, проходження процедур допуску, обладнання спеціальних приміщень для зберігання інформації тощо).

Загалом політика інформаційної безпеки повинна давати чітке уявлення про необхідну поведінку користувачів, адміністраторів та інших фахівців при впровадженні та використанні інформаційних систем і засобів захисту інформації, а також при здійсненні інформаційного обміну та виконанні операцій з обробки інформації. Крім того, з політики безпеки, якщо вона відноситься до певної технології та/або методології захисту інформації, повинні бути зрозумілі основні принципи роботи цієї технології. Важливою функцією політики безпеки є чітке розмежування відповідальностей в процедурах інформаційного обміну: всі зацікавлені особи повинні ясно усвідомлювати межу як своєї відповідальності, так і відповідальності інших учасників відповідних процедур і процесів.

Також одним із завдань політики безпеки є захист не тільки інформації та інформаційних систем, а й захист самих користувачів (співробітників організації, клієнтів і контрагентів).

Загальний життєвий цикл політики інформаційної безпеки включає в себе ряд основних кроків, які представлено на рис. 11.1. Цей цикл (рисунок) може повторюватися кілька разів з метою вдосконалення організаційних заходів у сфері захисту інформації та усунення виявлених недоробок.

Рисунок 11.1 – Цикли розвитку і вдосконалення політики інформаційної безпеки організації

Кібершпигунство та кібервійна стали інструментами державних та недержавних суб'єктів для отримання стратегічних переваг. У цьому контексті інформаційна безпека – це не лише захист даних, а й забезпечення експлуатаційної готовності критичної інфраструктури, підтримання економічної стабільності та захист демократичних процесів. Таким чином, прихильність держави до забезпечення високого рівня інформаційної безпеки має основне значення для її стійкості до зовнішніх загроз, збереження суспільної довіри та загального благополуччя громадян в епоху цифрових технологій.

### *11.3 Інформаційна безпека України у сфері прав і свобод людини*

Одним із найважливіших завдань держави на сучасному етапі є створенням належних умов для вільного вираження кожною особою своїх поглядів та переконань, усунення перешкод при реалізації цього права та притягнення винних осіб до відповідальності. Однак гарантуючи свободу слова українська держава зіткнулася із іншою проблемою – спотворення інформації та використання її у якості зброї в інформаційній війні. Тому на сьогодні не менш важливим завданням є забезпечення інформаційної безпеки України. В цьому контексті повинен бути віднайдений баланс між реалізацією права на свободу слова та інформаційною безпекою. Варто зазначити, що органи державної влади України поки що не належним чином забезпечують реалізацію державної інформаційної політики, спрямованої на утвердження свободи слова, плюралізму і демократичних засад інформаційної діяльності, інформаційного суверенітету та інформаційної безпеки України, зміцнення і розвиток її інформаційної інфраструктури. Поряд з цим чиновники користуються недосконалістю законів, на свій розсуд часто необґрунтовано засекречують інформацію, встановлюючи обмеження її поширення під грифами «для службового користування» чи «не для друку» та ховають непопулярні рішення,

інколи з ознаками корумпованості.

Правове поле частково регулював Закон України «Про доступ до публічної інформації», однак, як свідчить практика його застосування, наразі він потребує вдосконалення, зокрема положення, які стосуються внесення плати за надання інформації, процедури інформування запитувача інформації про розмір плати за надання інформації (оскільки поряд з фактичними витратами на копіювання і друк існують ще й фактичні витрати на пересилання відповіді, що складає значну частку вартості такої послуги, а їх відшкодування цим законом не передбачено). Крім того, Закон України «Про доступ до публічної інформації» не враховує, що іншими законами встановлено спеціальні процедури доступу до інформації, яка зберігається в архівах, державних реєстрах, базах персональних даних тощо.

Правом на свободу думки і слова, на вільне вираження своїх поглядів і переконань може користуватися кожен, не зважаючи на те, чи є він громадянином України чи ні, адже це право закріплене в Конституції України і наша держава зобов'язалася його гарантувати так само, як й інші основоположні права людини. Українське суспільство усвідомило необхідність утвердження загальновизнаних норм свободи слова, прийнятих міжнародною спільнотою, що підтверджується не лише ратифікацією міжнародних документів та приведенням у відповідність до них національного законодавства, а включенням цього права до програмних документів більшості політичних партій та громадських об'єднань. Під свободою слова слід розуміти правовий інститут міжнародного права та національних правових систем, який складається з правових норм, що мають на меті забезпечити право особи вільно думати про різні суб'єкти, об'єкти, явища, відносини та відомості, на підставі її уявлень і переконань, освіти, психологічного стану й середовища, в якому вона живе, а також можливість вільно виражати свої думки у словесній чи знаковій формах, вільно збирати, зберігати, використовувати, поширювати та отримувати інформацію у будь-якій формі, будь-якого змісту та обсягу, в межах, визначених чинним законодавством.

Наголошується, що обмеження на свободу слова мають відповідати трьом міжнародно-правовим вимогам: легітимності, необхідності та доцільності, які повинні бути чітко виписані в національному законі, зрозумілими та гарантувати правовий захист від довільного втручання з боку влади, мають бути необхідними в демократичному суспільстві, під яким Європейський суд з прав людини розуміє панування плюралізму та верховенства права, а також повинні відповідати встановленим міжнародним правом цілям. Загалом як можна побачити, реалізація права громадян на доступ до публічної інформації в Україні забезпечується недостатньо та зумовлена недоліками правового регулювання, зокрема сфери соціального управління, дій органів державної влади та самоврядування. Тому з метою ефективного забезпечення прав громадян на доступ до публічної інформації необхідно передбачити на законодавчому рівні пошук інформації як самостійного різновиду інформаційної діяльності. Водночас потребує подальшого розвитку і вдосконалення інформаційне законодавство як окрема галузь, що об'єднує у собі самостійні правові інститути. Тому й надалі актуальною залишається розробка та впровадження нових законодавчих актів, спрямованих на врегулювання статусу суб'єктів правовідносин у мережі Інтернет. Тобто варто систематизувати існуючі, визначаючи у них правові зв'язки, з метою подальшого їх кодифікування на рівні Інформаційного кодексу України. Цей кодифікований нормативний документ має об'єднати в одному законодавчому акті регулювання провідних суспільних відносин, об'єктом яких є інформація, незалежно від форми, способу, засобу чи технологій її прояву в суспільних відносинах.

Серед провідних завдань кодифікування інформаційного законодавства визначення консенсусу у суспільних відносинах, узгодженості розуміння та застосування юридичних

норм, правомірної поведінки учасників відносин в інформаційній сфері; забезпечення інформаційного суверенітету, незалежності України у міжнародних відносинах; забезпечення інформаційної безпеки громадян, їх окремих спільнот, суспільства та держави як складових національної безпеки України; визначення правомірної поведінки учасників інформаційних відносин в Україні; захист інформації від несанкціонованого доступу, правопорушень (знищення, модифікації, перекручування тощо).

Інформаційний кодекс має розроблятися з урахуванням європейських стандартів та розвитку інформаційних відносин в Україні. Тому розробка та введення його в дію сприятиме побудові розвинутого інформаційного суспільства нашої держави як органічного сегменту глобального інформаційного співтовариства, забезпеченню реалізації права на свободу слова та вільний доступ до публічної інформації, розвитку національних інформаційних ресурсів та інфраструктури, впровадженню новітніх інформаційних технологій. Тому з метою ефективного забезпечення прав громадян на доступ до публічної інформації необхідно передбачити на законодавчому рівні пошук інформації як самостійного різновиду інформаційної діяльності. Водночас потребує подальшого розвитку і вдосконалення інформаційне законодавство як окрема галузь, що об’єднує у собі самостійні правові інститути. Тому й надалі актуальною залишається розробка та впровадження нових законодавчих актів, спрямованих на врегулювання статусу суб’єктів правовідносин у мережі Інтернет, а для цього необхідно ввести в дію Інформаційний кодекс України. В цьому кодексі необхідно визначити та уніфікувати загальні положення інформаційного законодавства, а також засади та норми регулювання інформаційних відносин у різних галузях суспільної діяльності. Це сприятиме побудові в Україні розвинутого інформаційного суспільства як органічного сегменту глобального інформаційного співтовариства, забезпеченню реалізації конституційних прав на свободу слова та вільний доступ до інформації, що становить суспільний інтерес, а також до публічної інформації, розвитку національних інформаційних ресурсів та інфраструктури, впровадженню новітніх інформаційних технологій тощо. Вирішення цих питань дасть змогу забезпечити реальне здійснення передбаченого Конституцією України права людини на свободу слова.

### *11.4 Моделі системного впливу на інформаційну безпеку Української держави*

Інформаційна безпека має основне значення в сучасному взаємопов'язаному світі і є основою для захисту цілісності, конфіденційності та доступності даних на різних платформах та системах. Відтак, її суть полягає у захисті інформації від несанкціонованого доступу, розкриття, зміни та знищення, забезпечуючи тим самим безпеку, надійність та доступність даних для авторизованих користувачів.

Інформаційна безпека використовує низку методів, включаючи криптографічні методи, механізми контролю доступу та надійні протоколи безпеки для захисту цифрової та фізичної інформації. Значення інформаційної безпеки виходить за рамки захисту індивідуальних та корпоративних даних: вона відіграє вирішальну роль у забезпеченні конфіденційності комунікацій, забезпеченні безпеки фінансових транзакцій та захисті конфіденційної інформації.

Для забезпечення інформаційної безпеки необхідно виконати декілька ключових завдань. До них належать проведення регулярних оцінок ризиків для виявлення вразливостей, впровадження комплексних політик та процедур безпеки, а також забезпечення постійного моніторингу та реагування на потенційні інциденти безпеки.

Програми навчання та підвищення обізнаності мають вирішальне значення для інформування співробітників про їх роль у забезпеченні безпеки та потенційних загроз, з якими вони можуть зіткнутися. Крім того, необхідно розробити плани аварійного

відновлення та забезпечення безперервності бізнесу, щоб гарантувати швидке відновлення операцій після порушення безпеки чи інших збоїв.

Шифрування, безпечний контроль доступу та регулярні оновлення програмного забезпечення та систем також є фундаментальними компонентами надійної стратегії інформаційної безпеки (табл.11.1).

Таблиця 11.1 Ключові засади сучасної системи забезпечення інформаційної безпеки

| № п/п | Засади | Характеристика |
|---|---|---|
| 1. | Багаторівневий захист | Передбачає створення декількох рівнів захисту з метою забезпечення комплексного і глибинного захисту інформаційних систем. Він включає в себе не лише технічні засоби захисту, такі як фаєрволи і антивірусне програмне забезпечення, а й організаційній заходи, такі як політики доступу та процедури реагування на інциденти. |
| 2 | Впорядкованість | Полягає в наданні користувачам та системам лише тих прав і привілеїв, які необхідні для виконання їхніх завдань. Він допомагає мінімізувати потенційний ризик зловмисних дій або помилок, обмежуючи доступ до критично важливих ресурсів і даних. |
| 3 | Неперервний моніторинг та аналіз ризиків | Включає в себе регулярні оцінки вразливостей, аудити безпеки та наліз ризиків для адаптації захисних стратегій з урахуванням змінюваних умов та загроз. |
| 4 | Шифрування даних | Шифрування є критично важливим для захисту конфіденційності та цілісності даних під час їх зберігання та передачі. Воно гарантує, що навіть у разі несанкціонованого доступу, інформація залишиться незрозумілою та недоступною для зловмисників. |
| 5 | Освіта та тренінги з безпеки | Людський фактор часто є слабкою ланкою в системі інформаційної безпеки. Регулярні тренінги та освітні програми для співробітників сприяють підвищенню обізнаності щодо потенційних загроз і кращому розумінню політик безпеки, тим самим знижуючи ризик випадкових або навмисних порушень безпеки. |

Повномасштабна війна, розв'язана російською федерацією, глибоко вплинула на ситуацію з інформаційною безпекою України, виявивши вразливості та прискоривши суттєві зміни у стані кібербезпеки країни. Війна ведеться як на місцях, а й у цифрової сфері, де кібератаки стали найважливішим компонентом стратегії ведення війни. Україна зіткнулася зі шквалом кібератак, спрямованих на дестабілізацію уряду, посіяти хаос серед населення та завдати шкоди критично важливій інфраструктурі.

Ці атаки були націлені на широкий спектр секторів, включаючи урядові бази даних, фінансові установи, енергетичні мережі та системи зв'язку, намагаючись підірвати стабільність та стійкість країни. У відповідь на ці виклики Україна змушена була значно посилити заходи інформаційної безпеки. Уряд у співпраці з приватним сектором та міжнародними союзниками зміцнив свою інфраструктуру кібербезпеки для захисту від кібератак та пом'якшення їх наслідків. Це включало модернізацію існуючих протоколів кібербезпеки, підвищення безпеки критично важливої інфраструктури та впровадження складніших систем спостереження та виявлення. Крім того, Україна зосередила зусилля на створенні міцної нормативно-правової бази для більш ефективної протидії кіберзагрозам, включаючи створення спеціальних підрозділів із кіберзахисту у складі своїх сил безпеки та

оборони.

Війна також наголосила на важливості інформації для впливу на громадську думку та психологічні аспекти війни. Україні довелося боротися не лише із захистом своєї цифрової інфраструктури, а й із боротьбою з поширенням хибної інформації, спрямованої на ослаблення морального духу та підрив підтримки. У цьому контексті інформаційна безпека виходить за рамки технічних заходів і включає зусилля щодо підтримки цілісності інформації та протидії дезінформації за допомогою ініціатив щодо перевірки фактів та кампаній щодо підвищення обізнаності громадськості.

Цифровізація та широке використання соціальних мереж відіграли ключову роль у цьому аспекті конфлікту. Ці платформи стали полем битви, де інформація стає зброєю, що вимагає пильності та превентивних заходів для захисту від маніпуляцій та кібершпигунства. Ситуація підштовхнула Україну до інновацій у своєму підході до інформаційної безпеки, використання передових технологій та міжнародного співробітництва для посилення свого кіберзахисту (табл. 11.2).

| № п/п | Вплив | Сутність впливу |
|---|---|---|
| 1. | Посилення заходів кіберзахисту | В умовах воєнного стану зростає ризик кібератак з боку ворожих держав або їхніх агентів. Тому державні та приватні організації змушені значно посилити заходи кіберзахисту, включаючи моніторинг, виявлення та нейтралізацію загроз, а також вдосконалення систем шифрування та аутентифікації. |
| 2 | Обмеження доступу до інформації | З метою запобігання розповсюдженню інформації, яка може бути використана противником, можуть бути введені обмеження на доступ до певних даних та комунікаційних каналів. Це включає контроль над Інтернет-трафіком, цензурування ЗМІ та обмеження використання соціальних мереж. |
| 3 | Активізація інформаційної війни | Воєнний стан сприяє інтенсифікації інформаційних операцій, які включають пропаганду, дезінформацію та психологічні операції. Забезпечення інформаційної безпеки в цьому контексті означає не лише захист від ворожих інформаційних впливів, але й активне використання інформаційного простору для досягнення стратегічних цілей. |
| 4 | Зміни в законодавстві | Воєнний стан часто вимагає адаптації або введення нового законодавства, спрямованого на посилення інформаційної безпеки. Це може включати закони, які регулюють збір і обробку інформації, а також спеціальні повноваження для сил безпеки та розвідувальних служб. |
| 5 | Мобілізація ресурсів для кібероборони | В умовах воєнного стану ресурси держави, у тому числі фінансові, технічні, людські, можуть бути мобілізовані для зміцнення національної кібероборони. Це передбачає підготовку кадрів, розробку та впровадження передових технологій захисту інформації, а також створення спеціалізованих центрів кібербезпеки. |

Насамкінець, інформаційна безпека необхідна для захисту конфіденційності, цілісності та доступності даних в епоху цифрових технологій, що характеризується витонченими кіберзагрозами. Його роль у національній безпеці має вирішальне значення, оскільки він підтримує захист критичної інфраструктури країни, оборонного потенціалу та суспільної довіри.

Забезпечення інформаційної безпеки передбачає комплексний підхід, що включає

управління ризиками, реалізацію політик, безперервний моніторинг і адаптацію до цифрового ландшафту, що розвивається. Оскільки цифровізація продовжує розвиватися, важливість надійних заходів інформаційної безпеки та міжнародного співробітництва у зусиллях кібербезпеки стає все більш першорядною для захисту інтересів національної та глобальної безпеки.

Діджиталізація сучасного суспільства, масовий перехід в online, спровокований пандемією COVID-19, постійний розвиток інформаційних технологій, удосконалення комп'ютерних систем зберігання й обробки інформації ставлять економічні суб'єкти перед необхідністю вирішення комплексного завдання. З одного боку, суб'єкти повинні протистояти впливу внутрішніх та зовнішніх інформаційних загроз, які дестабілізують систему, а з іншого, не допустити створення інформаційних загроз для елементів зовнішнього середовища. В умовах збільшення кількості випадків хакерських атак, поширення комп'ютерних вірусів та комп'ютерного піратства слід кардинально підвищити рівень захисту інформації. Розбалансування і збої в інформаційній системі здатні завдати істотного економічного збитку. Однак створення ідеальної системи, безумовно здатної протистояти повному набору загроз вимагає істотних витрат, тому формування економічно виправданої системи оцінки ризиків інформаційної безпеки в умовах впливу дестабілізаційних факторів на рівні суб'єкта господарювання є вкрай важливим.

Концептуальна модель інформаційної безпеки, за умови невизначеності впливу дестабілізаційних факторів на основі нейронечітких мереж, потребує визначення ризику. Ризик інформаційної безпеки – це комплексне поняття, яке складається із значної кількості впливаючих дестабілізаційних факторів, основними з яких на етапі аналізу організації обрано:

– загрози інформаційної безпеки (програмні або людські злодіяння, які можуть призвести до руйнування чи втрати працездатності системи інформаційної безпеки);

– потенційно можливі збитки (фінансові втрати організації на полагодження системи інформаційної безпеки вразі її руйнування чи втрати працездатності);

– вразливість інформаційної системи (вразливі (непокриті концептуальною моделлю) місця інформаційної системи).

Методи, що вирішують завдання оцінки факторів системи, що дестабілізаційно впливають на систему інформаційної безпеки, можна розділити на кількісні та якісні (з числовою та лінгвістичною шкалою виміру цих факторів відповідно). Для кожного виду цих методів існують свої переваги та недоліки. Звести недоліки до мінімуму спільне використання числових коефіцієнтів разом з лінгвістичними. Тому саме такі змішані методи слід використовувати для оцінки ризику інформаційної системи на основі наявних дестабілізаційних факторів та експертної оцінки.

Задача моделювання системи інформаційної безпеки в умовах невизначеності впливу дестабілізаційних факторів на основі нейронечітких мереж полягає у кількісному визначенні значення ризику організації за допомогою нечіткої логіки за наявних факторів ризику, значення яких на вході подані у лінгвістичній терм-множині. Для моделювання ризику інформаційної безпеки підприємства, нечіткі моделі доцільно представляти у: Блок 1 (ресурси); Блок 2 (інформація); Блок 3 (витрати); Блок 4 (система заходів підвищення ІБ); Блок 5 (досягнення цілей підвищення ІБ). Крім того, повинні бути ще рівні: організаційно-управлінський рівень забезпечення інформаційної безпеки; сервісний рівень забезпечення інформаційної безпеки.

Розглядаючи особливості інформаційної функції системи управління економічною безпекою організації, слід зазначити, що для організації відповідного рівня інформаційної безпеки має бути обрана відповідна модель економічної безпеки, згідно з якою мають бути

враховані методи заподіяння шкоди елементам системи та системи в цілому, вибір яких ґрунтується на аналізі та оцінці наявних ризиків відмови інформаційної системи організації.

### *11.5 Недержавна система інформаційної безпеки як інституційний механізм її забезпечення*

У науці та практиці існує широкий спектр поглядів на необхідність пошуку оптимальних напрямків та механізмів здійснення перетворень в інформаційній сфері нашої держави. Питання активного залучення громадськості, є надзвичайно актуальним й зумовлює необхідність обговорення й відпрацювання комплексних заходів щодо удосконалення взаємодії органів державної влади з ІГС для подолання негативних явищ та процесів в інформаційній сфері.

Змістовна сутність громадського суспільства полягає передусім у забезпеченні прав і свобод людини та громадянина. Особистість у громадянському суспільстві має гарантоване законами право вибору різноманітних форм політичної, економічної, соціальної та іншої діяльності, право вибору певної ідеології, світогляду, віросповідання тощо.

Громадянське суспільство має створювати багаторівневу та багатофункціональну соціальну інфраструктуру, в якій знайшли б своє втілення життєво важливі інтереси всіх верств населення у сферах забезпечення національної безпеки, у тому числі й у інформаційній сфері.

Проблеми забезпечення реалізації конституційних прав і свобод людини та громадянина у сфері доступу до інформації, створення належних умов для розвитку сучасної та прозорої системи громадянського контролю за діяльністю органів державної влади та місцевого самоврядування, а також вирішення низки інших завдань можуть бути успішно вирішені за допомогою інститутів громадянського суспільства (ІГС).

Роль ІГС в сфері забезпечення інформаційної безпеки визначається їхньою здатністю виконувати наступні функції:

– раннього попередження назріваючих загроз інформаційній безпеці, виникнення суперечностей, конфліктів, кризових ситуацій та виявлення їх джерел;

– залучення широких верств населення до практичної діяльності, стабілізації ситуації в інформаційній сфері, досягнення загальногромадянського миру та злагоди;

– формування громадської думки та впливу на неї, розвитку громадянської самосвідомості;

– захисту прав, свобод та інтересів громадянського суспільства в інформаційній сфері;

– демократичного громадського контролю за діяльністю органів влади і управління, за виконанням їх рішень в інформаційній сфері.

При цьому варто зазначити, що в багатьох країнах світу довіра до ІГС у кілька разів більша, ніж до урядів цих держав.

ІГС можуть виконувати наступні завдання забезпечення інформаційної безпеки:

1. Надавати допомогу державі, виконувати окремі функції державних органів.

2. Доповнювати національну систему забезпечення інформаційної безпеки, виконувати ті функції захисту життєво важливих інтересів особистості й суспільства в цій сфері, які держава не виконує або не може виконувати через обмеженість ресурсів або з інших причин.

3. Створювати сприятливі умови для діяльності органів влади та управління для забезпечення інформаційної безпеки.

4. Здійснювати демократичний громадський контроль за діяльністю держави у виконанні функцій та забезпечувати оцінку ефективності діяльності держави із забезпечення інформаційної безпеки та її складових.

6. Спонукати державу до вживання заходів захисту інтересів особистості й суспільства, виправлення існуючих недоліків та прорахунків у цій сфері.

7. Здійснювати підготовку кваліфікованих кадрів, здатних посідати державні посади у сфері ЗІБ.

8. Виконувати наукові дослідження з актуальних проблем ІБ.

9. Здійснювати інформаційно-аналітичну роботу на постійній або на періодичній основі.

Таким чином, призначення ІГС як суб'єктів забезпечення інформаційної безпеки полягає в тому, щоб змусити державу ефективно відстоювати саме національні інтереси в інформаційній сфері, допомогти державі реалізувати в ній життєво важливі інтереси особистості й суспільства, сприяти стабільності в державі та суспільстві, гармонізації інтересів різноманітних соціальних груп та знаходженню балансу інтересів, перешкоджати можливій підміні національних інтересів корпоративними.

Механізм взаємодії державних органів з ІГС повинен визначатись, насамперед, мірою їхньої участі у вирішенні актуальних проблем забезпечення інформаційної безпеки ЗІБ. Це, у свою чергу, передбачає, що метод державного регулювання діяльності ІГС має базуватися не на забороні, а на створенні умов для активного використання їх з метою забезпечення інформаційної безпеки держави, суспільства, особистості.

Як свідчить досвід багатьох країн з високим рівнем довіри до інститутів громадянського суспільства, для підвищення ступня ефективності взаємодії ІГС з органами державної влади України з вирішення будь-яких проблем, державі необхідно забезпечити надання процесам прийняття державних рішень більшої прозорості, підзвітності, створення умов для вільного розвитку ЗМІ. У цьому контексті важливим є посилення зв'язків між неурядовими організаціями, акумулювання сил для посилення впливу на місцеву владу, запобігання антидемократичним проявам тощо.

Широкий доступ усіх верств населення до засобів поширення інформації здатен також якісно змінити відносини у самому суспільстві. Оскільки така "масова" інформація надходить постійно, стосується усіх значимих подій, апелює до цінностей або пропонує нові, враховує психологічні особливості людини, зрештою, пропонує певні моделі поведінки, – вона є вагомим фактором формування цінностей, світоглядних орієнтацій, уявлень про належну поведінку і спосіб мислення взагалі.

**ПИТАННЯ ДЛЯ САМОПЕРЕВІРКИ**

1. Якими є особливості забезпечення інформаційної безпеки України в різних сферах суспільного життя? Охарактеризуйте одну з них на вибір.
2. Вкажіть основні правила та заходи управління інформаційною безпекою організації.
3. На яких засадах ґрунтується політика інформаційної безпеки організації?
4. Окресліть принципові положення інформаційної безпеки України у сфері прав і свобод людини.
5. Які моделі системного впливу на інформаційну безпеку Української держави Ви знаєте? В чому полягають їх переваги та недоліки?
6. Охарактеризуйте недержавну систему інформаційної безпеки. Яка її головна роль?
7. Визначте інституційний механізм забезпечення недержавної системи інформаційної безпеки.
8. Обґрунтуйте форми і методи громадської активності як механізм протидії російським інформаційним впливам.

# ЛЕКЦІЯ 12
# МЕХАНІЗМИ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ВІЙНАМ ТА ЗАХИСТУ ІНФОРМАЦІЙНОМУ ПРОСТОРУ УКРАЇНИ

**План викладу:**

12.1 Інформаційна система як об'єкт інформаційного впливу: змістова і представницька складові, ціннісні аспекти.

12.2 Кібератаки на державні інформаційні системи та об'єкти критичної інформаційної інфраструктури України.

12.3 Реальні та потенційні загрози інформаційному простору України: спеціальні інформаційні операції (СІО) та акти зовнішньої інформаційної агресії (АЗА).

12.4 Забезпечення інформаційної безпеки України в умовах російської агресії.

12.5 Створення безпечних умов існування інформаційних технологій: питання захисту інформації, інформаційної інфраструктури держави, інформаційного ринку та розвитку інформаційних процесів.

## *12.1 Інформаційна система як об'єкт інформаційного впливу: змістова і представницька складові, ціннісні аспекти*

Інформаційна система - організований набір елементів, що збирає, обробляє, передає, зберігає та надає дані. Інформаційна система (ІС) складається із людей, обладнання, процесів, процедур, даних та операцій.

Кожна інформаційна система включає в себе наступні компоненти: структура системи; функції кожного елемента системи; вхід і вихід кожного елементу і системи в цілому; мета і обмеження системи та її окремих елементів.

Інформаційна система не тільки відображає функціонування об'єкта управління, а й впливає на нього через органи управління. Вона є сукупністю інформаційних процесів для задоволення потреби в інформації різних рівнів прийняття рішень.

Її метою є продукування інформації для використання (споживання) управлінським апаратом. Відповідно вона забезпечує нагромадження, передачу, збереження, оброблення та узагальнення інформації "знизу вгору", а також конкретизацію інформації "зверху донизу". Призначення ІС полягає в описі економічного об'єкта, його станів, взаємодії, що виражається через економічні показники. Вона покликана своєчасно подавати органам управління необхідну і достатню інформацію для прийняття рішень, якість яких забезпечує високоефективну діяльність об'єкта управління та його підрозділів.

До головних завдань належать: виявлення джерел інформації; збирання, реєстрація, обробка та видача інформації, що характеризує стан виробництва та управління; розподіл інформації між керівниками, підрозділами та виконавцями відповідно до їх участі в управлінні. Ключовими елементами кожної організації є персонал, структура, робочі процедури, політика і культура. Інформаційна система — це також важливий інструмент для здійснення управлінських функцій.

У системах обробки інформації головними її компонентами є дані та обчислення. Більшість інформаційних систем управління інформаційними ресурсами в організаціях містять і багато інших компонентів, таких як вимоги, запити, трігери і звіти. І всі вони, зокрема, містять великі описи свого власного змісту в тій чи іншій формі. Схему розвитку інформаційних систем, що ілюструє особливості розв'язування функціональних задач залежно від характеру інформаційного і математичного забезпечення, наведено на рис. 12.1

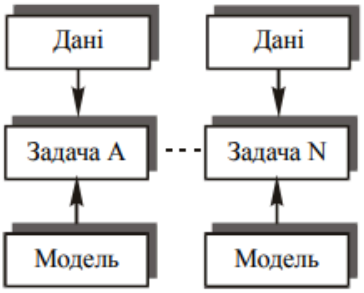
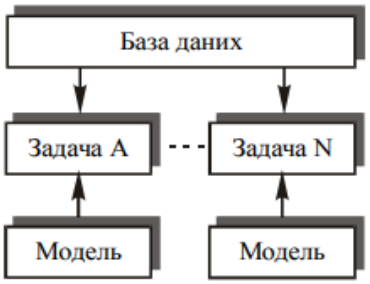
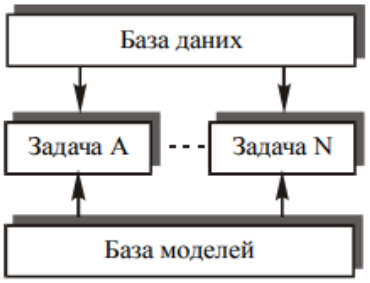
| Покоління ІС | Назва ІС | | Схема розв'язування задач | Примітка |
|---|---|---|---|---|
| | США | Україна | | |
| Перше покоління | Система обробки даних | АСУ-позадачний підхід |   | Надмірність: інформаційна, математична |
| Друге покоління | Управлінські інформаційні системи | АСУ-концепція баз даних |   | Надмірність: математична, розподіл даних |
| Третє покоління | Системи підтримки прийняття рішень СППР | |   | Розподіл: даних, обчислень |

Рис. Схема розвитку інформаційних систем

В інформаційних системах першого покоління, які в зарубіжній літературі відомі під назвою Data Processing System — DPS («Системи обробки даних», синоніми — «Електронна обробка даних», «Системи електронної обробки даних»), а у вітчизняній — «Автоматизовані системи управління (АСУ) — позадачний підхід» — для кожної задачі окремо готувалися дані і створювалася математична модель. Такий підхід зумовлював інформаційну надмірність (одні й ті самі дані могли використовуватись для розв'язування різних задач) і математичну надмірність (моделі розв'язування різних задач мали загальні блоки). Типовими прикладами систем обробки даних є системи керування запасами, виписування рахунків, нарахування зарплати.

Створення ІС першого покоління в нашій країні відносять до початку 60-х років XX століття, коли на великих підприємствах почали використовувати ЕОМ для розв'язування задач організаційно-економічного управління. Перші такі системи обмежувалися розв'язуванням деяких функціональних управлінських задач, наприклад задач бухгалтерського обліку. Тому системність автоматизованої обробки економічної інформації в зазначений період характеризувалася частковістю та локальністю.

Протягом наступних років поступово переходять від локальних систем обробки даних, призначених для тих чи інших ділянок управлінських робіт, до систем, що охоплюють широке коло задач управління. Подальший розвиток інформаційних систем пов'язаний з концепцією

баз даних. На цій основі з'явились інформаційні системи другого покоління. Інформаційні системи другого покоління відомі під назвою Management Information System — MIS («управлінські (адміністративні) інформаційні системи» або «інформаційні системи в менеджменті»), у нашій літературі використовується термін «АСУ — концепція баз даних».

Основною функцією таких систем є забезпечення керівництва інформацією. Типову управлінську інформаційну систему характеризує структурований потік інформації, інтеграція задач обробки даних, генерування запитів і звітів. В управлінських інформаційних системах (УІС) вже були визнані переваги колективного користування даними, а також відзначено, що в одній організації багато прикладних програм використовують одні й ті самі робочі дані і відбувається дублювання робіт у процесі збирання, зберігання і пошуку цих даних.

Зі збільшенням кількості прикладних програм, що обслуговують всі рівні управління та обробляють одні й ті самі робочі дані, зростав обсяг дублювання, що ставало гальмом на шляху комп'ютеризації управління. Більш того, це дублювання часто було неефективним, оскільки призводило до несумісності прикладних програм.

Виходом із цієї ситуації стала концепція створення єдиної централізовано керованої бази даних, яка за допомогою спеціального програмного продукту — СУБД обслуговує всі прикладні програми організацій. Основною проблемою створення великих розподілених баз даних є складність опису даних, що має на меті об'єктивного, незалежного від окремих прикладних програм, спростити колективне використання даних різними прикладними програмами. Для опису даних широко застосовуються моделі та словники даних.

Семантика даних, тобто вивчення їх змісту незалежно від окремих прикладних програм, стала самостійною галуззю досліджень. Подальшим розвитком інформаційних систем в економіці в колишньому СРСР саме й було створення АСУ (ІС) на основі ідеології автоматизованих банків даних і баз даних.

Цей етап створення ІС другого покоління розпочався 1972 року, коли вперше до державного плану було внесено питання розвитку економіки і створення АСУ. Економічна ефективність АСУ була значна. Крім прямого економічного ефекту впровадження АСУ мало великий вплив на зміну характеру діяльності управлінського персоналу. Підвищилась оперативність, наукова обґрунтованість та об'єктивність прийнятих управлінських рішень; стало можливим розв'язувати принципово нові економічні задачі, які до впровадження ІС не розв'язувалися апаратом управління; збільшився час на творчу роботу працівників за рахунок скорочення обсягів виконання рутинних операцій вручну; у результаті автоматизації процесів інформаційного обслуговування підвищилася інформованість управлінського персоналу. Системи підтримки прийняття рішень — СППР (Decision Support Systems — DSS) — це інформаційні системи третього покоління. СППР — інтерактивна комп'ютерна система, яка призначена для підтримки різних видів діяльності в разі прийняття рішень зі слабоструктурованих або неструктурованих проблем.

Інтерес до СППР як перспективної галузі використання обчислювальної техніки та інструментарію підвищення ефективності праці у сфері управління економікою постійно зростає. У багатьох країнах розробка та реалізація СППР перетворилася на сферу бізнесу, що швидко розвивається. СППР мають не тільки загальне інформаційне забезпечення, а й загальне математичне забезпечення — бази моделей, тобто реалізована ідея розподілу обчислень подібно до того, як розподіл даних став вирішальним фактором у звичайних інформаційних системах. Усвідомлення важливості розподілу обчислень в автоматизованих розрахунках виникло тоді, коли було помічено, що в багатьох прикладних програмах використовуються аналогічні обчислення, а індивідуальні фактори, які впроваджуються в прикладні програми для допомоги конкретному користувачеві, вносять незначні відмінності.

Крім того, спостерігалося значне дублювання дій і процедур під час розробки, реалізації та тестування цих обчислювальних функцій.

Розмаїття сфер економічної діяльності сприяє появі великої кількості інформаційних систем економічного характеру, які вбирають у себе всі особливості структури управління, схеми декомпозиції управлінських завдань і предметних технологій. Відповідно до сфери застосування виділяють такі інформаційні системи: банківські, страхові, податкові, фондового ринку, промислових підприємств. Інформаційні системи можуть значно різнитися за типами об'єктів управління, характером і обсягом розв'язуваних задач та низкою інших ознак.

За ступенем автоматизації перетворення економічної інформації інформаційні системи поділяються на такі групи: немеханізовані (ручні), напівмеханізовані, механізовані, автоматизовані та автоматичні. Для розв'язання за допомогою обчислювальної техніки будь-якої економічної задачі необхідно створити певні умови. Ця проблема вирішується розробкою і впровадженням різних видів забезпечення визначених державним стандартом з упровадження інформаційних технологій.

За час виникнення і розвитку ІС в економіці мали різну структуру цих компонентів, яка значною мірою залежала від техніко-експлуатаційних характеристик обчислювальної техніки, що в той чи інший період використовувалася для автоматизації економічних задач. Комп'ютерні інформаційні системи належать до класу складних систем, які містять у собі багато різноманітних елементів, що взаємодіють. Тому при створенні комп'ютерних ІС потрібно визначати їх структуру. До характерних ознак потрібно віднести: тривалий життєвий цикл; різноманітність апаратного забезпечення, що використовується; різноманітне ПЗ; масштабність і складність задач, що вирішуються; перетин безлічі різних предметних областей; територіальний розподіл і відповідно до цього орієнтацію на використання локальних і глобальних обчислювальних мереж для обміну і обробки інформації.

### *12.2 Кібератаки на державні інформаційні системи та об'єкти критичної інформаційної інфраструктури України*

Кібератаки на державні органи можуть бути складовою частиною кібервійни або гібридної війни і при цьому становити загрозу для національної та глобальної безпеки, оскільки вони можуть призвести до витоку важливої інформації, порушити роботу державних систем та призвести до різних негативних наслідків. Так, наприклад, в Європі основними цілями хакерів з 2022 року, окрім України, стали Польща, країни Балтії, Північної Європи та Німеччина. Частка кібератак на країни Європейського Союзу (далі – ЄС) зросла з близько 10% у першому кварталі 2022 року, до майже 50% у 2023 році. Загалом на Україну у 2022 році було здійснено 162 кібератаки; на Польщу – 114; Естонію, Литву та Латвію – 157; Швецію, Норвегію, Данію та Фінляндію – 95, Німеччину – 57.

Цілком зрозуміло, що державні органи зазвичай володіють ключовими частинами інфраструктури, такими як: енергетика, транспорт, телекомунікації тощо. А тому кібератаки, спрямовані саме на ці сектори, створюють найбільшу загрозу. А оскільки кіберзагрози можуть мати транснаціональний характер, дослідження відповідальності сприяє міжнародній співпраці у боротьбі з кіберзлочинами, а встановлення норм та міжнародних стандартів допомагає ефективніше реагувати на такі загрози.

Кібератака – це поняття, яке стало вже звичним явищем у сучасному суспільстві. Соціологи всього світу одностайно стверджують, що сучасне суспільство стало як ніколи раніше конфліктним. Кількість конфліктів у політичній, соціальній, трудовій, релігійній, а також особистісних сферах невпинно збільшується. В свою чергу, розвиток науки та новітніх технологій не завжди приносить користь, а навпаки – їх використання стає вдалим інструментарієм для винахідливих віртуальних злочинців. Основною метою цих атак є

завдання шкоди критичній інфраструктурі країни.

Глобально спостерігається стійка тенденція до зростання кількості цілеспрямованих кібератак на об'єкти критичної інфраструктури протягом останніх років. І тому, у зв'язку з можливими негативними наслідками в разі реалізації кібератак, важливо відзначити, що забезпечення ефективного функціонування системи кіберзахисту країни залишається високо пріоритетним завданням.

Створення безпечного кіберпростору є одним із напрямів інформаційної політики. В Окінавській хартії глобального інформаційного суспільства, прийнятій лідерами країн вісімки у японському м. Окінава у 2000 р., кіберпростір розглядається як частина глобального інформаційного простору, пов'язана з комп'ютерною інфраструктурою, насамперед з Інтернетом.

Кіберпростір це середовище, створене організованою сукупністю інформаційних процесів на підставі об'єднаних загальними принципами та правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем незалежно від форми власності. Кіберпростір держави перебуває під різноманітними кіберзагрозами, серед яких вплив на:

1) стан електронних інформаційних ресурсів та на можливість доступу до інформації;
2) функціонування об'єктів критичної інфраструктури;
3) складові частини інформаційно-комунікаційної інфраструктури;
4) морально-психологічний стан суб'єктів кіберпростору.

Тож поняття *кібербезпека* позначає стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та / або телекомунікаційних мереж, за якого мінімізується можливість завдати їм шкоди (через неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації) і стосується не лише технічних питань і технологічного складника, а й людського чинника – ворожих інсайдерських дій чи людський помилок, а також проблем владних відносин на національному та міжнародному рівнях.

Можливість країни впливати на кіберпростір у науковій літературі окреслили поняттям кіберпотужність, яка залежить від багатьох чинників (можливості інтернету та інформаційних технологій, можливості інтернет-ринку та IT-індустрії та ін.). Рідше у вітчизняних джерелах використовується термін кіберсила (CyberPower) – потужність на основі інформаційних ресурсів, що залежить від ресурсів, які характеризують кіберпростір. Кіберсила країни вимірюється через такі параметри: рівень залежності, атак та захисту в кіберпросторі. Подію, яка може порушити кібербезпеку (конфіденційність, цілісність та доступність інформації у кіберпросторі), називають кіберінцидентом.

До пріоритетів України в сфері кібербезпеки належать: розвиток інформаційної інфраструктури держави; розвиток мережі реагування на комп'ютерні надзвичайні події (CERT – Computer Emergency Response Team – команда реагування на комп'ютерні надзвичайні події), розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів, забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони, розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО для посилення спроможностей України у сфері кібербезпеки.

П'ятого жовтня 2017 року було прийнято Закон України «Про основні засади забезпечення кібербезпеки України», який «визначає правові та організаційні основи

забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки».

Важливим є питання формування ефективної національної системи кібербезпеки. Вона «має забезпечити взаємодію з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об'єднань, а також підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та / або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури».

Суб'єктами національної системи кібербезпеки, які становлять її основу, є Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи. Кожен з цих суб'єктів бере на себе частину зобов'язань, щоб забезпечувати кібербезпеку України, а координацію та контроль їх діяльності має здійснювати Рада національної безпеки і оборони України. Також «мають бути створені умови для залучення підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інфраструктури, до забезпечення кібербезпеки України».

Кіберзагрози охоплюють різноманітні впливи агресора, яким можуть бути окремі держави, групи та особи, на різні сфери життя держави: економічну, науково-технічну, сферу державного управління, оборонно-промисловий і транспортний комплекси, інфраструктуру електронних комунікацій, сектор безпеки і оборони України.

Нині кіберзлочинність не обмежується збиранням, зберігання, використанням, знищенням, поширенням персональних даних, незаконними фінансовими операціями, крадіжками та шахрайствами в мережі Інтернет, а стає транснаціональною проблемою та «здатна завдати значної шкоди інтересам особи, суспільства і держави.

*Кібератака* розглядається як сукупність дій противника або ворожої групи, яка намагається досягти певної негативної для об'єкта атаки цілі чи ефекту з використанням комп'ютерної техніки зокрема чи можливостей кіберпростору в цілому, найчастіше – з використанням спеціально розроблених для таких завдань засобів. Сукупність кібератак, що перевищують за своїм загальним негативним впливом певне порогове значення, можуть розглядатися як початок кібервійни.

Кібератаки можуть здійснюватися дилетантами, хакерами, інсайдерами з метою особистого збагачення чи вигоди, а також спонсоруватися державою з метою шпигунства чи в умовах ведення інформаційної війни.

До основних кіберзагроз України належать:

1) використання кібератак для досягнення політичних цілей (атаки на системи ЦВК під час двох виборчих кампаній, використання проти українських урядових і неурядових структур), зокрема за допомогою бот-мереж;

2) поява нових та модифікація наявних зразків шкідливого програмного забезпечення проти України (віруси BlackEnergy, Uroboros, EnergeticBear, CrouchingYeti, EpicTurla);

3) поширення шкідливого програмного забезпечення, спрямованого на формування бот-мереж; фальшивих антивірусів, вірусів для основних мобільних платформ (у т.ч. для збирання даних з пристроїв, спостереження, запису розмов і перехоплення повідомлень).

Загрози кібербезпеці актуалізуються через дію таких чинників:

1) невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам;

2) недостатній рівень захищеності критичної інформаційної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз;

3) безсистемність заходів кіберзахисту критичної інформаційної інфраструктури;

4) недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інформаційної інфраструктури та державних електронних інформаційних ресурсів;

5) недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру;

6) недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки.

Відповідно до Стратегії кібербезпеки України боротьба з кіберзлочинністю передбачає здійснення таких заходів:

1) створення ефективного і зручного контакт-центру для повідомлень про випадки кіберзлочинів та шахрайства у кіберпросторі, підвищення оперативності реагування на кіберзлочини правоохоронних органів, зокрема їх регіональних підрозділів;

2) удосконалення процесуальних механізмів щодо збирання доказів в електронній формі, що стосуються злочину, удосконалення класифікації, методів, засобів і технологій ідентифікації та фіксації кіберзлочинів, проведення експертних досліджень;

3) запровадження блокування операторами та провайдерами телекомунікацій визначеного (ідентифікованого) інформаційного ресурсу (інформаційного сервісу) за рішенням суду;

4) упровадження схеми (протоколу) координації правоохоронних органів щодо боротьби з кіберзлочинністю;

5) підготовка суддів (слідчих суддів), слідчих та прокурорів для роботи з доказами, що стосуються злочину, отриманими в електронній формі, з урахуванням особливостей кіберзлочинів;

6) запровадження особливого порядку зняття інформації з каналів телекомунікацій у випадку розслідування кіберзлочинів.

У межах реалізації Стратегії кібербезпеки України в 2015 році сформовано Департамент кіберполіції як структурний підрозділ Національної поліції України, що спеціалізується на попередженні, виявленні, припиненні та розкритті кримінальних правопорушень, механізмів підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних та комп'ютерних інтернет-мереж і систем. Його здобутками, зокрема, є те, що в 2016 р. було виявлено та знешкоджено бот-мережу Mumblehard, керовану з території Російської Федерації, що займалася розсиланням спаму.

### *12.3 Реальні та потенційні загрози інформаційному простору України: спеціальні інформаційні операції (СІО) та акти зовнішньої інформаційної агресії (АЗА)*

Спеціальна інформаційна операція (СІО) – це сплановані дії, спрямовані на ворожу, дружню або нейтральну аудиторію з метою схилення до прийняття управлінських рішень або (та) вчинення дій, вигідних для суб'єкта інформаційного впливу. СІО можуть передбачати також вплив на інформаційно-технічну інфраструктуру, але для більш ефективного впливу на свідомість і поведінку людей. СІО здійснюються в кілька етапів і можуть бути

довгостроковими (більше місяця), середньостроковими (два-чотири тижні) й короткостроковими (один-два тижні).

Слід зауважити, що СІО складається з поєднаних між собою часом, метою, завданнями, силами й засобами проведення акцій інформаційного впливу. СІО здійснюються за приблизно однаковою схемою:

1. Інформаційний етап передбачає створення інформаційного приводу – конкретної або вигаданої події, яка використовується в СІО.

2. "Розкручування" інформаційного приводу забезпечує поступове зростання напруження (кількості повідомлень і їх сенсаційності, тенденційності, емоційності та, як правило, недостовірності).

3. Загострення напруження є основною частиною СІО, що полягає у використанні інформаційного приводу для досягнення цілей операції.

4. Вихід із операції або етап закріплення – забезпечення плавного завершення СІО після досягнення поставленої мети. Якщо мету не досягнуто, як правило, готується нова СІО.

Слід виокремити основні ознаки проведення СІО: збільшення кількості повідомлень негативного змісту з певної соціальнополітичної або (та) економічної тематики; зростання емоційності; зростання тенденційності; збільшення сенсаційності; лавиноподібність (на першому етапі – поступове, на другому – значне, на третьому – різке зростання напруження); взаємоузгодження дій суб'єктів проведення СІО; час проведення (від одного тижня до двох місяців, але переважно від двох тижнів до місяця).

Суб'єктами проведення СІО є: керівництво іноземної держави – головний суб'єкт, всі інші – виконавці; ЗМІ (іноземні та підконтрольні вітчизняні); неурядові організації (іноземні й підконтрольні вітчизняні); спецслужби іноземної держави; Інтернетні ресурси; агентура впливу іноземних держав та підконтрольні лобістські структури із представників влади, управління, місцевого самоврядування, політичних партій, громадських і релігійних організацій та відомих діячів культури.

СІО та АІВ передбачають досягнення таких цілей:

1. У мирний час: домінування в інформаційному просторі, вплив на соціально-політичну ситуацію в регіоні, формування власного позитивного іміджу.

2. У воєнний час: інформаційно-психологічне забезпечення діяльності вищого військово-політичного керівництва.

3. У післявоєнний час: забезпечення процесу формування лояльної влади, сприяння соціально-економічному розвитку в регіоні, впровадження програм гуманітарної допомоги.

Основними методами СІО та АІВ є: дезінформування; пропаганда; диверсифікація громадської думки; психологічний тиск; поширення чуток.

Дезінформування – це метод, який передбачає обман чи уведення об'єкта впливу в оману щодо справжності намірів для спонукання його до запрограмованих дій.

Пропаганда – поширення політичних, філософських, наукових, художніх, інших мистецьких ідей із метою їх упровадження в громадську думку та активізації використання цих ідей у масовій практичній діяльності населення. Водночас до пропаганди належать повідомлення, які поширюються для здійснення вигідного впливу на громадську думку, провокування запрограмованих емоцій та зміни ставлення чи поводження певної групи людей у напрямі, безпосередньо чи опосередковано вигідному організаторам.

Диверсифікація громадської думки – це розпорошення уваги панівної еліти держави на різні штучно акцентовані проблеми й відволікання цим від вирішення нагальних завдань суспільно-політичного та економічного розвитку для нормального функціонування суспільства й країни.

Поширення чуток – це діяльність щодо поширення різної інформації (переважно

неправдивої) серед широких верств населення здебільшого неофіційними каналами з метою дезорганізації суспільства та держави або їхніх установ чи організацій. За одним із визначень, чутки – це циркулююча форма комунікації, за допомогою якої люди, котрі перебувають у неоднозначній ситуації, об'єднуються, утворюючи зрозумілу їм інтерпретацію цієї ситуації, спільно використовуючи при цьому власні інтелектуальні можливості.

Чутки самопоширювані. Їхня природа базується на інформації, яку важко втримати. Особа обов'язково має розповісти про почуте комусь іншому. Достатньо створити відповідну чутку та запустити її в обіг у потрібному місці в слушний час. "Людський поголос" зробить решту. Позитивний чинник використання цієї форми СІО полягає ще й у тому, що практично немає ефективних засобів протидії чуткам.

На офіційному рівні зупинити їх неможливо: офіційні заходи протидії викликають прямо протилежний ефект: для людей, яких безпосередньо цікавлять чутки, це є підтвердженням правдивості останніх. Чим численніші намагання їх спростувати, тим більша упевненість у їхній достовірності. Єдиний можливий спосіб подолання ефективності чуток – цілковите їх ігнорування. Як правило, через деякий час напруження спадає, зайва активність в обговоренні уже неактуальних новин згасає, інтерес до порушеної в чутках проблеми зникає.

СІО та АІВ належать до специфічних форм і методів впливу, ефективне використання яких потребує відповідної підготовки та високої майстерності, ґрунтовних наукових розробок і постійного практичного вдосконалення. Сучасна розвинена держава спроможна за допомогою СІО та АІВ отримати певну перевагу над противником ще до застосування традиційних бойових засобів. За оцінками фахівців, СІО якісно змінюють характер бойових дій, про що наочно свідчать останні локальні конфлікти та війни: перемагає той, хто здобув інформаційну перевагу.

Здійснення СІО й захист від них є невід'ємною передумовою забезпечення національної безпеки держави, вони проводяться як за мирного часу, так і у воєнний період. Основні аспекти СІО – психологічний, культурний, інтелектуальний, технологічний та економічний. Концепції національної безпеки багатьох провідних країн світу визначають основні напрями застосування збройних сил у XXI столітті. Підкреслюється, що головною рисою нового століття буде перенесення акцентів у галузь інформаційного протиборства, а досягнення інформаційної переваги стане обов'язковою умовою перемоги над будь-яким противником.

### *12.4 Забезпечення інформаційної безпеки України в умовах російської агресії*

В умовах воєнного стану країни особливо актуальним постало питання необхідності єдиної інформаційної політики. У зв'язку із цим Президент України підписав Указ № 152/2022, яким увів в дію Рішення Ради національної безпеки і оборони України «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану». Раніше РНБО України, «ураховуючи пряму військову агресію з боку Російської Федерації, активне поширення державою-агресором дезінформації, викривлення відомостей, а також виправдовування або заперечення збройної агресії Російської Федерації проти України, з метою донесення правди про війну, забезпечення єдиної інформаційної політики в період дії в Україні правового режиму воєнного стану», вирішила: «Установити, що в умовах воєнного стану реалізація єдиної інформаційної політики є пріоритетним питанням національної безпеки, забезпечення якої реалізується шляхом об'єднання усіх загальнонаціональних телеканалів, програмне наповнення яких складається переважно з інформаційних та/або інформаційно-аналітичних передач, на єдиній інформаційній платформі стратегічної комунікації – цілодобовому інформаційному марафоні «Єдині новини #UAразом».

В умовах інформаційної війни, у ході якої поширюється безліч фейків, важливо, щоб

суспільство мало певний рівень медіакультури та медіаграмотності. Щоб люди не панікували до того, як перевірять інформацію. Щоб уміли відрізняти брехню від правди, виявляти ботів у соціальних мережах. Корисну роботу із цією метою проводить Національна спілка журналістів України.

Коли російські агресори завдали ракетного удару по житловому будинку в Одесі, у результаті якого загинуло вісім і поранено 18 людей, вони намагалися зняти з себе відповідальність за скоєне, поширивши спочатку фейк про те, що вразили військовий об'єкт, потім після його викриття військовий об'єкт перетворився на якусь нафтобазу.

І цю брехню було викрито Одеською міською владою, яка опублікувала фото з місця трагедії. Тоді російські пропагандисти вигадали новий фейк про те, що житловий будинок став жертвою українських ППО. Однак і цей ворожий фейк був спростований фотографією будинку з характерними руйнуваннями від ракетних ударів. Це вже далеко не перший фейк кремлівської пропаганди, «російська пропаганда вже намагалася неодноразово приховати свою причетність до масової загибелі українців. Яскравий приклад цьому – ракетний обстріл залізничного вокзалу в Краматорську, коли кремль спочатку радів знищенню «військової інфраструктури у Краматорську». Коли ж стала відома правда про вбивство пів сотні цивільних людей, то росіяни негайно видалили всі свої «новини» та звинуватили в усьому нашу державу».

Для того щоб ворожа брехня не мала негативного впливу на населення, необхідно, за можливості, викривати всі фейки, що запускаються в український інформаційний простір. Це дасть змогу громадянам не лише отримувати правдиву інформацію, а й відчувати підтримку влади, яка постійно з ними на зв'язку.

Створення ефективної системи стратегічних комунікацій, метою якої є гарантування ефективної інформаційної взаємодії між органами державної влади, органами місцевого самоврядування та суспільством з питань кризових ситуацій. Зміцнення позитивного іміджу України.

Якщо стратегічні комунікації – це система внутрішніх і зовнішніх комунікацій, то зв'язки з громадськістю – це один зі складників стратегічних комунікацій. На нашу думку, в умовах війни органи державної влади, органи місцевого самоврядування демонструють високий рівень інформаційної взаємодії із суспільством. Міністерства та відомства систематично доводять до суспільства актуальну інформацію. А виступи Президента України, голів обласних військових адміністрацій, присвячені аналізу поточної ситуації, звіту про свою роботу, стали для громадян звичними. Формування іміджу України – це зона відповідальності зовнішніх комунікацій. Зміцнення позитивного іміджу України, як внутрішнього, так і зовнішнього, необхідне тому, що він багато в чому впливає на політичну, економічну та культурну перспективу розвитку країни.

Формування інформаційного суспільства і розвиток інформаційних технологій, що продовжується, чинять значний вплив на відносини у сфері військової безпеки: інформаційні технології активно використовуються не лише в комерційній, а й у військовій галузі. Слід зазначити, що інформаційна безпека у військовій справі є досить традиційною сферою. Військові структури завжди захищалися від засобів розвідки всіма способами: пасивними та активними. Сьогодні одним із найістотніших об'єктів безпеки в оборонній сфері є інформаційні ресурси та інформаційна структура оборонного потенціалу країни (збройних сил та військово-промислового комплексу).

Важливо, що це сучасні засоби озброєння, військової техніки, системи управління військами і зброєю є системами критичних додатків із високим рівнем комп'ютеризації. Ці системи можуть виявитися дуже вразливими з погляду впливу інформаційної зброї як у військовий, так і у мирний час. Останнє може призвести до того, що до загрозливого періоду

зброя стримування країни виявиться повністю або частково заблокованою за рахунок прихованого впровадження у програмне забезпечення систем управління ним програмних закладок. Про реальність такої ситуації свідчить досвід локальних воєн останніх років.

Не випадково багато авторитетних дослідників уважають, що забезпечення військової безпеки в XX1 ст. все більше залежатиме від інформаційних чинників. Так, відомий американський футуролог О. Тоффлер у книзі «Війна та антивійна» зазначає, що інформація стає найважливішим військово-стратегічним ресурсом щонайменше або навіть важливішим, аніж традиційні види озброєнь і військової техніки. А це означає, що держава, яка дбає про свій оборонний потенціал, має приділяти величезну увагу розвитку методів інформаційної протидії та інформаційного впливу. Ця теза підтверджується історією воєн XX і початку XX1 ст., у яких роль інформаційного чинника у забезпеченні оборонної безпеки різко зросла.

Важко уявити сучасний збройний конфлікт, у ході якого не задіяні інформаційні можливості конфліктуючих сторін. Із метою інформаційної війни використовується практично вся інформаційна інфраструктура держави та суспільства. Щодо військової сфери, то рівень її забезпечення засобами захисту від застосування інформаційно ємних технологічних досягнень прямо впливає на рівень національної безпеки держави. Нові інформаційні технології відкрили небачені раніше можливості отримання інформації про противника, а відповідно, і попередження про можливі конфлікти та напади. «Своєчасне інформування про наміри Росії, енергійний інформаційний та дипломатичний діалог дали змогу Заходу консолідувати свою позицію та зусилля. У результаті європейська і світова реакція на розв'язану війну виявилася несподівано (для Кремля) швидкою та сильною, а світова громадська думка, будучи обізнаною заздалегідь, негайно стала на бік жертви агресії. У результаті Кремль уперше за багато років начисто програв світове інформаційне поле».

Застосування інформаційних технологій військовими відкрило нові можливості щодо забезпечення оборони держави. Володіння інформаційними ресурсами та його захист у військовій сфері стали таким самим неодмінним атрибутом, як озброєння, боєприпаси, транспорт тощо. Виграш України в інформаційному протиборстві під час війни з Росією сприятиме досягненню її стратегічних цілей.

### *12.5 Створення безпечних умов існування інформаційних технологій: питання захисту інформації, інформаційної інфраструктури держави, інформаційного ринку та розвитку інформаційних процесів*

Інформаційна безпека передбачає можливість безперешкодної реалізації суспільством і окремими його членами своїх конституційних прав, пов’язаних з можливістю вільного одержання, створення й розповсюдження інформації. Поняття інформаційної безпеки держави слід також розглядати у контексті забезпечення безпечних умов існування інформаційних технологій, які включають питання захисту інформації, як такої інформаційної інфраструктури держави, інформаційного ринку та створення безпечних умов існування і розвитку інформаційних процесів. Необхідний рівень інформаційної безпеки забезпечується сукупністю політичних, економічних, організаційних заходів, спрямованих на попередження, виявлення й нейтралізацію тих обставин, факторів і дій, які можуть вчинити збиток чи зашкодити реалізації інформаційних прав, потреб та інтересів країни і її громадян .

На підставі аналізу існуючих методик побудови підсистем захисту інформації виділяються різні заходи, заходи і форми реалізації принципів інформаційної безпеки. Деякими авторами, наприклад, рекомендується використовувати технологічні, адміністративні, законодавчі і фізичні заходи, інші науковці у якості базових домінант виділяють морально-етичні, законодавчі, організаційні, економічні і технічні заходи.

На нашу думку, сутність заходів при синтезі і аналізі основних напрямів

інформаційної безпеки зводиться до наступних основних заходів: 1) морально-етичних; 2) правових; 3) страхових; 4) організаційних; 5) інженерно-технічних; 6) апаратно-програмних.

*Морально-етичні заходи.* Сукупність цих заходів повинна включати навчання персоналу, підвищення кваліфікації, профілактичні бесіди, проведення занять із залученням провідних організацій і фахівців, проведення спеціальної підготовки EIS на предмет протидії шахрайству. Мета вказаних дій – досягти правильного розуміння співробітниками підприємства завдань по захисту конфіденційних відомостей і їх максимальне сприяння в питаннях забезпечення інформаційної безпеки. При підборі на відповідальну роботу необхідно враховувати психологічні особливості кандидата, застосовувати працю психологів, соціологів, використовувати тестування.

*Правові заходи.* Належне оформлення права власника (підприємства, фірми або організації) на інформаційні ресурси (програми, дані про технологічні процеси та ін.), закріплення відповідальності обслуговуючого персоналу і користувачів інформаційно-обчислювальних комплексів і мереж, підвищення правової культури співробітників підприємства, визначення переліку конфіденційних даних дозволяє належним чином організувати і реалізувати підсистему захисту інформації.

*Страхові заходи.* Досягти абсолютної безпеки інформації неможливо. Навіть при організації підсистеми захисту завжди існує реальна можливість настання непередбачуваної події, що спричиняє за собою зниження працездатності виробничих систем, втрату конфіденційної інформації і втрату доходу. Тому проблема страхування стає особливо актуальною.

Страхування інформаційних ризиків господарюючих суб’єктів, таких як відмови, збої технічних і програмних засобів, впровадження „вірусів”, ненавмисні дії персоналу, несанкціонований доступ, просочування інформації за рахунок побічних електромагнітних випромінювань і наведень, може стати гарантом інформаційній безпеці, покрити збитки підприємства в разі настання страхового випадку. Крім того, необхідно забезпечити можливість отримання спеціальної підготовки і консультацій працівників підприємства. У ряді країн (США, Канада, Ізраїль) такого роду механізм вже запущений, що сприяє забороні зростання числа злочинів проти особи і власності.

Виходячи з класифікації ризиків і враховуючи введення інформації в систему товарних, майнових відносин, інформаційні ризики відносяться до чистих, майнових, виробничих ризиків.

*Організаційні заходи.* Основна увага при проектуванні і реалізації підсистеми інформаційної безпеки завжди приділялася інженерно-технічним і апаратно-програмним заходам. Створення механізмів розмежування доступу до програмних і апаратних ресурсів засобів обчислювальної техніки і носіїв інформації, організація пропускного режиму, регламентація обліку, зберігання конфіденційної інформації, обстеження об’єктів обчислювальної техніки, проведення спецдосліджень і спецперевірок технічних засобів, реєстрація дій суб’єкта і його процесу, розробка можливих реакцій підсистеми і персоналу у випадку виникнення критичних ситуацій є неповним переліком організаційних заходів (заходів) інформаційної безпеки. Розробка організаційних заходів є найбільш трудомістким етапом побудови підсистеми інформаційної безпеки, на який припадає до 60% загального обсягу заходів щодо забезпечення інформаційної безпеки.

До організаційних заходів, на нашу думку, можна віднести розробку посадових інструкцій по забезпеченню інформаційної безпеки, розмежування допуску і доступу до інформаційних ресурсів, визначення порядку експлуатації носіїв інформації, привласнення грифів документів і масивам даних, контроль допуску і доступу до інформації, постійний контроль дотримання режиму і інструкцій, встановлення повноважень і відповідальності.

Організаційні заходи регламентують процеси функціонування підсистеми інформаційної безпеки, використання ресурсів, діяльність працівників підприємства, порядок взаємодії з підсистемою, визначають взаємозв'язок всіх підсистем промислового підприємства із зовнішнім середовищем. Важливо відмітити, що поки не будуть реалізовані дієві заходи організаційного (адміністративною) захисту об'єкту інформаційної безпеки, інші заходи будуть, без сумніву, неефективні.

Необхідність і ефективність *інженерно-технічних заходів* підтверджується статистикою, відповідно до якої більше 50 % вторгнень здійснюється в комерційні об'єкти з вільним доступом персоналу і клієнтів і лише 5 % – в об'єкти з посиленим режимом охорони, із застосуванням спеціально вивченого персоналу і складних технічних систем охорони .

Основу захисту складають механічні засоби і інженерні споруди, що перешкоджають фізичному руху зловмисників до місця знаходження об'єкту захисту, технічні засоби, що інформують про проникнення зловмисників в контрольовану зону і що дозволяють спостерігати ситуацію в них, а також засоби і люди, що усувають загрози.

*Апаратно-програмні заходи.* До них відносяться різні електронні пристрої і спеціальні програми, які реалізують самостійні або в комплексі з іншими засобами ідентифікацію і аутентифікацію користувачів інформаційних ресурсів, розмежування доступу до ресурсів, контроль і забезпечення якісних характеристик інформації конфіденційності даних, реєстрацію і аналіз подій підсистеми інформаційної безпеки, резервування інформаційних ресурсів і компонентів виробничої системи.

До основних апаратно-програмних заходів щодо розмежування доступу до ресурсів, забезпечення цілісності і конфіденційності інформації необхідно віднести криптографічний захист інформації, ідентифікацію і аутентифікацію користувачів. Криптографічні перетворення дозволяють вирішити дві головні проблеми захисту даних: проблему конфіденційності (шляхом позбавлення противника можливості витягувати інформацію з каналу зв'язку) і проблему цілісності (шляхом позбавлення противника можливості змінити повідомлення так, щоб змінився його сенс, або ввести помилкову інформацію в канал зв'язку). Окрім вказаних заходів існують інші функції, що виконуються програмами з метою захисту даних від спотворення і руйнування. Вживання простих методів резервування інформації, створення резервних копій при обробці даних інформаційною системою, перевірка достовірності повідомлень дозволяють досягти стійкості функціонування виробничої системи.

**ПИТАННЯ ДЛЯ САМОПЕРЕВІРКИ**

1. Охарактеризуйте змістовну і представницьку складові, ціннісні аспекти інформаційної системи.
2. Що включає в себе інформаційна система як об'єкт інформаційного впливу?
3. Вкажіть об'єкти критичної інформаційної інфраструктури України.
4. Яка мета здійснення кібератак на державні інформаційні системи?
5. Окресліть реальні та потенційні загрози інформаційному простору України.
6. В чому полягає сутність проведення спеціальних інформаційних операцій (СІО) та актів зовнішньої інформаційної агресії (АЗА)?
7. Яким чином здійснюється забезпечення інформаційної безпеки України в умовах російської агресії?
8. Вкажіть шляхи створення безпечних умов існування інформаційних технологій.
9. Якими є перспективи розвитку інформаційного ринку та розвитку інформаційних процесів?

# ЛЕКЦІЯ 13
# ІНФОРМАЦІЙНА БЕЗПЕКА СИСТЕМИ ПУБЛІЧНОГО УПРАВЛІННЯ ТА АДМІНІСТРУВАННЯ

**План викладу:**

13.1Особливості феномену інформаційної безпеки у сфері публічного управління

13.2Безпека інформаційного простору в публічному управлінні: заходи забезпечення ефективної діяльності системи публічного управління.

13.3Діяльність органів та установ державного і публічного управління з питань захисту інформації.

13.4Організації системи захисту інформації у структурах державних органів та установ.

13.5Виклики та завдання побудови системи забезпечення кібербезпеки в органах публічного управління.

## *13.1 Особливості феномену інформаційної безпеки у сфері публічного управління*

В умовах повномасштабної військової агресії важливе значення та нові пріоритети набувають процеси реалізації функцій публічного управління у системі інформаційної безпеки. Аналізуючи нові виклики та перспективи впровадження інформаційних технологій визначають необхідність формування сучасних теоретико-методичних підходів до визначення поняття *публічного управління інформаційною безпекою*, що можна визначити як процес керування заходами, спрямованими на захист конфіденційної інформації від несанкціонованого доступу, використання, розголошення та знищення на рівні держави, організацій або громадян. Цей процес може включати створення відповідних законодавчих актів, установлення відповідних органів контролю та нагляду, проведення навчань та тренінгів з питань інформаційної безпеки, а також встановлення відповідних технологій та систем безпеки для захисту конфіденційної інформації.

Метою публічного управління інформаційною безпекою є забезпечення безпеки конфіденційної інформації від потенційних загроз, таких як кібератаки, віруси, шпигунський софт та інші шкідливі програми.

Однак, публічне управління інформаційною безпекою може також здійснюватися на рівні окремих організацій або громадян. Це може включати створення відповідних політик та процедур управління інформаційною безпекою, проведення навчань та тренінгів з питань інформаційної безпеки, а також встановлення відповідних технологій та систем безпеки для захисту конфіденційної інформації.

Враховуючи нові тенденції та виклики доцільно розподілити напрями публічного управління інформаційною безпекою на наступні – рис. 13.1

Враховуючи визначення сучасної ситуації доцільно сформувати запити до побудови системи публічного управління інформаційної безпеки на глобальному та національному рівнях. Зокрема, це аналіз викликів і загроз, які можуть вплинути на інформаційну безпеку, включаючи ризики кібератак, витоків даних, вірусів, шпигунського софту та інших загроз та розробка стратегії публічного управління інформаційною безпекою, включаючи визначення мети, завдань, призначення та відповідальності. А також, визначення необхідності створення органів управління інформаційною безпекою, їхніх повноважень та функцій та розробка політик і процедур для захисту інформації, включаючи контроль доступу до інформації, забезпечення цілісності та конфіденційності, а також процедур реагування на інциденти безпеки.

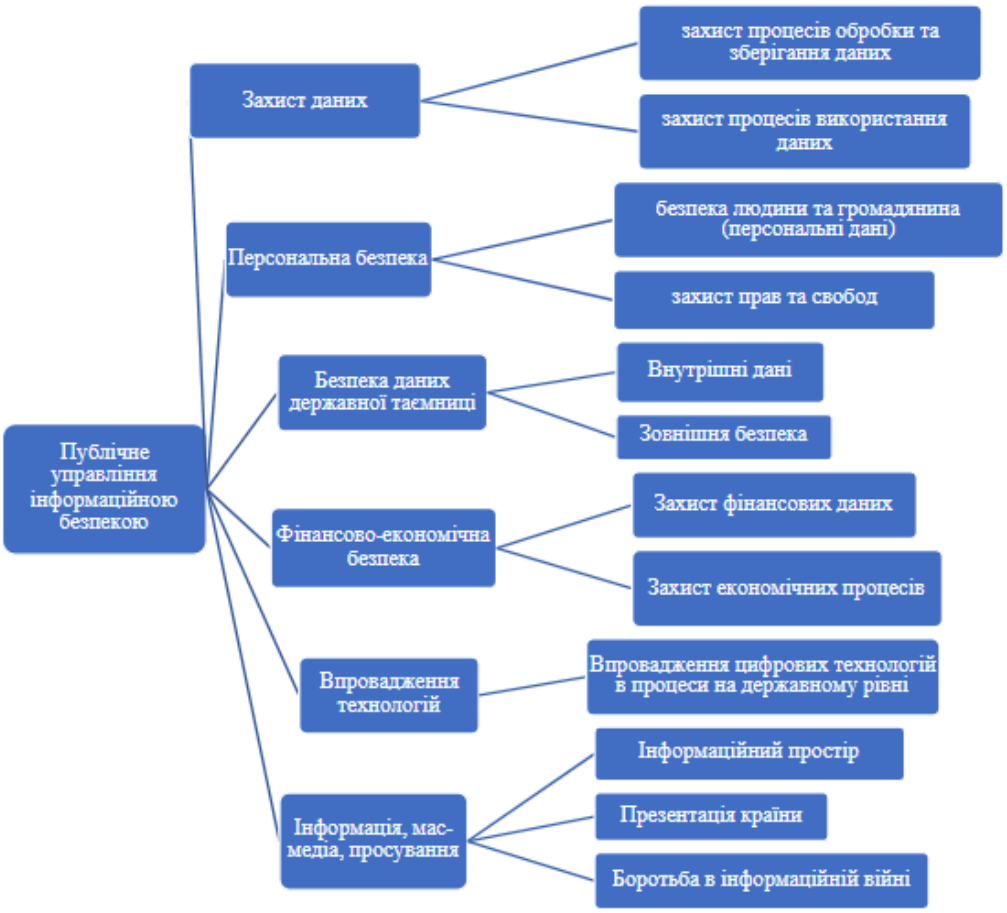



***Рис. 1*** *Структура напрямів публічного управління інформаційною безпекою*

Крім того, встановлення відповідних технологій та систем безпеки, таких як антивірусне програмне забезпечення, системи контролю доступу та системи моніторингу; проведення навчань та тренінгів з питань інформаційної безпеки для співробітників, клієнтів та інших зацікавлених сторін; розробка плану дій для реагування на інциденти безпеки, включаючи процедури повідомлення, відновлення даних та комунікації зі зацікавленими сторонами; оцінка ефективності системи публічного управління інформаційною безпекою та її відповідності вимогам законодавства та стандартів.

***13.2 Безпека інформаційного простору в публічному управлінні: заходи забезпечення ефективної діяльності системи публічного управління.***

Аналізуючи функції публічного управління та запити до побудови процесів інформаційної безпеки необхідно визначити системність таких процесів, що може бути представлено у вигляді наступної схеми – рис. 13.2.

Розглянемо *алгоритм реалізації державної політики у сфері інформаційної безпеки* в умовах сучасних викликів:

- Оцінка загроз. Перш за все, необхідно оцінити наявні загрози для інформаційної безпеки. Для цього можна використовувати різноманітні засоби аналізу та моніторингу, що дозволять виявити можливі джерела загроз та оцінити ступінь їхньої серйозності.

- Розробка стратегії. На основі результатів оцінки загроз слід розробити стратегію забезпечення інформаційної безпеки. Стратегія повинна передбачати заходи з превентивного захисту, виявлення та реагування на загрози, а також відновлення інформаційної інфраструктури в разі її порушення.

- Впровадження заходів. Для впровадження стратегії необхідно прийняти конкретні

заходи забезпечення інформаційної безпеки. Це можуть бути заходи з кібербезпеки, забезпечення захисту інформації від несанкціонованого доступу, захист критично важливих інформаційних систем, тощо.

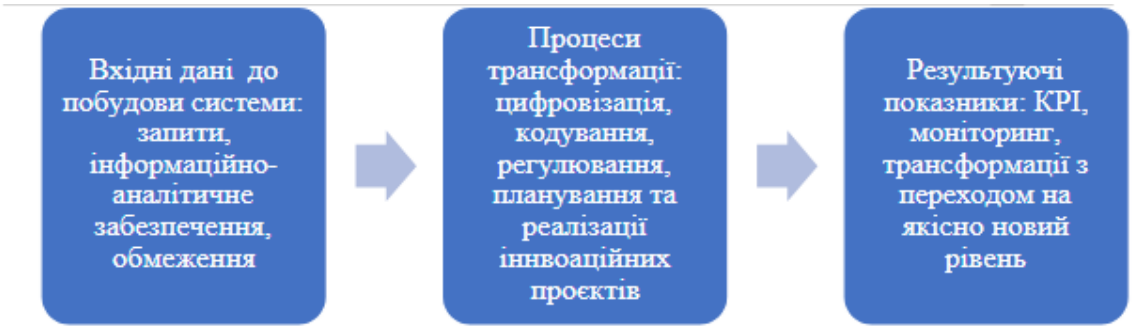



***Рис. 2*** *Система побудови процесів інформаційної безпеки на рівні публічного управління*

- Контроль та моніторинг. Для успішної реалізації стратегії необхідний постійний контроль та моніторинг за станом інформаційної безпеки. Це дозволить вчасно виявляти можливі загрози та реагувати на них.

- Підготовка та навчання кадрів. Для успішної реалізації політики інформаційної безпеки необхідно мати досвідчених та кваліфікованих кадрів. Тому необхідно проводити підготовку та підвищувати кваліфікацію співробітників, а також проводити навчання з питань кібербезпеки та захисту інформації.

- Співпраця з іншими державами та міжнародними організаціями. Загрози для інформаційної безпеки мають глобальний характер, тому співпраця з іншими країнами та міжнародними організаціями є важливою складовою державної політики в цій сфері. Це може включати обмін досвідом, спільні проекти з кібербезпеки, розробку стандартів безпеки, тощо.

- Забезпечення прав людини та свободи слова. При розробці політики інформаційної безпеки необхідно дбати про забезпечення прав людини та свободи слова. Це означає, що заходи, пов'язані з контролем та регулюванням інформаційного простору, повинні бути пропорційними та не обмежувати права людей на свободу висловлювання та інформаційну свободу.

- Фінансування. Реалізація державної політики у сфері інформаційної безпеки потребує достатнього фінансування. Для цього можуть бути виділені кошти з державного бюджету, або залучені кошти від інших джерел.

Отже, реалізація державної політики у сфері інформаційної безпеки в умовах сучасних викликів передбачає комплексні заходи забезпечення безпеки інформаційного простору, оцінку та моніторинг загроз, розробку та впровадження стратегії, контроль та моніторинг, підготовку та навчання кадрів, співпрацю зі стейкхолдерами.

Визначивши процеси системності та запити до реалізації функцій публічного управління інформаційною безпекою доцільно запропонувати наступні пропозиції щодо побудови системи публічного управління на національному рівні:

- раціоналізація ієрархічної структури управління інформаційною безпекою із визначенням відповідальних за розробку та впровадження стратегічних напрямів і політики інформаційної безпеки на національному рівні;

- розробка та впровадження відповідних стандартів та нормативно- правових актів з інформаційної безпеки, що будуть відповідати міжнародним стандартам;

- створення системи моніторингу та аналізу загроз та ризиків для інформаційної

безпеки на рівні публічного управління;

- забезпечення публічного управління кадровою складовою, що сприятиме формуванню та підтримці професійним забезпеченням;
- реалізація механізмів забезпечення безпеки інформаційних технологій шляхом застосування сучасних засобів криптографії, захисту мережі та захисту від кібератак;
- забезпечення доступу до інформації та даних у відповідності з вимогами законодавства та стандартів інформаційної безпеки.
- забезпечення взаємодії між різними органами влади та стейкхолдерами у реалізації системи інформаційної безпеки.

Для побудови ефективної національної системи публічного управління інформаційною безпекою доцільно розробити стандарти та нормативно-правові акти, створити систему моніторингу та аналізу загроз, розвивати кадрову політику, забезпечити безпеку інформаційних технологій, забезпечити доступ до інформації та даних та забезпечити взаємодію між різними органами влади.

### *13.3 Діяльність органів та установ державного і публічного управління з питань захисту інформації*

Публічне управління має важливу роль у забезпеченні інформаційної безпеки в умовах воєнного стану. У таких умовах державні органи та інші зацікавлені сторони повинні працювати в єдиному інформаційному просторі та діяти в координації один з одним та дотримуватися вимог законодавства.

Інформаційна політика держави має чотири основні напрями: розвиток національного інформаційного простору, розвиток інформаційного суспільства, розвиток офіційної комунікації та забезпечення інформаційної безпеки держави. Важливою складовою кожного з цих напрямів є державна політика інформаційної безпеки, адже вона забезпечує захист інформаційного суверенітету та інформаційних прав та свобод громадян.

Публічне управління здійснює контроль за виконанням законодавства, ке стосується інформаційної безпеки, та забезпечує дотримання прав та свобод громадян. Крім того, публічні органи управління мають розробляти та впроваджувати стратегії та програми щодо захисту критично важливої інформації в умовах війни. Оскільки ворог намагатиметься заволодіти важливою інформацією.

Під час війни публічне управління відіграє важливу роль у моніторингу інформаційних потоків, а також в поширенні точної та достовірної інформації про ситуацію на фронті та в країні в цілому.

Особливо небезпечними для безпеки держави і громадян є розміщення в публічному просторі інформації про критичну інфраструктуру, військові об’єкти, пересування військ тощо. Тому органи публічної влади мають звести до мінімуму поширення зазначеної інформації, оскільки першочерговими завданнями захисту інформації в автоматизованій системі в процесі електронної взаємодії є запобігання, поширення, модифікація, знищення, копіювання, блокування та неправомірне тиражування інформації обмеженого доступу.

Органам влади необхідно слідкувати за дотриманням статті 6 ЗУ «Про доступ до публічної інформації». Так, інформацією з обмеженим доступом є: конфіденційна інформація; таємна інформація; службова інформація.

Зауважимо й те, що обмеження доступу до інформації здійснюється відповідно до закону при дотриманні сукупності таких вимог:

«1) 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» (Закон, 2011, ст. 6).

Також публічні органи управління мають забезпечувати ефективну комунікацію між зацікавленими сторонами, щоб уникнути спотворення та недостовірної інформації.

Окрім того, публічне управління в умовах війни повинне забезпечити захист інформації від хакерських атак та кібернападів, а також запобігати поширенню фейків та дезінформації. Отже, роль публічного управління у забезпеченні інформаційної безпеки в умовах війни полягає у забезпеченні контролю за дотриманням законодавства, розробці та впровадженні стратегій та програм захисту інформації.

Умови воєнного стану ставлять перед державою особливі виклики з питань забезпечення інформаційної безпеки та публічного управління. Воєнна загроза вимагає від держави швидкої та ефективної реакції, що передбачає наявність готових та досконало спланованих механізмів забезпечення інформаційної безпеки. У цьому контексті система забезпечення інформаційної безпеки та публічного управління в умовах воєнного стану має бути досконалою та добре підготовленою.

Деякі методи та можливості забезпечення інформаційної безпеки в умовах війни включають забезпечення кібербезпеки: це охорона комп'ютерних систем від несанкціонованого доступу, вірусів та інших шкідливих програм.

Для забезпечення кібербезпеки в умовах війни можуть використовуватися різноманітні технічні та програмні засоби, такі як брандмауери, антивіруси, мережеві інструменти моніторингу та інші.

Забезпечення захисту інформації: це заходи для захисту конфіденційної інформації від несанкціонованого доступу. Забезпечення захисту інформації може включати шифрування, автентифікацію та інші методи.

Сприяння інформаційній війні: це використання інформації як зброї для ведення війни. В умовах війни інформаційна війна може включати розповсюдження дезінформації та пропаганди, використання соціальних мереж для впливу на громадську думку та інші методи.

Забезпечення фізичної безпеки інформації: це заходи для захисту комп'ютерної техніки та інших засобів зберігання інформації від фізичної руйнівної дії, такої як вандалізм або крадіжка.

У механізмі правового забезпечення діяльності публічних адміністрацій важливе місце займає громадський контроль. За умов дії правового режиму воєнного стану деякі нормотворчі процедури відбуваються у спрощеному порядку, а громадянська активність має певні обмеження. Отже, звичні для української політико-правової реальності інструменти коригування невдалих з точки зору громадськості правових новел (мітинги, блокування органів публічної влади тощо) нині не використовуються.

Змінилися форми впливу на ефективність вказаного процесу: перевагу отримали експертні обговорення та публікації у засобах масової інформації. Публічний службовець не має права обмежити доступ до інформації, не пояснивши, чому її оприлюднення завдасть більше шкоди, ніж принесе користі.

Відповідно до Закону України «Про доступ до публічної інформації», гарантується кожному громадянину доступ до публічної інформації. Запровадження обмеження доступу до конкретної інформації за результатами розгляду запиту на інформацію допускається лише за умови застосування вимог пунктів 1-3 частини другої статті 6 Закону (Закон, 2011).

Ці вимоги є «трискладовим тестом», який повинна пройти публічна інформація для визначення її відкритою чи обмеженою. Доступ до інформації може бути обмежено за умови додержання сукупності всіх трьох підстав (Гвоздік, 2022, с. 26).

Конфіденційною є інформація про фізичну особу, інформація, доступ до якої обмежено

фізичною або юридичною особою, крім суб'єктів владних повноважень, а також інформація, визнана такою на підставі закону (Закон, 1992).

В умовах воєнного стану, система забезпечення інформаційної безпеки та публічного управління стає важливим механізмом управління державою та забезпечення захисту інтересів громадян. В цьому контексті розглядається питання забезпечення безпеки інформаційного простору, управління інформацією, зокрема забезпечення конфіденційності та цілісності інформації, а також забезпечення взаємодії між різними державними структурами, військовими підрозділами та громадськістю.

Одним з найважливіших методів забезпечення інформаційної безпеки в умовах воєнного стану є розробка та впровадження спеціальних заходів технічного захисту інформації, які дозволяють забезпечувати конфіденційність і цілісність даних.

До таких заходів відносяться розробка та впровадження захисту від несанкціонованого доступу до інформації, шифрування даних, створення резервних копій, контроль доступу до інформації та інші. Крім того, важливим методом є розробка та впровадження спеціальних заходів забезпечення кібербезпеки, які дозволяють захищати інформаційний простір від хакерських атак та інших загроз.

Ще одним важливим методом забезпечення інформаційної безпеки та публічного управління в умовах воєнного стану є забезпечення ефективної комунікації між державними структурами та військовими підрозділами.

Один з методів забезпечення інформаційної безпеки в умовах воєнного стану – це використання системи раннього попередження про надходження інформаційної загрози. Ця система дозволяє оперативно виявляти, аналізувати та реагувати на інформаційні загрози. Крім того, важливим методом є розвиток кібербезпеки, що включає в себе заходи з попередження кібератак та забезпечення захисту від таких атак.

Одним з можливих методів забезпечення публічного управління в умовах воєнного стану є використання інформаційних технологій та електронного управління. Це дозволяє забезпечувати оперативний обмін інформацією між різними державними органами, а також між цими органами та населенням.

Крім того, важливим методом є впровадження систем електронного голосування, що дозволяє забезпечити швидке та безпечне голосування в умовах війни.

Ще одним важливим методом забезпечення публічного управління є розвиток системи публічної інформації та масової комунікації. Для цього необхідно розвивати та підтримувати роботу ЗМІ та соцмереж.

Один із методів забезпечення інформаційної безпеки в умовах воєнного стану – це створення ефективної системи моніторингу та аналізу інформації. Для цього потрібні спеціалізовані центри, які мають відповідні комп'ютерні програми для автоматизації збору та обробки інформації. Ці центри, як своєрідні «Мозкові центри» мають бути здатні оперативно реагувати на будь-які зміни у ситуації та забезпечувати необхідну інформацію для прийняття рішень.

Дієвим методом є підвищення медіакультури населення, саме державними органами проводиться низка заходів, які стосуються інформаційної гігієни.

Ще одним методом є забезпечення кібербезпеки. В умовах війни кібератаки можуть спричинити серйозні наслідки для держави, тому необхідно забезпечувати захист критичних об'єктів, систем керування та комунікаційних мереж. Необхідно розробити відповідні стратегії та програми для запобігання та протидії кібератакам.

Основним механізмом воєнно-інформаційної безпеки в умовах війни є розвідка і контррозвідка. Розвідка займається збором інформації про ворога, його зброю, техніку, тактику та плани. Контррозвідка ж займається захистом власної інформації та виявленням

та припиненням шпигунської діяльності. Отже, ефективна інформаційна діяльність може суттєво впливати на національну безпеку України. Взаємозв'язок між системами забезпечення інформаційної безпеки та публічного управління є вагомим у воєнних умовах.

### *13.4 Організації системи захисту інформації у структурах державних органів та установ*

Основним шляхом пошуку захисту інформації в складних інформаційних системах є вдосконалення системного підходу до самої проблеми захисту.

Під системністю розуміється, що захист інформації передбачає не лише створення відповідних захисних механізмів, але також включає регулярний процес, який застосовується на всіх етапах життєвого циклу інформаційної системи та використовує всі наявні засоби захисту. Це означає, що захист інформації повинен бути розглянутий як невід'ємна частина всієї інформаційної системи, а не просто як окремий компонент.

У сучасних умовах глобалізації та зростаючої конкуренції, захист інформації стає надзвичайно важливим аспектом як для організацій, так і для державних підприємств та корпорацій України. Створення надійних систем захисту і збереження інформаційних ресурсів на рівні всієї організації і її окремих підрозділів стає все більш актуальним, а успішність таких заходів безпосередньо впливає на конкурентоспроможність організації в цілому.

На сьогодні існують два основних підходи до визначення оптимальної стратегії побудови систем захисту інформації організацій. Перший підхід базується на перевірці відповідності рівня захищеності інформації в організації вимогам законодавчих актів або стандартів в галузі інформаційної безпеки. Однак цей підхід має свої недоліки, зокрема, коли рівень захисту інформації не визначений чітко, ускладняється вибір оптимального варіанту системи захисту. Другий підхід використовує методи та моделі оптимізації складних систем для визначення найкращого варіанту побудови систем захисту інформації. Цей підхід дозволяє більш ефективно враховувати особливості конкретної організації та знаходити оптимальні рішення з урахуванням різноманітних факторів.

Стрімкий розвиток інформаційних технологій привів до проблем захисту інформації або забезпечення безпеки інформації. Комплексні системи захисту інформації (КСЗІ) допомагають у вирішенні цих проблем. Дослідження та огляд методів і засобів, об'єднаних єдиним цільовим призначенням, які забезпечують необхідну ефективність захисту інформації в автоматизованих системах (АС) є актуальними в цей час.

Інформаційна безпека – стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації.

Українське законодавство по своєму захищає інформацію, відповідно до ст. 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» «Умови обробки інформації в системі: Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю»

Також законодавець визначає низку нормативно-правових документів у сфері комплексної системи захисту інформації: Закони України «Про інформацію»; «Про доступ до публічної інформації»; «Про захист персональних даних»; «Про електронні документи та електронний документообіг»; «Про захист інформації в інформаційно-телекомунікаційних системах»; «Про Державну службу спеціального зв'язку та захисту інформації України»; та «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» (затверджені ПКМУ від 29.03.2006 №373).

КСЗІ – це система технічних і нетехнічних заходів, що дозволяють запобігти або ускладнити можливість доступу до інформації, оброблюваної автоматизованим способом в інформаційно телекомунікаційних системах (ІТС). До процесу створення КСЗІ залучаються:

– організація, для якої здійснюється побудова КСЗІ (Замовник);

– організація, що здійснює заходи з побудови КСЗІ (Виконавець);

– Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ) (орган контролю);

– організація, що здійснює державну експертизу КСЗІ (Організатор експертизи);

– організація, у разі необхідності, залучена Замовником або Виконавцем для виконання деяких робіт зі створення КСЗІ (Підрядник).

Основною проблемою реалізації систем захисту є:

– з одного боку, забезпечення надійного захисту ідентифікації, що знаходиться в системі: унеможливлення випадкового і навмисного отримання інформації сторонніми особами, розмежування доступу до пристроїв і ресурсів системи всіх користувачів, адміністрації та обслуговуючого персоналу;

– з іншого боку, системи захисту не повинні створювати помітних незручностей користувачам в ході їх роботи з ресурсами системи.

Проблема забезпечення бажаного рівня захисту інформації досить складна, що вимагає для свого рішення не просто здійснення деякої сукупності наукових науково-технічних, організаційних заходів і застосування спеціальних засобів і методів, а створення цілісної системи організаційно-технологічних заходів і застосування комплексу спеціальних засобів і методів. Ефективність функціонування комплексних систем захисту інформації (КСЗІ) залежить від багатьох взаємопов'язаних елементів, які взаємодіють між собою. Зазвичай, оцінка ефективності КСЗІ здійснюється шляхом аналізу різноманітних критеріїв.

Процес визначення ефективності систем захисту розпочинається з вибору та обґрунтування показників або критеріїв, які використовуються для оцінки ефективності КСЗІ. Після цього переходять до розробки або вибору методик розрахунку цих показників, що дозволяють оцінити рівень захисту системи.

Істотна частина проблем забезпечення захисту такої інформації може бути вирішена відомими правовими та організаційними заходами, однак, враховуючи розвиток інформаційних технологій, наявна тенденція зростання необхідності застосування технічних заходів і засобів її захисту.

Організаційні заходи включають в себе створення концепції інформаційної безпеки, а також: складання посадових інструкцій для користувачів та обслуговуючого персоналу; створення правил адміністрування компонентів інформаційної системи, обліку, зберігання, знищення носіїв інформації, ідентифікації користувачів; розробка планів дій у разі виявлення спроб несанкціонованого доступу до інформаційних ресурсів системи, виходу з ладу засобів захисту, виникнення надзвичайної ситуації; навчання правилам інформаційної безпеки користувачів.

### *13.5 Виклики та завдання побудови системи забезпечення кібербезпеки в органах публічного управління.*

Комплексний (системний) підхід до побудови будь-якої системи містить в собі: перш за все, вивчення об'єкта впроваджуваної системи; оцінювання загроз безпеки об'єкта; аналіз засобів, якими будемо оперувати при побудові системи; оцінювання економічної доцільності; вивчення самої системи, її властивостей, принципів роботи та можливість збільшення її ефективності; співвідношення всіх внутрішніх і зовнішніх чинників; можливість додаткових змін в процесі побудови системи і повну організацію всього процесу від початку до кінця.

Основні завдання, які повинна вирішувати комплексна система захисту інформації включають: управління доступом користувачів до ресурсів інформаційної системи, забезпечення захисту від несанкціонованого доступу та втручання з боку сторонніх осіб, а також з обмеженням повноважень персоналу організації та користувачів та захист даних, які передаються по каналах зв'язку, щоб забезпечити конфіденційність і цілісність інформації; реєстрацію, збір, зберігання, обробку і видачу інформації про всі події, пов'язані з безпекою системи, для забезпечення контролю та аналізу потенційних загроз; контроль діяльності користувачів системи з боку адміністрації, а також оперативне сповіщення адміністратора безпеки про спроби несанкціонованого доступу. А також, забезпечення цілісності критичних ресурсів системи та перевірка середовища виконання прикладних програм з метою попередження можливих загроз безпеці; створення замкнутого середовища для перевіреного програмного забезпечення з метою захисту від шкідливих програм, вірусів та засобів обходу системи захисту; управління засобами комплексної системи захисту, що включає їх конфігурацію, моніторинг та аналіз ефективності.

Основними принципами організації КСЗІ є: системність; комплексність; безперервність захисту; розумна достатність; гнучкість управління і застосування; відкритість алгоритмів і механізмів захисту; простота застосування захисних заходів і засобів.

Забезпечення безпеки і захисту інформації стає надзвичайно важливим у сучасних умовах глобалізації та зростаючої конкуренції для організацій і державних підприємств України. Підхід до захисту інформації повинен бути системним і охоплювати всі аспекти процесу, від початкового проектування та розробки системи до експлуатації, підтримки та оновлення.

Стрімкий розвиток інформаційних технологій призводить до проблем захисту інформації, але комплексні системи захисту інформації (КСЗІ) допомагають у їх вирішенні. Ефективність КСЗІ залежить від взаємодії багатьох елементів, і оцінка їх ефективності вимагає вибору відповідних показників та методик розрахунку.

Законодавство України також регулює питання захисту інформації, вимагаючи застосування комплексної системи захисту з підтвердженою відповідністю для інформації з обмеженим доступом. Загалом, ефективність систем захисту інформації визначається ретельним аналізом, плануванням та впровадженням комплексу організаційних, технологічних і технічних заходів, які забезпечують надійний захист інформації в умовах зростаючих загроз та вимог сучасного світу.

## ПИТАННЯ ДЛЯ САМОПЕРЕВІРКИ

1. Якими є, на Вашу думку, особливості феномену інформаційної безпеки у сфері публічного управління?
2. Охарактеризуйте безпеку інформаційного простору в публічному управлінні.
3. Визначте заходи забезпечення ефективної діяльності системи публічного управління.
4. Що входить у діяльність органів та установ державного і публічного управління з питань захисту інформації?
5. Яким чином здійснюється організація системи захисту інформації у структурах державних органів та установ ?
6. Які виклики постали перед системою забезпечення кібербезпеки в органах публічного управління?
7. Обґрунтуйте завдання побудови системи забезпечення кібербезпеки в органах публічного управління на сучасному етапі.

# ЛЕКЦІЯ 14
# ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ В УМОВАХ РОСІЙСЬКОЇ ВІЙСЬКОВОЇ АГРЕСІЇ

**План викладу:**

14.1Проблеми забезпечення інформаційної безпеки держави в умовах воєнного стану.

14.2Характеристика і особливості реалізації функцій забезпечення інформаційної безпеки публічного адміністрування за умов дії правового режиму воєнного стану в Україні.

14.3Забезпечення стійкості України в умовах інформаційної війни: напрями й інструменти захисту українського інформаційного поля.

14.4Інформаційно-аналітична діяльність органів публічної влади в умовах російської агресії: механізми протидії методам гібридних атак.

14.5Стандарти захисту інформації в Україні під час дії воєнного стану.

## *14.1 Проблеми забезпечення інформаційної безпеки держави в умовах воєнного стану*

Нині розвиток інформаційних технологій охоплює багато сфер життя кожної людини. Не стало винятком використання інноваційних технологій у державних органах України. Реальними загрозами національним інтересам та національній безпеці України в інформаційній сфері є:

− проведення спеціальних інформаційних операцій, спрямованих на диверсію обороноздатності, деморалізацію особового складу Збройних сил України та інших військових формувань, провокування екстремістських проявів, панічні настрої, загострення та дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних та міжконфесійних конфліктів в Україні;

− недостатній розвиток національної інформаційної інфраструктури, що обмежує перспективи України ефективно протистояти інформаційній агресії та діяти активно в інформаційній сфері для реалізації національних інтересів нашої держави;

− неефективність державної інформаційної політики, недосконалість законодавства щодо регулювання суспільних відносин в інформаційній сфері, недостатній рівень медіакультури нашого суспільства;

− поширення звернень до радикальних дії, пропаганда ізоляціоністських та автономістських концепцій регіонального співіснування в Україні.

Аналізуючи сучасний стан інформаційної безпеки, слід підкреслити, що її рівень неповною мірою відповідає вимогам часу. Є проблеми, які серйозно заважають повній інформаційній безпеці людини, суспільства та держави. До основних проблем у цій сфері відносить такі як:

− відсутність чіткості під час проведення державної політики у сфері формування українського інформаційного простору;

− недостатня державна підтримка діяльності інформаційних агентств України із просування своєї продукції на зовнішній інформаційний ринок;

− відсутність ефективних механізмів захисту інформації;

− формування інноваційних інформаційних небезпек, які потребують негайного та ефективного вирішення;

− відсталість вітчизняних інформаційних технологій;

− непослідовність і нерозвиненість правового регулювання суспільних відносин у сфері інформації, що ускладнює дотримання необхідного балансу особистих, суспільних і державних інтересів у цій сфері;

– забезпечення підготовки якісних кадрів у системі державного управління у сфері інформаційної безпеки.

На сьогодні однією з головних проблем забезпечення інформаційної безпеки України є інформаційна експансія, необ'єктивне та неупереджене висвітлення фактів та явищ з боку російської федерації. Технології російських інформаційно-психологічних операцій налаштовані на забезпечення домінування в українському інформаційному просторі та на утримання медійної переваги. Через російські пропагандистські акції та медійні події відбувається вплив не лише на суспільну свідомість громадян України, а й на світову спільноту.

Так, російські військові хакери в кіберпросторі роблять те саме, що й їхні «колеги» на землі. Вони намагаються зруйнувати все, чого можуть досягти, створити хаос, дестабілізувати уряд, залякати населення, спричинити гуманітарну катастрофу та позбавити людей доступу до життєво важливих послуг. Тому атакують вони все: від органів влади та сектору безпеки й оборони – до локальних провайдерів і просто цивільних громадян. Критична інфраструктура піддається найбільшій атаці.

Останнім часом спостерігається надзвичайно велика кількість кібератак, спрямованих на гуманітарну катастрофу в Україні: атакується логістичний сектор, кілька днів не працюють сайти і державних органів.

Варто підкреслити, що на відміну від державних органів влади, органи місцевого самоврядування піддаються більшому ризику. Адже під загрозою є найважливіша інформація, яка належить місцевим органам. До такої інформації слід віднести: іпотечні документи, записи про минулі злочини, народження, смерть, медичне страхування, а також доступ до інформації про військовослужбовців та іншої конфіденційної інформації.

До основних причин, які негативно впливають на створення ефективної системи захисту інформації в органах місцевого самоврядування, відносять:

ігнорування місцевими органами нормативних вимог;

відсутність тісної взаємодії з іншими департаментами для забезпечення єдиної інфраструктури інформаційної безпеки в муніципалітеті;

несумлінне ставлення службовців, що призводить до зниження якості та безпеки;

відсутність бюджету для створення ефективної, працездатної програмної платформи;

призначення некваліфікованого службовця у сфері інформаційної безпеки.

В епоху інформаційного суспільства необхідно адаптуватися до всіх інновацій у сфері інформаційних технологій. І під час створення новітніх технологій розробляти засоби захисту від організацій, що становлять загрозу інформаційній безпеці.

### *14.2 Характеристика і особливості реалізації функцій забезпечення інформаційної безпеки публічного адміністрування за умов дії правового режиму воєнного стану в Україні*

Відносини у сфері забезпечення інформаційної безпеки органів публічного адміністрування мають публічно-правовий характер, оскільки пов'язані з виконанням державою своїх функцій, спрямованих на захист інформаційного суверенітету, забезпеченням інформаційних прав і свобод учасників правовідносин.

Визначимо, що функції забезпечення інформаційної безпеки публічного адміністрування в Україні – як притаманні діяльності публічних адміністрацій способи збереження власної функціональності за умов деструктивних інформаційних впливів і попередження спричинення шкоди (небезпеки) інформаційним правам та інтересам людини, громадянського суспільства, органів, підприємств, установ та організацій і держави в цілому.

На основі контентного аналізу діяльності публічних адміністрацій в інформаційній

сфері можна виокремити такі стадії реалізації функцій забезпечення інформаційної безпеки публічного адміністрування:

• стадія констатації та узагальнення призначена для визначення існуючих інформаційних загроз, накопичення інформації щодо них та виявлення спільних властивостей. Вказана стадія дозволяє від трансцендентного сприйняття інформаційних загроз перейти до їх аналізу, що базується на підтверджених фактах спричинення або спроби спричинення шкоди інформаційним правовідносинам.

• стадія аналізу дозволяє виявити і структурувати притаманні об'єкту закономірності, скласти ієрархію найбільш значущих з них, виявити періодичність, джерело, форми розповсюдження найбільш значущих інформаційних загроз, їхню мету, спрямованість та особливості керованості;

• стадія моделювання дає змогу визначити найбільш вразливі точки інформаційної діяльності противника щодо продукування інформаційних загроз і підготувати оптимальні засоби та способи її припинення або ослаблення (зниження ефективності);

• стадія нормативного закріплення передбачає прийняття управлінського рішення щодо включення оптимальних способів і засобів припинення інформаційної діяльності противника до актуальних завдань та комплексу оперативних дій публічної адміністрації й інших суб'єктів забезпечення інформаційної безпеки, а також закріплення вказаного рішення у відповідних нормативно-правових актах;

• стадія практичної реалізації функцій забезпечення інформаційної безпеки публічного адміністрування включає безпосереднє здійснення визначених у нормативно-правових актах завдань, дій і засобів для подолання інформаційних ризиків та загроз;

• стадія рефлексії та оцінювання дозволяє визначити ефективність діяльності на попередніх стадіях і скоригувати майбутню діяльність у сфері інформаційної безпеки для збільшення її ефективності.

Вказані стадії зазвичай реалізуються послідовно, проте не можна не згадати про випадки, коли внаслідок недоліків в організації та плануванні або через дефіцит часу, викликаного підвищеною небезпекою певної інформаційної загрози, певні стадії можуть бути пропущені. Слід вважати, що це сприяє збільшенню хаотичності у функціонуванні системи забезпечення інформаційної безпеки.

Функції забезпечення інформаційної безпеки публічного адміністрування можна класифікувати за різними критеріями, проте доцільнішою нам видається класифікація за критерієм результативності.

Функція збереження інформаційного суверенітету – це спроможність системи публічного адміністрування управляти процесами зовнішніх інформаційних впливів, даючи відсіч деструктивним інформаційним способам спричинити шкоду національній безпеці держави та інтересам громадянського суспільства.

Функція інформування міжнародного співтовариства щодо порушення противником законів і звичаїв війни, спричинення шкоди здоров'ю, життю та майну цивільного населення передбачає випередження руйнівного впливу фейків та інших способів спотворення об'єктивної інформації щодо ведення бойових дій та поводження з цивільними особами. Таке випередження досягається завдяки активній роботі публічних адміністрацій щодо оприлюднення на широкий міжнародний загал фактів, які характеризують дії противника.

Функція виховання високого рівня інформаційної культури обумовлює створення органами публічного адміністрування умов для найповнішого оволодіння їх персоналом, а також широкими верствами громадян знаннями, вміннями та навичками, які унеможливлюють вразливість системи публічного адміністрування та суспільства від інформаційних атак противника, у тому числі кібератак.

За умов повномасштабної збройної агресії російської федерації таке унеможливлення вразливості виступає однією із складових кібероборони – сукупності політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі і спрямовані на забезпечення захисту суверенітету й обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії.

Функція консолідації – це спрямованість зусиль публічних адміністрацій на створення загальнонаціонального консенсусу, що передбачає об'єднання різних суб'єктів забезпечення інформаційної безпеки на основі усвідомлення загальної мети, толерантності та взаємоповаги. З цього приводу хотілося б зробити деякі зауваження щодо розуміння сутності такої взаємодії у правовій та демократичній державі.

Людина і громадянин, окремі інститути громадянського суспільства проявляють свою активність у той момент і спосіб, які самі вважають доцільними (якщо така активність не порушує законодавчі приписи). Примушення до громадської активності в демократичному суспільстві неприпустиме, а отже, сутність функції консолідації включає збирання інформації щодо позицій недержавних суб'єктів забезпечення інформаційної безпеки та пошук спільних підстав сумісної з ними діяльності.

Таким чином, функції забезпечення інформаційної безпеки публічного адміністрування є одними з пріоритетних з-поміж інших функцій забезпечення національної безпеки. Відмінність реалізації означених функцій за умов повномасштабної збройної агресії російської федерації полягає в тому, що первинним на сьогодні є застосування кінетичної зброї. Однак можливість України вистояти та ефективно протистояти російській агресії значним чином залежить від вміння та вдалого застосування функції інформування міжнародного співтовариства щодо порушення противником законів і звичаїв війни, спричинення шкоди здоров'ю, життю та майну цивільного населення. Окрім того, зберігає свою актуальність функція виховання високого рівня інформаційної культури, що унеможливлює руйнівний вплив противника на життєдіяльність держави і громадянського суспільства.

### *14.3 Забезпечення стійкості України в умовах інформаційної війни: напрями й інструменти захисту українського інформаційного поля*

Серед напрямів інформаційної політики України, визначених у Законі України “Про інформацію”, на перше місце виходить забезпечення інформаційної безпеки держави. Від початку запровадження на території України воєнного стану державні органи в Україні прийняли низку документів, присвячених забезпеченню інформаційної безпеки. Так, зокрема, 12 березня 2022 року Кабінет Міністрів України видав Постанову № 263 “Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану”, в якому запропонував міністерствам, іншим центральним та місцевим органам виконавчої влади, державним та комунальним підприємствам, установам, організаціям, що належать до сфери їх управління, для забезпечення належного функціонування інформаційних, інформаційно-комунікаційних та електронних комунікаційних систем, публічних електронних реєстрів, володільцями (держателями) та/або адміністраторами яких вони є, та захисту інформації, що обробляється в них, а також захисту державних інформаційних ресурсів, можуть вжити додаткових заходів. При цьому Постановою передбачено заборону використання хмарних ресурсів та/або центрів обробки даних, розташованих на тимчасово окупованій території України, або тих, що належать державі, визнаній Верховною Радою України державою-агресором чи державою-окупантом, або належать державі чи суб’єктам,

діяльність яких підпадає під дію Закону України “Про санкції”, щодо яких прийнято рішення про застосування санкцій в Україні та/або іншій державі та на територіях держав, які входять до митних та воєнних союзів з такими державами.

Зазначаємо, що особливістю інформаційної системи в Україні стало те, що робота багатьох організацій, установ та підприємств, а також система освіти перейшли на віддалений режим роботи. Це відбулося ще до початку російської агресії проти України під впливом пандемії COVID-19 2019 – 2022 років. Ця вже налагоджена система дозволяє багатьом громадянам працювати дистанційно без відриву від їх основної діяльності навіть в умовах евакуації, а також збільшує цінність інформаційних мереж в Україні. Пошкодження цієї системи призведе до розірвання зв’язків, як всередині окремих організацій, так і між ними, тож нагальним завданням держави є недопущення такого сценарію.

В умовах війни на перше місце виходить підтримка цілісності інформаційної системи взагалі. Тобто заходи, спрямовані на захист від кібернетичних атак інформаційних систем державних органів, інформаційних систем, які містять національні інформаційні ресурси, комп’ютерних систем критичної інфраструктури, а також налагодження й забезпечення безперебійної роботи систем оповіщення населення щодо небезпеки (повітряні тривоги, артилерійські обстріли, необхідність евакуації у зв’язку з наближенням ворога, тощо).

І тут варто відзначити визначальну роль у доступі населення до критично важливої інформації під час війни, яку виконують офіційні інформаційні канали в соціальних мережах, а також українські державні сервіси, реалізовані у таких застосунках, як, зокрема, “Дія”, “Київ цифровий” та застосунках, призначених для миттєвого оповіщення населення щодо повітряної тривоги та доведення іншої необхідної інформації. Безумовно одним з важливих елементів інформування населення на сьогодні залишається телебачення.

Згідно із вже згаданим Законом України “Про інформацію”, в окремий напрям інформаційної політики нашої держави виділено створення умов для формування в Україні інформаційного суспільства. В умовах війни українське громадянське суспільство показало високий рівень самоорганізації, зокрема щодо протистояння ворогу в інформаційній сфері. Величезна кількість Телеграм та YouTube каналів, створених українцями, дозволяє забезпечувати громадян актуальною інформацією та швидко спростовувати ворожі фейки.

Зазначимо, що 18 березня 2022 р. було прийняте Рішення Ради національної безпеки і оборони “Щодо реалізації єдиної інформаційної політики в умовах воєнного стану” у якому було вирішено, що в умовах воєнного стану реалізація єдиної інформаційної політики є пріоритетним питанням національної безпеки, забезпечення якої реалізується шляхом об’єднання усіх загальнонаціональних телеканалів, програмне наповнення яких складається переважно з інформаційних та/або інформаційно-аналітичних передач на єдиній інформаційній платформі стратегічної комунікації – цілодобовому інформаційному марафоні “Єдині новини #UAразом”.

Наступний напрям інформаційної політики держави, згаданий у Законі України “Про інформацію”, – забезпечення відкритості та прозорості діяльності суб’єктів владних повноважень, попри нагальну необхідність нерозголошення і навіть втаємничення певної інформації про стан збройних сил та діяльність органів влади у воєнний період, проте цей напрям нікуди не зникає. Навпаки, постійне доведення громадськості чіткої та правдивої інформації щодо діяльності влади, заходів, які вона здійснює для організації оборони країни, протистояння агресору, налагодження економічних та соціальних зав’язків, мирного життя, тощо – є значним вкладом у співпрацю з громадянським суспільством.

Навіть за часів, коли йде війна, такі напрями інформаційної діяльності держави, як створення інформаційних систем і мереж інформації, розвиток електронного урядування та постійне оновлення, збагачення та зберігання національних інформаційних ресурсів

залишаються актуальними. Більше того, створюються державні інформаційні ресурси, яких у мирний час не існувало, зокрема ресурси, які акумулюють інформацію щодо військових злочинів країни-агресора, шкоди завданої громадянам України, а також держава будує зворотний зв'язок, через який громадяни можуть, наприклад залишити інформацію, щодо пересування військових частин ворога.

Останнім напрямом інформаційної політики, зазначеним у Законі України "Про інформацію" – є сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору.

Зазначимо, що можливість активного та успішного опору України військовій агресії РФ, окрім самого героїчного супротиву народу України, постала, зокрема, і завдяки значній економічній та військовій підтримці світового співтовариства. Україна змогла донести до світової громадськості своє бачення цієї війни і спростувати більшість наративів ворога, завдяки активній дипломатичній і безпрецедентній інформаційній роботі з іноземними ЗМІ, чіткого і правдивого висвітлення перебігу подій в Україні на всіх рівнях. Наслідком успішно проведеної роботи стала військова, економічна і соціальна допомога та надзвичайна моральна підтримка з боку громадянського суспільства світових демократичних країн.

Особливо хотілося б підкреслити необхідність взаємодії та узгодження дій, пов'язаних з формулюванням українських наративів всередині країни та на світовій арені з боку різних державних органів, а також у донесенні інформації до населення з питань, пов'язаних зі станом справ на фронті, необхідністю евакуюватися тощо. У цьому напряму головним має бути відсутність суперечностей у виступах різних спікерів від органів української влади, наявність обґрунтованих та ретельно продуманих меседжів, спрямованих на різні верстви населення всередині країни та на іноземну аудиторію – політиків і громадян, які можуть впливати на власну політичну еліту. Також важливо відслідковувати зміни настроїв як всередині країни, так і за кордоном, та вчасно реагувати на ці зміни.

### *14.4 Інформаційно-аналітична діяльність органів публічної влади в умовах російської агресії: механізми протидії методам гібридних атак*

Відповідно до офіційної позиції ЄС, гібридні загрози – це такі загрози, що впливають на вразливі місця та використовують їх, щоб завдати шкоди нижче порогу відкритої агресії. Вони являють собою суміш примусової та підривної діяльності, звичайних і нетрадиційних методів, які використовуються скоординовано в багатьох сферах. Авторитарні режими дедалі частіше намагаються підірвати спільні демократичні цінності і поляризувати суспільства для власних цілей, використовуючи різні типи гібридної діяльності, такі як маніпулювання інформацією, кібератаки, закон, економічний примус або інструменталізація мігрантів.

Прикладами є перешкоджання демократичним процесам прийняття рішень шляхом масових кампаній дезінформації, використання соціальних медіа для контролю над політичним наративом або для радикалізації, вербування та спрямування проксі-акторів.

Гібридні загрози можуть включати в себе різні елементи, такі як інформаційна війна, кібератаки, економічний тиск, підтримку нелегальних груп, дезінформацію та інші дії, що не обов'язково включають в себе військову агресію.

Говорячи про гібридні загрози варто водночас розуміти різницю між гібридною загрозою та гібридною війною. Хоча характер обох є однаковим, гібридна війна є більш масовим явищем, як у просторовому, так і часовому. Так, гібридні загрози можуть бути «одноразовими заходами», але вони в свою чергу можуть передувати вже більш активним діям. Окрім того, гібридна війна включає також військову агресію, тоді як загрози цілеспрямованої військової атаки не передбачають (але й не виключають терористичні акції, збройні провокації тощо).

Варто також наголосити, що розбудова міжнародної системи протидії гібридним загрозам відбулася вже на фоні військової агресії рф проти України у 2014 р., таким чином, український досвід, став передовим для побудови та законодавчого закріплення протидії відповідним загрозам з боку ймовірних агресорів. Разом з тим, країни ЄС та США більш оперативно оцінили власний потенціал та ступінь відповідних небезпек, нормативно закріпивши механізми протидії гібридним загрозам, саме тому використання подібного досвіду буде ефективним і для українського суспільства.

Відповідно до пункту 2 статей 8–11 Європейської конвенції з прав людини (ЄКПЛ), відповіді на гібридні загрози мають бути встановлені законом, переслідувати законну мету та бути необхідними для демократичного суспільства. У випадку широкомасштабних гібридних чи невійськових дій європейські держави завжди можуть застосувати на свою користь статтю 17 ЄКПЛ. Ця стаття забороняє зловживання правами і тісно пов'язана з принципом добросовісності в міжнародних відносинах. Подібним чином, у разі надзвичайного стану в державі, стаття 15 тієї ж конвенції дозволяє державам-учасницям призупинити виконання своїх зобов'язань згідно з ЄКПЛ, за винятком застосування права на життя, заборони тортур, рабства, смертної кари та подвійного покарання, а також принцип nulla poena sine lege («немає покарання без закону»).

З 2016 р. Європейська Комісія разом із Верховним представником ЄС із закордонних справ і політики безпеки запровадила широкий спектр заходів для протидії гібридним загрозам у значній кількості сфер політики за допомогою Спільної рамкової програми 2016 р. щодо протидії гібридним загрозам – «Спільна структура протидії гібридним загрозам – відповідь Європейського Союзу».

Взагалі, у Стратегії визначено 21 заходи для боротьби Європейського Союзу із гібридними загрозами. Більшість відповідальностей у цьому контексті покладено на Комісію, Верховного представника, а також на Центр для аналізу гібридних загроз «Hybrid Fusion Cell» ЄС (далі – HFC). Цей центр був створений в рамках Центру розвідки та ситуації ЄС (далі – EU INTCEN) та Європейської служби зовнішніх дій. HFC повинен отримувати, аналізувати і обмінюватися конфіденційною інформацією, а також інформацією з відкритим доступом, яка стосується показників і попереджень щодо гібридних загроз від різних зацікавлених сторін у EEAS, включаючи представництва ЄС, Комісії та агентства ЄС, а також від держав-членів.

Зі свого боку, Європейська Комісія повинна забезпечувати зв'язок з існуючими національними та європейськими органами. Цим документом пропонується державам-членам ЄС створити національні контактні пункти для оцінки гібридних загроз з метою співпраці та безпечного зв'язку з HFC ЄС. Документом було визначено, що для ефективної протидії гібридним загрозам необхідно звернути увагу на потенційну вразливість ключових інфраструктур, ланцюгів постачання та суспільства. Такими галузями були визнані:

- енергетика (диверсифікації джерел енергії та просування стандартів безпеки та безпеки для підвищення стійкості ядерної інфраструктури);
- безпека транспорту та мережі постачання (комплексно вирішувати проблеми безпеки на морі, включаючи протидію гібридним загрозам, шляхом міжгалузевої співпраці між цивільними та військовими особами для захисту критично важливої морської інфраструктури, глобального ланцюга поставок, морської торгівлі та морських природних та енергетичних ресурсів);
- космос (налагодження безперебійного супутникового зв'язку).

Окрім вищеозначеного, ЄС щороку робить звіт про хід виконання Спільної рамкової програми протидії гібридним загрозам та Спільного повідомлення щодо підвищення стійкості і зміцнення можливостей протидії гібридним загрозам. Зокрема важливою темою останнього звіту була гібридна політика кремля, їх атаки по дезінформації європейського

суспільства у зв'язку з розв'язаною рф війною проти України. В перспективі, подібні звіти мають стати традицією і для українського суспільства, але в умовах воєнного часу, на наш погляд це є недоречним, адже несе нові виклики системі національної безпеки.

Також важливо звернути увагу на Стратегію безпеки ЄС ухвалену у 2020 р. На відміну від двох попередніх стратегій, а саме «Безпечна Європа в кращому світі» (2003 р.) і «Сильніша Європа. Глобальна стратегія зовнішньої політики та політики безпеки Європейського Союзу» (2016 р.), в цій стратегії приділено значно більше уваги гібридним загрозам. Зокрема, з чотирьох розділів Стратегії, частина друга під назвою «Боротьба з загрозами, що розвиваються» була приурочена саме гібридним загрозам. Комісія та Високий представник у цій Стратегії висвітлили підхід ЄС до гібридних загроз, який об'єднує зовнішній і внутрішній аспекти у безперервний процес.

Цей підхід охоплює широкий спектр заходів – від раннього виявлення, аналізу, інформування, підвищення стійкості та запобігання до кризового реагування та управління наслідками. Також передбачає подальше посилення співпраці у сфері розвідування з компетентними службами держав-членів через EU INTCEN, оптимізацію потоків інформації з різних джерел у країнах-членах та агентствах ЄС (ENISA, Європол, Frontex, Комісія, HFC) та забезпечення безперебійної співпраці між ЄС і НАТО.

Відповідно до Стратегії 2020 HFC і надалі виконує центральну координуючу роль у попередженні гібридних загроз; проводить аналіз гібридних та кіберзагроз з усіх джерел на основі розвідки у тісній співпраці з Управлінням розвідки Військового штабу ЄС (надає письмові оцінки та організовує брифінги; продовжує організовувати два рази на рік зустрічі своєї мережі національних контактних пунктів для протидії гібридним загрозам; підтримує тісну співпрацю з Відділом аналізу гібридних загроз НАТО та Центром передового досвіду з протидії гібридним загрозам. Тоді як ЄС активно займається у сфері протидії гібридним загрозам та їх досвід буде досить важливим для України, то стратегії ООН є менш вдалими.

Загалом відзначити, що міжнародне право (а власне певні міжнародні організації) закріплюють поступово шляхи боротьби з гібридними загрозами, розуміючи, що у сучасному динамічному світі вони є невід'ємною складовою як відкритої, так і тіньової боротьби. Україна намагається активно використовувати юридичну площину у боротьбі із загрозами, зокрема це було продемонстровано зверненнями до міжнародних судів. Водночас, політика санкцій, яка наразі є найбільш активним засобом міжнародного сприяння у боротьби із гібридними загрозами, активно застосовується у боротьбі проти російського агресора. Міжнародні спільноти, включаючи Європейський Союз і ООН, вживають різноманітні санкційні заходи проти РФ з метою вплинути на її поведінку та змінити агресивну політику.

Держави, що застосовують гібридні методи атак, використовують невизначеність міжнародного права у відповідних сферах, тим самим виправдовуючи свої дії тим, що жодного порушення норм не відбулося. Водночас, сьогодні світова спільнота прагне локалізувати відповідний вакуум нормативно-правової сфери, окресливши міжнародні загрози та сфери протидії ним.

### *14.5 Стандарти захисту персональних даних в Україні під час дії воєнного стану*

За атрибуцією абсолютна більшість кіберінцидентів пов'язана з хакерськими угрупуваннями, що фінансуються урядом рф. Важливою умовою правомірної обробки персональних даних у період дії правового режиму воєнного стану є забезпечення громадянам належного рівня захисту їхніх прав, пов'язаних із персональними даними. Після набрання чинності регламентом Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист

даних) (далі – Регламент) (zakon.rada.gov.ua/laws/show/984_008-16#Text) чимало компаній зіткнулися з проблемою адаптації політики приватності до нових вимог у сфері захисту персональних даних.

Ключові вимоги до змісту політики приватності містяться у статтях 13 і 14 Регламенту. Основна помилка при складенні політики приватності – це розпорошення інформації про окрему обробку персональних даних серед різних розділів, коли укладачі описують категорії оброблюваних даних окремо від цілей, а цілі – окремо від правових підстав обробки (згода, інтерес, вимога закону тощо). Якщо проведений аналіз щодо персональних даних буде бездоганним, а людина залишається неуважною, це надасть іншим суб'єктам можливість соціального контролю.

В Україні діє Закон України «Про захист персональних даних», який має на меті захист прав і свобод громадян України від неправомірного використання їхніх персональних даних. Закон встановлює правила збору, зберігання, обробки та передачі персональних даних, а також відповідальність за їх неправомірне використання. Однак Європейський Союз має більш суворі вимоги до захисту персональних даних. Зокрема, в ЄС було прийнято Загальний регламент про захист персональних даних, який набрав чинності 25 травня 2018 року. Цей Регламент встановлює єдині правила збору, зберігання, обробки та передачі персональних даних в ЄС, а також відповідальність за порушення правил їх захисту, за що можуть бути накладені великі штрафи аж до 20 млн євро, або 4 % річного обороту компанії.

Щодо відмінностей між принципами захисту персональних даних в Європейському Союзі та Україні, то можна зауважити, що Регламент передбачає більш суворий контроль за захистом персональних даних, враховуючи необхідність отримання згоди на їх збір та обробку. Крім того, GDPR вимагає від компаній проводити оцінку впливу на захист персональних даних та повідомляти про порушення правил захисту персональних даних протягом 72 годин.

Стандарти з кібербезпеки не тільки встановлюють загальні принципи та вимоги до кібербезпеки, які потім можуть бути відтворені або адаптовані національними законами та правилами, але й визначають найкращі практики та рекомендації. Окрім міжнародних стандартів, розроблених фахівцями ISO, існує перелік міжнародних стандартів з кібербезпеки, розроблених фахівцями Британського інституту стандартів (BSI). До речі, у Великій Британії вони описані як класична модель системно-інституційної відповідності (Systemic-Institutional Alignment – SIA), що слугує забезпеченню вимог щодо конфіденційності, цілісності та доступності інформації. Окремо винесено вимогу спостережливості (підзвітності). Вимога конфіденційності застосовується до інформації, всі інші - як до інформації, так і до системи в цілому.

Міжнародна стандартизація складових системи управління інформаційною безпекою формує три напрямки розвитку в цій сфері:

група стандартів: «Методи забезпечення безпеки» - ISO/IEC 27000-ISO/IEC 27037;

група стандартів «Методи та засоби забезпечення безпеки» - ISO/IEC 15408 (загальні критерії, три частини), ISO/IEC 13335 (п'ять частин) та ISO/IEC 18045;

група стандартів з управління та аудиту інформаційних технологій (CobIT, ITSM, ITIL та ін.).

Так, відповідно до реферативного огляду міжнародних стандартів у сфері інформаційної безпеки групи ISO 27000, то вони визначають технічні та організаційні вимоги до механізму управління інформаційною безпекою, включно з кібербезпекою, демонструють кращі практики протидії ризикам у відповідній сфері. Зазначена група стандартів також охоплює методи протидії кіберризикам, порушенням конфіденційності інформації, закріплює засоби технічного захисту інформації з урахуванням правових режимів і сфери поширення

інформації. Наприклад, стандарт ISO/IEC 27001 дає організаціям можливість створити систему управління інформаційною безпекою та застосувати процес управління ризиками, який можна адаптувати та масштабувати відповідно до розвитку організації.

Крім того, з 22 серпня 2023 року набрали чинності національні стандарти, гармонізовані з міжнародними стандартами (стосовно інформаційних систем, керування ними, кібербезпеки та захисту конфіденційності, критеріїв оцінювання безпеки IT тощо), а також прийнято зміни до національного стандарту ДСТУ ISO/IEC 29146:2023 (ISO/IEC 29146:2016)/Зміна № 1:2023 (ISO/IEC 29146:2016/Amd 1:2022, IDT) «Інформаційні технології. Методи безпеки. Структура керування доступом» та скасовано чинність низки національних стандартів, гармонізованих з міжнародним стандартом.

Міжнародні стандарти та рекомендації можуть стати базою для розробки внутрішньої політики безпеки даних та захисних заходів. Такі стандарти дозволяють гарантувати високий рівень безпеки даних та підвищують довіру клієнтів і споживачів до організації.

**ПИТАННЯ ДЛЯ САМОПЕРЕВІРКИ**

1. Визначте проблеми забезпечення інформаційної безпеки держави в умовах воєнного стану.
2. Охарактеризуйте особливості реалізації функцій забезпечення інформаційної безпеки публічного адміністрування за умов дії правового режиму воєнного стану в Україні.
3. Яким чином можна забезпечити стійкість України в умовах інформаційної війни?
4. Вкажіть напрями й інструменти захисту українського інформаційного поля.
5. Які механізми протидії методам гібридних атак Ви знаєте? Охарактеризуйте їх коротко.
6. Окресліть інформаційно-аналітичну діяльність органів публічної влади в умовах російської агресії.
7. Які напрямки розвитку формує Міжнародна стандартизація складових системи управління інформаційною безпекою?
8. На Вашу думку, які саме стандарти захисту інформації треба запровадити в Україні під час дії воєнного стану?

# ЛЕКЦІЯ 15
# АДАПТАЦІЯ МІЖНАРОДНОГО ДОСВІДУ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

**План викладу:**

15.1 Інструменти, інститути та правова основа забезпечення інформаційної безпеки Європейського Союзу.

15.2 Забезпечення інформаційної безпеки у США.

15.3 Азійська модель забезпечення інформаційної безпеки.

15.4 Кібернетична безпека та поширення засобів інформаційного впливу: зарубіжний досвід.

14.1Інформаційна безпека України в умовах євроінтеграції

## *15.1 Інструменти, інститути та правова основа забезпечення інформаційної безпеки Європейського Союзу*

Моделі інформаційної безпеки європейських країн засновуються на відповідному законодавстві Європейського Союзу та національному законодавстві держав-учасниць.

Головні акти ЄС у сфері захисту інформаційного простору:

Закон ЄС «Про ENISA (Агентство Європейського Союзу з питань кібербезпеки) та про сертифікацію кібербезпеки інформаційних та комунікаційних технологій та скасування Регламенту (ЄС) № 526/2013 (Закон про кібербезпеку)» від 17.04.2019 р. (Закон «Про ENISA та сертифікацію»),

Директива про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу (Директива NIS) від 06.07.2016 р.,

Регламент (ЄС) 2016/679 Європейського парламенту і Ради від 27 квітня 2016 року про захист фізичних осіб стосовно обробки персональних даних та про вільне переміщення таких даних і скасування Директиви 95/46 / ЕС (Загальні положення про захист даних) (англ. General Data Protection Regulation, GDPR) та ін.

Закон ЄС «Про ENISA та сертифікацію» прийнятий Європейським парламентом 12 березня 2019 року, а потім Радою Європейського Союзу 7 червня 2019 року, знаменує собою крок уперед для європейської стратегічної автономії. Він переслідує подвійну мету: прийняття постійного мандата ENISA – Європейського агентства з кібербезпеки та визначення Європейської основи сертифікації у сфері кібербезпеки, що має важливе значення для підвищення безпеки Європейського єдиного цифрового простору.

Закон ЄС «Про ENISA та сертифікацію» також вводить європейські рамки сертифікації кібербезпеки як засіб створення європейських схем сертифікації кібербезпеки для продуктів, послуг і процесів інформаційно-комунікаційних технологій. Закон про кібербезпеку надає Комісії право приймати європейські схеми сертифікації кібербезпеки. Європейська комісія опублікує «Профспілкову робочу програму», в якій будуть визначені стратегічні пріоритети європейських схем сертифікації кібербезпеки, щоб допомогти промисловості, національним органам і органам по стандартизації підготуватися до таких режимів сертифікації.

Директива NIS спрямована на створення сильної та надійної Європи, яка ґрунтується на національних можливостях держав–членів у сфері кібербезпеки, створенні ефективних і дієвих механізмів захисту найважливіших економічних і соціальних інтересів нації, щоб колективно протистояти ризикам кібератак. Вона визначає правила безпеки в таких критично важливих сферах: енергетиці, охороні здоров’я, транспорті, банківській діяльності та інфраструктурі, фінансовому ринку, цифровій інфраструктурі, а також вимоги безпеки у сферах онлайн-послуг (пошукових систем, хмарних технологій, торгових майданчиків тощо).

Регламент (ЄС) 2016/679 Європейського парламенту і Ради від 27 квітня 2016 року про захист фізичних осіб стосовно оброблення персональних даних та про вільне переміщення таких даних і скасування Директиви 95/46 / ЄС (Загальні положення про захист даних, GDPR) покликаний підсилити та уніфікувати захист персональних даних усіх осіб в ЄС. Регламент також направлено на експорт даних з ЄС.

Розглянемо детальніше моделі інформаційної безпеки Франції та Німеччини.

Правовою основою забезпечення інформаційної безпеки Франції виступає Конституція, національне та європейське законодавство. Слід зазначити, що питання інформаційної безпеки держави та людини, у Конституції Французької Республіки не врегульовані, міститься лише бланкетна норма щодо встановлення законами правил користування громадянськими правами та публічними свободами, серед яких право на інформацію, плюралізм та свобода ЗМІ тощо. Система інформаційної безпеки Франції є складовою національної безпеки, і основні її принципи закладені у Білих книгах оборони та національної безпеки. В Оборонному огляді значна увага приділяється інформаційним загрозам та заходам протидії ним. Так, зазначається, що у кіберпросторі деякі напади, зумовлені їх масштабами та серйозністю, можуть бути віднесені до категорії збройної агресії. Труднощі з розподілом акцій і поєднання прямих дій з методами впливу і пропаганди уможливлюють безліч сценаріїв інструменталізації з метою дестабілізації або підтримки простіших операцій.

Сьогодні чинним є Закон Франції «Про військове планування на період з 2019 до 2025 року та інші положення, що стосуються оборони» № 2018-607 від 13.07.2018 р. Для Франції серйозною загрозою її інформаційному простору залишається так званий «кіберджихадизм», який полягає у застосуванні інтернет-технологій та послуг, особливо соціальних мереж в просуванні джихадизм – насильства. Він здійснюється шляхом злому урядових сайтів, корпоративних сайтів або організацій, пропаганди та вербування. Заходами протидії ньому виступають блокування сайтів та акаунтів, створення контрпропагандистських сайтів тощо.

Важливою складовою інформаційної безпеки є регулювання цифрового простору. Зокрема у Франції усвідомлення мережі Інтернет як джерела ризиків та загроз національній безпеці держави відбувалося поступово і було зумовлено зростанням залежності від інформаційно-технологічних процесів та все ширшим використанням цифрових технологій у найважливіших сферах французького суспільства і держави.

У 2015 році Франція прийняла Національну стратегію цифрової безпеки. Розроблена для підтримки цифрового переходу французького суспільства, вона відповідає новим викликам, що виникають в результаті еволюції цифрового використання і пов’язаних з ним загроз. У ній визначено п’ять напрямів діяльності: гарантувати національний суверенітет; забезпечувати рішучу відповідь проти актів кіберзлочинності; інформувати громадськість; зробити цифрову безпеку конкурентною перевагою для французьких компаній; зміцнити голос Франції на міжнародному рівні.

Німецька модель забезпечення інформаційної безпеки держави діє на підставі Конституції ФРН, федеральних законів та законів земель, рішень конституційних судів, наднаціонального законодавства та відповідних підзаконних нормативно-правових актах. Так, відповідно до параграфа 1 статті 5 Конституції ФРН кожен має право на свободу вираження і поширювання своєї думки усно, письмово і за допомогою образотворчих засобів, безперешкодно отримувати інформацію з усіх загальнодоступних джерел. Гарантується свобода друку і свобода передавання інформації за допомогою радіо й кіно. Цензура не здійснюється.

Головним суб’єктом системи забезпечення інформаційної безпеки німецької держави виступає Федеральне відомство з безпеки в сфері інформаційних технологій (BSI). Це цивільний орган влади у структурі Федерального міністерства внутрішніх справ Німеччини, який відповідає за питання безпеки ІТ. Зазначене відомство як національний орган з кібербезпеки розроблює інформаційну безпеку у цифровому просторі шляхом запобігання, виявлення та реакції для держави, економіки та суспільства. Повноваження та засади діяльності BSI визначаються Законом про Федеральне відомство з інформаційної безпеки (нім. Act BSI) від 1991 р. Метою відомства є профілактичне посилення інформаційної та кібербезпеки з метою полегшення і просування безпечного використання інформаційних та комунікаційних технологій у державі, бізнесі та суспільстві.

Федеральне відомство з безпеки в сфері інформаційних технологій контролює діяльність Національного центру кіберзахисту (далі – Cyber-AZ), який був запущений 1 квітня 2011 року. Cyber-AZ є міжвідомчим органом німецької влади на федеральному рівні, метою якого є запобігання електронним атакам на ІТ-інфраструктуру у ФРН та її економіку.

Федеральний уряд також надає фінансову підтримку та інформаційні продукти для виготовлення, ліцензування й поширення таких програм в інших регіонах світу. На

військовому рівні забезпечення інформаційної безпеки Німеччини здійснюється Федеральними збройними силами Німеччини (Бундесвером), зокрема відділом інформаційних та комп'ютерних мережевих операцій командування стратегічної розвідки.

Отже, система забезпечення інформаційної безпеки Франції та Німеччини ґрунтується на усвідомленні ризиків і загроз, які зумовлюються швидким розвитком інформаційних та комунікаційних технологій. Тому політика цих країни у вказаній сфері є послідовною, засновується на компетентних оцінках та стратегіях, спрямована на професійну підготовку кадрів та розвиток технологій.

Так, одним з головних суб'єктів системи забезпечення інформаційної безпеки Франції виступає Національне агентство безпеки інформаційних систем, а у Німеччині – Федеральне відомство з безпеки у сфері інформаційних технологій та відділ інформаційних та комп'ютерних мережевих операцій командування стратегічної розвідки Бундесверу. Основними тенденціями в роботі цих суб'єктів є збільшення бюджету, розширення штату, технологічне лідерство та міжнародне співробітництво.

### *15.2 Забезпечення інформаційної безпеки у США*

Загалом державна політика США у сфері інформаційної безпеки пройшла значний еволюційний шлях. Так, він складається з чотирьох етапів:

– виникнення (1939–1947 рр.);
– становлення (1947–1982 рр.);
– активний розвиток (1983–2001 рр.);
– докорінне вдосконалення (2001 р. – дотепер).

З приходом у 1981 р. до влади президента США Р. Рейгана та його адміністрації управління інформаційними ресурсами, відповідно із «Законом про свободу інформації», напрям інформаційної безпеки був визначений як пріоритетний в урядовій політиці. Ще 1992 р. у США прийнято програми «Національна інформаційна політика» та «Глобальна інформаційна політика» (GII). Військово-політичне керівництво США з початку 90-х років приділяло значну увагу розвитку інформаційних технологій, високо оцінюючи їх потенційні можливості для досягнення військової переваги.

Саме про це стверджується у директиві МО США TS 1992 р. «Інформаційна війна». Так, було зазначено на необхідності всебічного обліку інформаційних ресурсів при організації планування і функціонування систем управління в інтересах підвищення ефективності дії своїх військ в умовах протидії супротивника.

Складовими концепта «інформаційна війна» стало: оперативна безпека, введення супротивника в оману, психологічні операції, електронна війна і вогневе знищення, які проводяться в комплексі з глибокою і всебічною розвідкою як для дезорганізації системи управління противника, так і для захисту власної системи управління в ході бойових дій.

Для Пентагону, який використовує кількасот різних інформаційних систем і мереж, питання інформаційної безпеки фактично прирівнюється до питань військової безпеки. Інформаційні військові дії проводяться для досягнення інформаційної переваги в інтересах національної військової стратегії і здійснюються шляхом впливу на інформацію та інформаційні системи противника при одночасному захисті власної інформації і своїх інформаційних систем.

За 1997–2001 роки на законодавчому рівні у сфері інформаційної безпеки США було зроблено чимало: пом'якшено експортні обмеження на криптографічні продукти, сформовано інфраструктуру з відкритими ключами, розроблено ряд стандартів про електронний цифровий підпис – FIPS 186-2 (2000 р.). На базі цих актів у США сформовано загальнонаціональну інфраструктуру електронної аутентифікації. Окрім цього, в законодавстві США прийнято директиви, спрямовані на захист інтересів АНБ, ФБР, ЦРУ, Міністерства оборони.

У США на офіційному рівні визнають, що контроль над секретними комунікаціями противника при одночасному захисті своїх власних надає їм унікальні можливості для збереження лідируючих позицій у світі. Б. Обама оголосив цифрову інфраструктуру США стратегічною національною цінністю, а захист цієї інфраструктури – національним пріоритетом. У 2010 р. з метою реалізації захисту держави та уряду від кібератак та хакерів президент США затвердив «Ініціативу зі всеосяжної національної кібербезпеки» Ради

національної безпеки США, яка містить дванадцять загальних положень. Ця ініціатива є складовою частиною розділу Військової доктрини США, що стосується кібернетичної оборони.

Документом передбачено створення єдиної федеральної мережі, пов'язаної захищеними каналами зв'язку, який у свою чергу, має здійснюватися через контрольовані точки доступу. Крім того, ініціатива передбачає об'єднання всіх наявних у США центрів оперативного реагування на кіберзлочини з метою підвищення ефективності їх діяльності та проведення більш глибокого аналізу щодо хакерських атак. Також з метою протидії іноземним кібершпигунам документом передбачено створення підрозділів кіберконтррозвідки в державних органах США, зокрема для захисту секретних внутрішніх мереж Міністерства оборони США від терористичних атак.

Передбачено також створення системи управління ризиками для прогнозування наслідків зламу систем, викрадення або пошкодження інформації та мінімізації збитків від таких протиправних втручань. Отже, як можна зрозуміти, держава бере участь у захисті ключових приватних інфраструктурних мереж (телекомунікації, електромережі, мережі банківських розрахунків, інтернет-провайдери).

Загалом система нормативного регулювання інформаційної безпеки США, насамперед федеральне законодавство, у цій сфері включає чотири основні напрями: інформаційна безпека держави; захист даних фінансових установ; безпека інформації організацій охорони здоров'я; діяльність правоохоронних органів по збиранню інформації.

Відповідно, основними законами у вказаних напрямах є: Федеральний закон «Про управління інформаційною безпекою» від 2014 (FISMA), Федеральний закон Грема-Ліча-Блілі від 1999 р., Федеральний закон «Про мобільність та підзвітність медичного страхування» від 1996 р., «Акт патріота» від 2001 р., Федеральний закон «Про обмін інформацією про кіберзагрози» від 2015 р. Федеральний закон «Про управління інформаційною безпекою» (FISMA).

Політика США у сфері захисту інформаційного простору та ведення інформаційних війн здійснюється шляхом розроблення та реалізації національних стратегій, державних військових програм та доктрин. Сполучені Штати Америки одні з перших усвідомили стратегічну важливість забезпечення безпеки кіберпростору. Розвиток інформаційної сфери, збільшення її ролі у житті суспільства і держави та пов'язане з цим збільшенням загроз в економіці, яка все більше залежала від інформаційно-комунікаційних технологій, а також терористичні акти 2001 р. стали причиною прийняття Національної стратегії захисту кіберпростору 2003 р.

Сприяння розвитку і захист американських винаходів та інновацій має вирішальне значення для забезпечення стратегічної переваги США в кіберпросторі. Однією з цілей є забезпечення лідерства Сполучених Штатів у сфері нових технологій і сприяння виявленню та забезпечення підтримки цих технологій з боку уряду, включаючи штучний інтелект, квантову інформатику й телекомунікаційну інфраструктуру наступного покоління.

Кіберстратегія США від 2018 р. орієнтована на збереження лідерства, посилення впливу і просування інтересів США на міжнародній арені. Безпека кіберпростору США виступає складовою їх національної безпеки, що підтверджується кореляцією напрямів однойменних стратегій. Розвиток та стійкість цифрової економіки розглядається як основа американського процвітання. Важливо, що саме висококваліфіковані кадри у сфері забезпечення кібербезпеки визнаються стратегічною перевагою для національної безпеки США, тому пошук молодих талантів та спеціалістів здійснює уряд по всьому світу в межах різноманітних державних програм.

### *15.3 Азійська модель забезпечення інформаційної безпеки сучасних держав*

Китайська модель забезпечення інформаційної безпеки засновується на тотальному контролі державою її інформаційного простору, що суперечить європейським практикам у цій сфері, і, відповідно, вважається негативним прикладом інформаційної державної політики. У Конституції КНР від 04.12.1982 р. (у редакції 2018 р.) немає поняття «інформаційна безпека» та «інформація», але декларується свобода слова та право на таємницю листування.

Головним актом у сфері інформаційної безпеки КНР є Закон про кібербезпеку

Китайської Народної Республіки, який був прийнятий Постійним комітетом Всекитайських зборів народних представників 07.11.2016 р. і набрав чинності 01.06.2017 р. (Закон про кібербезпеку КНР).

Цей закон знаходиться на вершині пірамідального законодавства про кібербезпеку. Він є еволюцію існуючих раніше правил і норм з кібербезпеки з різних рівнів і сфер, асимілюючи їх для створення структурованого закону на макрорівні. Закон також пропонує основні норми з певних питань, які не є невідкладними, але мають довгострокове значення. Закон про кібербезпеку КНР закріплює:

– вимоги безпеки інтернет-провайдерів, продуктів і послуг;

– правила захисту персональної інформації;

– принцип суверенітету кіберпростору;

– правила транснаціональної передачі даних в критично важливій інформаційній інфраструктурі;

– систему безпеки для ключової інформаційної інфраструктури.

Державний контроль і цензура запроваджені і в китайському онлайн просторі. Це зумовлено насамперед тим, що в Китаї найбільша кількість інтернет-користувачів у світі – 802 млн користувачів і 42% світових транзакцій електронної торгівлі надходять з цієї країни.

У зв'язку з цим у КНР реалізується проект «Золотий щит» (англ. The Golden Shield Project), який ще називають Великий китайський фаєрвол, програма фільтрації інтернетконтенту в КНР. Цей проект був запущений у 2003 році. Його програма охоплює такі напрями, як система управління трафіком, система інформування про правопорушення, система управління безпекою, інформаційна система моніторингу, система контролю виходу і введення. «Золотий щит» є одним з 12 ключових проектів КНР у сфері електронного уряду, іменованих «золотими».

Іншими «золотими» проектами є: «Золота митниця» (для іноземних торгів), «Золоті мости» (для загальноекономічної інформації), «Золоті фінанси» (для управління фінансами), «Золота картка» (для електронних валют), «Золота вода» (для інформації про водні ресурси), «Золоте сільське господарство» (для сільськогосподарської інформації) «Золота якість» (для контролю якості), «Золоте оподаткування » (для оподаткування) і т. д.

Проект «Золотий щит» передбачає обмеження доступу до низки іноземних сайтів, веб-сторінки фільтруються по кодовим словам, пов'язаним з національною безпекою та чорним списком сайтів.

Сайти, які розміщені в Китаї, повинні проходити реєстрацію у Міністерстві промисловості та інформаційних технологій. Крім того, в Китаї діє армія блогерів, які за винагороду позитивно висловлюються в чатах, блогах і на форумах про державну політику Китаю.

### *15.4 Кібернетична безпека та поширення засобів інформаційного впливу: зарубіжний досвід*

Кібербезпека це 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 у кіберпросторі. Кіберрозвідка визначається як діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням.

Для виявлення взаємозв'язку між цими сутностями Фондом академії електронного врядування Естонії розроблено і реалізується Національний індекс кібербезпеки (NCSI), а Глобальний індекс кібербезпеки (GCI) укладає Міжнародний союз електрозв'язку (MCE), він є ініціативою для зацікавлених сторін, спрямованою на підвищення обізнаності щодо кібербезпеки та вимірювання прихильності країн до кібербезпеки та її широкого застосування в різних галузях і секторах. Рівень розвитку кібербезпеки кожної країни аналізується за п'ятьма категоріями: правові заходи, технічні заходи, організаційні заходи, розбудова

потенціалу та співробітництво. Зазначені індекси є комплексними показниками, що оцінюють рівень кібербезпеки країн і є тісно пов'язаними з розвідкою кіберзагроз, оскільки кіберрозвідка є невід'ємною частиною загальної стратегії забезпечення кібербезпеки.

Структура кіберрозвідки країн-членів НАТО є складною та багаторівневою, оскільки кожна країна має власні організації та підрозділи, відповідальні за кібербезпеку та кіберрозвідку. Проте, існують загальні риси та спільні структури, які забезпечують координацію між країнами-членами. Основні компоненти кіберрозвідки країн НАТО включають національні кіберрозвідувальні агентства, військові підрозділи, а також міжнародні організації НАТО, які сприяють співпраці та обміну інформацією.

Структура кіберрозвідки та розвідки з кіберзагроз країн-членів НАТО є гнучкою та децентралізованою, що дозволяє кожній країні розробляти власні підходи до кібербезпеки, одночасно співпрацюючи в рамках НАТО для забезпечення загального захисту від кіберзагроз. Слід зазначити, що для забезпечення ефективності кіберрозвідки необхідне стабільне та достатнє фінансування, оскільки така діяльність потребує відповідного апаратного забезпечення, спеціалізованого програмного забезпечення, підтримки та постійного удосконалення системи моніторингу та аналізу даних, залучення та мотивації висококваліфікованих фахівців з кібербезпеки, аналітиків даних та інженерів програмного забезпечення тощо. Постійний розвиток технологій вимагає від фахівців з кіберрозвідки постійного професійного навчання та підвищення кваліфікації. Також, відповідного фінансування вимагає проведення операцій з кіберрозвідки, включаючи витрати на зв'язок, ліцензії, підписки на інформаційні ресурси, інвестування у нові технології та методи захисту та атаки, що є необхідним для випередження кіберзлочинців.

Розглядаючи міжнародний досвід боротьби з кіберзлочинами в різних регіонах, варто розглянути й Японію, яка є лідером в інноваційних технологіях, робототехніці та комп’ютерних тенденціях. Відзначимо, для цієї країни питання кібербезпеки є одним з перспективних напрямків діяльності. Так, зокрема, з 2013 року головна роль у боротьбі з кіберзлочинами зосереджена в Раді з питань інформаційної безпеки Японії. Цей державний орган є також одним з основних законодавчих суб’єктів: самостійно видає нормативно-правові акти з протидії кіберзлочинності, також аналізує, редагує і проводить експертизу подібних документів інших суб’єктів законодавчого процесу.

Основним документом, що передбачає санкції, є Кримінальний кодекс Японії. Варто відмітити досить суворі покарання за суспільно не-безпечні протиправні дії. Наприклад, за «фальсифікацію комп’ютерних даних» передбачено кримінальну відповідальність у вигляді позбавлення волі строком на 10 років.Слід акцентувати увагу й на Законі про заборону незаконного доступу (офіційна назва «Закон про заборону незаконного доступу та інше») був прийнятий у лютому 2012 року. Цей закон, що складається з 14 статей, має на меті запобігти кіберзлочинам та підтримувати порядок у сфері електронних комунікацій. Згідно статті 1, метою цього закону є «запобігання злочинам, пов’язаним з комп’ютерами, через телекомунікаційні лінії, а також підтримка порядку в телекомунікаціях, які здійснюються за допомогою функцій контролю доступу, шляхом заборони незаконного доступу, встановлення кримінальних покарань за це та заходів допомоги від комісії з громадської безпеки префектур для запобігання повторенню таких дій, та тим самим сприяти здоровому розвитку високоінформаційного суспільства». При цьому, Закон про заборону незаконного доступу не лише визначає незаконні дії доступу та покарання за них, але й накладає обов’язки на адіністраторів для запобігання незаконному досту-пу до серверів та інших систем. Незважаючи на це, слід відмітити, з 2018 року в Японії практично удвічі зросла кількість що вірогідною причиною зростання кількості атак є збільшення числа можливих цілей, таких як під’єднана до Інтернету домашня техніка. 7 липня 2022 року набула чинності поправ-ка до

Кримінального кодексу Японії, відповідно до якої за образу людини в інтернеті можна потрапити до в'язниці. Віднині за кіберзалякування можна отримати тюремний термін до одного року або штраф до 300 000 єн (2200 доларів). Раніше цей злочин карався тюремним терміном до 30 днів або штрафом до 10 000 єн (менше за 74 долари). Також збільшено термін давності за образи з одного року до трьох років.

Що стосується практики застосування законодавства про кіберзлочини в Японії, відзначимо, якщо особа стає жертвою кіберзлочину та повідомляє ро це в поліцію, зазвичай очікується, що поліція проведе розслідування, встановить винуватця та приступить до арештів та притягнення до відповідальності. Це «звичайне уявлення громадянина». Однак, на жаль, в Японії, коли мова йде, зокрема, про економічні злочини, які не пов'язані з загрозами життю або фізичному здоров'ю, особливо у випадку кіберзлочинів, практичні ресурси поліції для розслідування є обмеженими. Без ретельного розслідування та створення обширної документації з боку жертви, такої як «звіти про інциденти», важко ефективно стимулювати поліцейські роз-слідування навіть для високотехнологічної Японії.

Також, на наш погляд, вартим уваги є факт, що за даними Офісу національної безпеки президента Південної Кореї, високопоставлені чиновники національної безпеки трьох країн (США, Японія, Південна Корея) досягли угоди під час зустрічі у Вашингтоні домовилися створити робочу групу для посилення заходів проти кібератак Північної Кореї. Вважається, що Пхеньян здійснив атаки для фінансування своєї ядерної та ракетної програм. Так, ще у жовтні 2023 року Рада безпеки ООН заявила, що минулого року північнокорейські хакери вкрали криптовалюту на загальну суму в 1,7 мільярда доларів.

Офіс національної безпеки президента Південної Кореї вважає, що потенційні кіберзагрози з боку міжнародних хакерських груп будуть зменшені завдяки постійній та різноманітній ро-боті з країнами, які поділяють демократичні цінності. Новий консультаційний орган буде займатися розробкою заходів блокування кіберзлочинів Північної Кореї і посиленням можливостей спільного реагування трьох країн на глобальні кіберзагрози.

Основними складовими успішних практик є створення комплексної нормативно-правової бази, що регулює інформаційний простір, розробка та впровадження сучасних технологічних засобів захисту, а також активна взаємодія державних структур з приватним сектором і громадянським суспільством. Крім того, у зарубіжній практиці важливу роль відіграє міжнародне співробітництво в сфері інформаційної безпеки. Партнерства на рівні міждержавних угод, участь у міжнародних організаціях та обмін інформацією між країнами сприяють підвищенню ефективності заходів щодо протидії глобальним кіберзагрозам.

### *15.5 Інформаційна безпека України в умовах євроінтеграції*

Нинішній етап інформаційної боротьби за-свідчив, що український інформаційний простір також потребує додаткового захисту від негативного інформаційно-психологічного впливу, який іде ззовні. Таким чином, українські національні інтереси в інформаційній безпеці полягають у тому, щоб розширювалися сучасні телекомунікаційні технології, а державні інформаційні ресурси були поза несанкціонованим доступом. Шляхами імплементації зарубіжного досвіду у сфері забезпечення інформаційної безпеки в умовах євроінтеграції України є:

1. Прийняття та адаптація міжнародних стандартів. Україна має приймати та адаптувати міжнародні стандарти з інформаційної безпеки, такі як ISO/IEC 27001, які визначають вимоги до створення, впровадження, підтримки та постій-ного покращення системи управління інформаційною безпекою.

2. Міжнародне співробітництво. Розширення співробітництва з міжнародними організаціями, такими як Європейський Союз, НАТО та ООН, з метою обміну інформацією про кіберзагрози, кращими практиками та спільної розробки рішень для протидії кіберзлочинності. Спільні навчання, участь у міжнародних кібербезпекових ініціативах та програмах допоможуть підвищити рівень національної безпеки та сприятимуть інтеграції України у глобальну систему кіберзахисту.

3. Розвиток законодавчої бази. Україна має вдосконалювати своє законодавство, враховуючи міжнародний досвід та стандарти у сфері інформаційної безпеки, що включає оновлення існуючих законів, розробку нових нормативних актів та створення правових механізмів, що забезпечать ефективний захист інформації в державному та приватному секторах, а також належний рівень відповідальності за порушення у цій сфері.

4. Розвиток державно-приватного партнерства. Ефективне забезпечення інформаційної безпеки можливе лише за умови тісної співпраці між державою та приватним сектором. Державно-приватне партнерство сприятиме обміну інформацією про кіберзагрози, спільному розробленню технологічних рішень та впровадженню інноваційних підходів до захисту інформації.

5. Забезпечення доступу до інформаційних технологій. Для ефективного впровадження заходів з інформаційної безпеки важливо забезпечити доступ до сучасних інформаційних технологій на сіх рівнях, що включає розвиток інфраструктури, підтримку та модернізацію державних та приватних інформаційних систем.

6. Впровадження технічних засобів захисту інформації. Важливим аспектом захисту інформації є впровадження сучасних технічних засобів, таких як системи шифрування, міжмережеві екрани, системи виявлення та запобігання вторгнень.

Запропоновані кроки сприятимуть підвищенню рівня інформаційної безпеки в Україні та дозволять ефективно адаптувати найкращі міжнародні практики до національних умов.

**ПИТАННЯ ДЛЯ САМОПЕРЕВІРКИ**

1. Якою є правова основа забезпечення інформаційної безпеки Європейського Союзу?
2. Охарактеризуйте інструменти та інститути забезпечення інформаційної безпеки Європейського Союзу.
3. Вкажіть особливості функціонування американської моделі забезпечення інформаційної безпеки.
4. На Вашу думку, в чому полягають переваги та недоліки азійської моделі забезпечення інформаційної безпеки?
5. Наведіть приклади поширення засобів інформаційного впливу за кордоном.
6. Окресліть складові кібернетичної безпеки (на прикладі зарубіжногот досвіду).
7. Якою, на Вашу думку, має бути інформаційна безпека України в умовах євроінтеграції? Обґрунтуйте свою відповідь.

## РЕКОМЕНДОВАНА ЛІТЕРАТУРА

**Основна література:**


1. Бабарикіна Н.А., Горло Н.В., Заболотна М.Ф., Кіндратець О.М., Сергієнко Т.І. (2022). Державний суверенітет в умовах глобалізації: теорія та практика : монографія. Запоріжжя : Запорізький національний університет, 226 с.
2. Безпека інформації : конспект лекцій (2021) / укладач О. С. Кушнерьов. Суми. 99 с.
3. Валюшко І.О. Інформаційна безпека України в контексті російсько-українського конфлікту: дис. … канд. політ. Наук, спеціальність 23.00.04. Миколаїв.
4. Гребенюк А.М., Рибальченко Л.В. (2020). Основи управління інформаційною безпекою: навч. посібник. Дніпро. 144 с.
5. Гур'єв В. , Мехед Д., Ткач Ю., Фірсова І. (2018). Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека». 166 с. http://ir.stu.cn.ua/bitstream/handle/123456789/19246/Інформ.%20безпека%20держ.%20New%20booklet%201.pdf?sequence=1&isAllowed=y
6. Доронін І.М. (2020). Національна безпека України в інформаційну епоху: теоретико-правове дослідження: дис. .. д-ра юрид. наук, спеціальність 12.00.01. Київ. 539 с.
7. Задерейко О., Троянський О., Чанишев Р., Дика А. (2022). Концептуальні основи захисту інформаційного суверенітету України : монографія. 220 с. URL: http://dspace.onua.edu.ua/server/api/core/bitstreams/dba680a2-4208-4586-b57a-8a6c45527ffa/content
8. Захаренко К.В. (2021). Інституційний вимір інформаційної безпеки України: трансформаційні виклики, глобальні контексти, стратегічні орієнтири: дис. .. д-ра політ. Наук, спеціальність 23.00.02. Львів
9. Золотар О.О. Інформаційна безпека людини: теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с.
10. Інформаційна війна і національна безпека : монографія / П.П. Ткачук, Р.В. Гула, О.І. Сивак, О.М. Щурко, В.В. Шемчук. Львів: НАСВ, 2015. 265 с.
11. Концептуальні основи захисту інформаційного суверенітету України : монографія (2022) / О. В. Задерейко, О. В. Троянський, Р. І. Чанишев, А. І. Дика. 2-ге вид., перероб. і доп. Одеса. 220 с.
12. Копійка М.В. (2020). Політика інформаційної безпеки у сучасних міжнародних відносинах: дис. … д-ра філософії, спеціальність 291. Київ. 205 с.
13. Кушакова-Костицька Н.В. (2018). Право на інформацію в інформаційну епоху (порівняльне дослідження): монографія. Київ: Логос. 271 с.
14. Любовець Г., Король В. (2021). Контент негативу. Як захистити себе та країну в умовах тотального інформаційного протистояння : монографія. Київ : Видавничий дім «Києво-Могилянська академія», 2021. 266 с.
15. Мужанова Т.М. (2019). Інформаційна безпека держави: Навчальний посібник. Київ. 131 с.
16. Нестеренко Г. (2022). Інформаційна безпека: курс лекцій. Київ: НАУ. 102 с.
17. Новіков В.О. (2024). Інституційні механізми публічного управління в умовах інформаційно-гібридних війн: дис. … канд. наук. з держ. упр., спеціальність 25.00.05. Національний університет цивільного захисту України. Харків. 218 с.
18. Панченко О.А. (2020). Державне управління інформаційною безпекою в епоху турбулентності: дис. д-ра наук із державного управління, спеціальність 25.00.05. Національний університет цивільного захисту України. Харків. 521 с.
19. Перун Т.С. (2019). Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні: дис. … канд. юрид. наук, спеціальність 12.00.07. Львів. 268 с.
20. Публічне управління та адміністрування в умовах інформаційного суспільства: вітчизняний і зарубіжний досвід: монографія (2017) / С. Чернов та ін. Запоріжжя.: ЗДІА. 602 с.
21. Російська війна проти України як тригер змін міжнародної безпеки: базові

наративи : аналіт. доп. / [Б. О. Парахонський, Г. М. Яворська]. Київ : НІСД, 2024. 49 с. (Серія «Міжнародні відносини»). URL:https://doi.org/10.53679/NISS-analytrep.2024.02

22. Сиротенко А.М. та ін. (2020). Воєнні аспекти протидії "гібридній" агресії: досвід України : монографія. К. : НУОУ ім. Івана Черняховського, 176 с.

23. Ткачук Т.Ю. (2019). Правове забезпечення інформаційної безпеки в умовах євроінтеграції України: дис. … д-ра юрид. наук, Ужгород. 487 с.

24. Торчий В.О. (2020). Інформаційне забезпечення державної безпеки України в умовах трансформаційних викликів і загроз: дис. … д-ра наук з держ. упр., спеціальність 25.00.05. Національний університет цивільного захисту України. Харків. 375 с.

25. Шемчук В.В. (2020). Конституційне-правове забезпечення інформаційної безпеки сучасних держав: порівняльно-правовий аналіз: дис. … д-ра юрид. наук, спеціальність 12.00.02. Ужгород. 2020. 411 с.

26. Яровенко Г.М. (2021). Інформаційна безпека як драйвер розвитку національної економіки: дис. … д-ра економіч. наук, спеціальність 08.00.03. Суми. 2021. 590 с.

**Додаткова література:**

1. Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 26 березня 2021 р.). [Електронне видання]. Київ : НА СБУ, 2021. 346 с.

2. Алещенко В. (2022). Інформаційно-психологічна безпека особистості в умовах гібридної війни. Вісник Київського національного університету імені Тараса Шевченка: Військово-спеціальні науки, 1(49), 13-21. DOI: https://doi.org/10.17721/1728-2217.2022.49.13-21

3. Амро Т. (2022). Взаємозв'язок систем забезпечення інформаційної безпеки та публічного управління в умовах воєнного стану: методи та можливості. Публічне урядування. № (5 (33), 83-88. DOI: https://doi.org/10.32689/2617-2224-2022-5(33)-11

4. Анісімович-Шевчук О. (2023). Сучасні інформаційно-психологічні впливи в системі міжнародних відносин у контексті російсько-української війни 2014–2022 років. Baltija publishing, 99-119. DOI https://doi.org/10.30525/978-9934-26-262-3-6

5. Бігдан М., Войціховський А. (2023). Діяльність НАТО із забезпечення інформаційної безпеки. Протидія кіберзлочинності та торгівлі людьми : зб. матеріалів міжнар. наук.-практ. конф. (м. Вінниця, 31 трав. 2023 р.), 27-29. URL: https://dspace.univd.edu.ua/handle/123456789/17091

6. Бондаренко Р.В., Михальчук В.М.(2021). Інформаційна безпека держави. Державне управління. № 5, 95-101. DOI: 10.32702/2306-6814.2021.5.95

7. Грицай Р.О. (2023). Інформаційні війни: пошук стратегій протидії. Теорія та історія публічного управління. № 33, 18-23. DOI: https://doi.org/10.32782/pma2663-5240-2023.33.3

8. Гришин М. (2023). Маніпулювання інформацією: теоретичні аспекти наукового дискурсу. Інтегровані комунікації, (2 (16), 38-43. DOI: https://doi.org/10.28925/2524-2644.2023.164

9. Гулай В., Базюк К.(2022). Інформаційно-психологічна складова гібридної війни Російської Федерації проти України (2014–2021 рр.): теоретико-методологічні засади дослідження. The Russian-Ukrainian war (2014–2022): historical, political, cultural-educational, religious, economic, and legal aspects: Scientific monograph. Riga, Latvia: "Baltija Publishing". URL: http://baltijapublishing.lv/omp/index.php/bp/ catalog/view/237/6326/13362-1

10. Дрига Д. (2023). Особливості розуміння феномену інформаційної безпеки у сфері публічного управління. Актуальні проблеми у сфері публічного управління. № 34. 108-111. DOI https://doi.org/10.32782/ pma2663-5240-2023.34.21

11. Дубовик Д. (2024). Удосконалення процесів втілення державної інформаційної стратегії в контексті глобальних змін. Національний університет «Житомирська політехніка». https://conf.ztu.edu.ua/wp-content/uploads/2024/02/63.pdf

12. Залєвська І.І., Удренос (2022). Інформаційна безпека України в умовах російської військової агресії. Південноукраїнський правничий часопис. № 1-2, 20-26. DOI: https://doi.org/10.32850/sulj.2022.1-2.4

13. Зінченко Д., Джафарова О. (2023). Інформаційно-психологічне забезпечення публічної безпеки в умовах воєнного конфлікту. Захист та дотримання прав громадян органами Національної поліції України в умовах воєнного стану : тези доп. учасників наук.-практ. конф. (м. Вінниця, 7 груд. 2023 р), 220-222. https://dspace.univd.edu.ua/handle/123456789/19713

14. Клочко А. (2023). Забезпечення інформаційної безпеки в умовах сучасного суспільства. Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління, (3(63), 38-42. DOI: https://doi.org/10.32689/2523-4625-2022-3(63)-6

15. Ковальов К. (2023). Інформаційна безпека: міжнародно-правовий аспект. Інформація і право. №4 (47), 159-167. DOI: https://doi.org/10.37750/ 2616-6798. 2023.4(47).291624

16. Кононенко В.П., Здоровко С.С., Корольова А.Є. (2023). Інформаційна безпека як стан. Науковий вісник Ужгородського Національного Університету. Серія: Право. Том 2 № 76, 244-250. URL: http://visnyk-juris-uzhnu.com/wp-content/uploads/2023/06/41-1.pdf

17. Крестьянполь Л., Мельник О., Новачевський С. (2023). Інформаційне протиборство як компонента забезпечення безпеки держави. MODERN WAYS OF SOLVING THE PROBLEMS OF SCIENCE IN THE WORLD Abstracts of VI International Scientific and Practical Conference Warsaw, Poland (February 13 – 15, 2023), 405-406. ttps://repositsc.nuczu.edu.ua/bitstream/123456789/17057/1/MODERN-WAYS-OF-SOLVING-THE-PROBLEMS-OF-SCIENCE-IN-THE-WORLD.pdf#page= 406

18. Легомінова С., Гайдур Г. (2023). Аналіз сучасних загроз інформаційній безпеці організацій та формування інформаційної платформи протидії їм. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 54–67. URL: https://doi.org/10.28925/2663-4023.2023.22.5467

19. Мазуренко Л. (2022). Інформаційна безпека в умовах російсько-української війни: виклики та загрози. Вісник Харківського національного університету імені В. Н. Каразіна, серія «Питання політології», № 42, 50-57. URL: https://doi.org/10.26565/2220-8089-2022-42-08

20. Нагорняк М. (2023). Інформаційна безпека надання електронних послуг: світовий досвід публічного управління. Наукові перспективи. № 12(42), 225-235. DOI: https://doi.org/10.52058/2708-7530-2023-12(42)-225-235

21. Онопрієнко С.Г. (2020). Понятя інформаційної безпеки сфери публічного адміністрування. Теоретичні питання юриспруденції і проблеми правозастосування: виклики XXI століття. Харків. 103-106.

22. Панченко О. (2021). Публічне управління інформаційною безпекою в умовах діджиталізації. Актуальні проблеми державного управління. Том 3 № 84, 150-157. DOI: https://doi.org/10.35432/1993-8330appa3842021246363

23. Помаза-Пономаренко А.Л., Новіков В.О. Шляхи трансформації інституційних механізмів публічного управління в Україні: від інформаційних загроз до гібридних війн // Державне будівництво. 2023. № 2. URL: https://periodicals.karazin.ua/db/issue/archive.

24. Рижков Е. (2024). Законодавче забезпечення інформаційної безпеки України в умовах воєнного стану. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/6900/1/22_12_2023.pdf#page=140

25. Ряполов А. (2023). Окремі напрями удосконалення забезпечення інформаційної безпеки в умовах війни. Scientific Collection «InterConf», (152), 303–307 https://archive.interconf.center/index.php/conference-proceeding/article/view/3169

26. Саган О.В. Протидія медіа-інформаційному тероризму як питання національної безпеки України : автореф. дис. ... канд. політ. наук: 21.01.01. Київ,2021. 22 с. URL: https://niss.gov.ua/sites/default/files/2021-04/06.04.2021_1-avtorefer_pidpis.-sagan_sig.pdf

27. Скочиляс-Павлів О.В. (2023). Сучасні загрози інформаційній безпеці України в умовах правового режиму воєнного стану. Юридичний науковий електронний журнал. № 9. 263-266.

28. Смотрич Д., Браіло Л. (2023). Інформаційна безпека в умовах воєнного стану. Науковий вісник Ужгородського національного університету. Серія: Право. Том 2 № 77, 121-127. DOI: https://doi.org/10.24144/2307-3322.2023.77.2.20

29. Талдикін О. (2023). Інформаційний суверенітет та його зміст. Науковий вісник Дніпропетровського державного університету внутрішніх справ, № 2, 132-138. DOI: 10.31733/2078-3566-2023-2-132-138

30. Усик С. (2021). Дослідження правового механізму забезпечення інформаційної безпеки в умовах надзвичайних ситуацій. Науковий вісник: Державне управління. № (4(6), 266–280. DOI: https://doi.org/10.32689/2618-0065-2020-4(6)-266-280

31. Філіпішина Л., Костик Є., Дзевелюк М. (2023). Публічне управління у сфері інформаційної безпеки (подолання сучасних загроз). Актуальні питання у сучасній науці, № 5 (11), 196-205. URL: https://www.academia.edu

32. Хорошко В., Хохлачова Ю., Пірцхалава Т., Іванченко І. Інформаційна зброя як інструмент інформаційної війни. Захист інформації. Том 24, No 2, квітень-червень 2022. С. 50–58. URL: https://jrnl.nau.edu.ua/index.php/ZI/article/view/16930

33. Черниш Р.Ф., Ігнатюк М.В. (2022). Протидія деструктивному інформаційному впливу в Україні: правові та організаційні аспекти. Юридичний науковий електронний журнал. № 1. 213-216. DOI https://doi.org/10.32782/2524-0374/2022-1/54

34. Чмир Я. І. Проблеми забезпечення інформаційної безпеки в системі публічного управління. Аспекти публічного управління. – 2018. – Т. 6. – № 9. – С. 16-22.

35. Шевчук О.М. (2023). До питання генези поняття інформаційної безпеки як складової національної безпеки. Науковий вісник Ужгородського національного університету. Серія: Право. Том 2 № 78, 134-139. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/285994

36. Шопіна І.М. (2022). Поняття інформаційної безпеки: концептуальні підходи до визначення. Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького: Серія Право. №13(25), 133-140. URL: http://visnyk.iful.edu.ua/wp-content/uploads/2022/06/Шопіна.pdf

37. Шустенко О. (2023). Маніпулятивні технології як феномен цифрової дійсності. Вісник Львівського університету. Серія філос.-політолог. студії, № 49, 200-204. URL: http://fps-visnyk.lnu.lviv.ua/archive/49_2023/25.pdf

38. Яковлєв П. (2020). Функції державного регулювання у сфері забезпечення інформаційної безпеки в Україні. Часопис Київського університету права, № 1, 155-159. URL: https://chasprava.com.ua/index.php/journal/article/view/277/262

**Інформаційні ресурси**

1. Електронна бібліотека Державного університету «Одеська політехніка» [Електронний ресурс]. URL: http://opu.ua/education/e-library

2. Національна бібліотека України імені В.І. Вернадського. [Електронний ресурс]. URL: http://www.nbuv.gov.ua.

3. Національна бібліотека України імені Ярослава Мудрого. [Електронний ресурс]. URL: http://nplu.org

4. Одеська національна наукова бібліотека [Електронний ресурс]. URL: http://www.odnb.odessa.ua

5. Офіційне інтернет-представництво Президента України [Електронний ресурс]. URL: http://www.president.gov.ua.

6. Офіційний вебпортал парламенту України [Електронний ресурс]. URL: https://www.rada.gov.ua

7. Єдиний веб-портал органів виконавчої влади України. [Електронний ресурс]. URL: https://www.kmu.gov.ua

8. Центр протидії дезінформації [Електронний ресурс]. URL: https://cpd.gov.ua