Міністерство освіти та науки України
Одеський національний морський університет

КОБОЗЄВА АЛЛА АНАТОЛІЇВНА

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ

Конспект лекцій

для здобувачів
першого (бакалаврського) рівня вищої освіти
спеціальності F5 Кібербезпека та захист інформації

частина І

Одеса-2025

Розробник: Кобозєва Алла Анатоліївна, доктор технічних наук, професор, завідувач кафедри «Кібербезпека та захист інформації»

Конспект лекцій схвалено на засіданні кафедри «Кібербезпека та захист інформації»
(Протокол від «06» жовтня 2025 р. №2)

Конспект лекцій схвалено на засіданні НМК ННІ ІТІП
(Протокол від «14» жовтня 2025 р. № 2)

ЗМІСТ

ТЕМА 1. ПОНЯТТЯ ТА ЗМІСТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

План

1. Вступ
2. Інформація та джерела її отримання
3. Роль інформації для суспільства та окремої людини
4. Поняття та зміст інформаційної безпеки як певної діяльності
5. Інформаційна безпека як соціальна діяльність для розвитку і реалізації національних інтересів

1. Вступ

Революційні зміни останніх років у електронній індустрії, в першу чергу, поява цифрових технологій і розповсюдження різних новітніх методів зв'язку, створили передумову і призвели до початку фундаментальних перетворень, результатом якого є об'єднання інфокомунікаційних і комп'ютерних систем і мереж у єдиний інформаційний простір.

Інформаційний простір стає сферою і середовищем боротьби, аналогічним суші, воді, повітрю, космосу, а також політики, економіці, оборони тощо. Крім того, інформаційний простір став середовищем різноманітних протиправних дій окремих осіб та різноманітних національних й міжнародних терористичних угрупувань.

Провідні країни світу та міжнародні організації в остані роки різко посилили увагу до проблеми власної безпеки. Критичні елементи національних інфраструктур практично усіх країн світу є вразливими від різних впливів і, поряд із звичними, кібернетичними.

Державна політики багатьох країн спрямована на здійснення національного та глобального моніторингу і впливу, у тому числі через інформаційний простір, на політичні, економічні, військові, екологічні та інші процеси з метою одержання однобічних переваг.

На сьогодні інформаційний вплив на інформаційний простір держави та суспільства більш ефективний, ніж політичний, економічний, а іноді і воєнний. Країни з більш розвиненою інформаційною інфраструктурою визначають умови формування і діяльність інформаційних структур в інших країнах, здійснюють суттєвий вплив на розвиток їхніх інформаційних сфер. При формуванні державної інформаційної політики одним із найбільших пріоритетів стає розвиток і гарантування ***інформаційної безпеки держави***.

Водночас, необхідно чітко бачити і враховувати ***протиріччя***, пов'язані із впровадженням в інформаційні ресурси держави та застосуванням у них заходів та засобів захисту. Ці протиріччя пов'язані з тим, що застосування систем захисту, якими б досконалими вони не були, створює певні «незручності» використання захищеного інформаційного простору держави.

2. Інформація та джерела її отримання

Інформацією називаються будь-які відомості, що отримані при вивченні даного питання і допомагають дати більш повний та обґрунтований ***висновок***.

Слід розрізняти: ***факти*** (дані), ***думки*** (особисті припущення), ***інформацію*** (аналітично опрацьовані дані).

Корисною виявляється будь-яка інформація навіть неперевірена чи та, що не може бути перевіреною, неправдива, неповна та ін., яка може бути використана для отримання обґрунтованого висновку. Тільки отримання максимально можливої в даних умовах інформації дозволяє зробити правильний та обґрунтований аналітичний висновок. Крім того, ця інформація використовується для перевірки надійності джерел інформації, визначення каналів дезінформації і т.д. Для вирішення будь-якої проблеми потрібна оптимальна, якісна, достовірна інформація.

Інформацію прийнято вважати цінною лише тоді, коли її можна використовувати, причому корисність інформації залежить від її повноти, точності та своєчасності.

Інформація дозволяє:

- Орієнтуватися в ситуації;
- Чітко планувати свої дії:
- відстежувати результативність акцій, що проводяться;
- Ухилятися від несподіванок;
- Маніпулювати окремими людьми та угрупованнями.

Інформація поділяється на:

- Тотальну або стратегічну (дає загальне оглядове уявлення про проблему та учасників – індивідів та організаторів ситуації);
- Поточну або оперативну (тримає в курсі подій, що змінюються);
- Конкретну (заповнює виявлені прогалини у даних чи відповідає на певні питання);
- Непряму (підтверджує або спростовує деякі припущення, будучи стикованою з останніми даними лише опосередковано);
- Оціночну (розтлумачує події та дає прогноз щодо їх розвитку у майбутньому; це – оптимально оброблені дані).

Розрізняють два основних види інформації:

- Біологічна,
- Соціальна.

Соціальна інформація представляє найбільший інтерес для дослідження в галузі життєдіяльності суспільства.

Соціальна інформація тісно пов’язана з практичною діяльністю людини, тому тут можна виділити стільки типів і різновидів, скільки є видів діяльності людини.

Прикладами можуть служити політична, військова, естетична, етична, економічна, технологічна (ноу-хау), вимірювальна, науково-технічна інформація. При цьому можливі різноманітні класифікації по різноманітних ознаках. Зокрема соціальна інформація ділиться на два класи:

- масова інформація;
- спеціальна інформація.

Масова інформація адресована всім членам суспільства незалежно від їхнього становища і роду діяльності. Спеціальна інформація адресована не всім членам суспільства, а певним соціальним групам (вченим даної спеціальності, економістам, військовим тощо). Ось найбільш важливі різновиди спеціальної соціальної інформації:

Наукова інформація утворюється в результаті науково-технічної діяльності. Наукову інформацію можна визначити як передане в інформаційному процесі наукове знання. Наукова інформація, як і наукове знання, є результатом абстрактно-логічного мислення й адекватно відбиває об'єктивні закономірності, явища і процеси реального світу, суспільства і духовної діяльності людини, вона повинна бути природно отримана науковими методами, що забезпечують істинність знання.

Технічна інформація створюється у сфері техніки і призначена для вирішення технічних задач (розробка нових технічних виробів, матеріалів, технологій). Структура і властивості наукової і технічної інформації досить близькі, тому ці два види часто об'єднують терміном «науково-технічна інформація». Проте, розрізняючи науку і техніку як сфери суспільного виробництва, розрізняють й інформаційні процеси, характерні для цих сфер, а також документи, призначені для техніки (патенти, стандарти, комп'ютерні програми, конструкторська документація) або переважно для науки (звіти про науково-дослідні роботи, монографії, теоретичні журнали, збірники наукових праць).

Технологічна інформація безпосередньо використовується для створення матеріальних благ. Нові високоефективні технології створюють певний імідж суспільства, держави.

Планово-економічна інформація про стан і перспективи розвитку народного господарства використовується для організації планового накопичення і впливу на управління суспільним виробництвом, у тому числі й в умовах ринкових відносин.

Необхідно відзначити, що інформація може бути: **відкритою, напівзакритою та секретною**. Розвідка спрямована насамперед на добування секретної інформації, проте розвідка не нехтує і відкритою інформацією: вона може отримувати секретну інформацію на основі збору та аналізу великого обсягу конфіденційної або навіть відкритої інформації. Саме тому роль розвідки в сучасному світі є надзвичайно високою, що необхідно обов'язково враховувати при розробці заходів з інформаційної безпеки. Сьогодні будь-які серйозні заходи, які проводяться державою, корпораціями, а часом і злочинними спільнотами, починаються зі збору інформації про потенційного супротивника для її подальшого аналізу та прийняття рішення.

Для отримання інформації можуть використовуватись **легальні, напівлегальні та нелегальні методи.**

До легальних методів належать: вивчення публікацій у засобах масової інформації; участь у науково-технічних конференціях; аналіз суспільно-політичних, наукових та технічних видань; відвідування виставок, дослідження повідомлень електронних ЗМІ (телебачення, радіо, Інтернет та ін.).

До напівлегальних методів можна, зокрема, віднести: бесіди із співробітниками у неофіційній обстановці; уявні переговори щодо купівлі продукції; неправдиві конкурси; запрошення на роботу провідних спеціалістів; отримання інформації від загальних постачальників, споживачів, через фонди та благодійні організації, через контролюючі органи та ін.

До нелегальних методів належать: викрадення образів продукції та/або технологічного обладнання; викрадення документів, що містять інформацію, що цікавить; закидання агентів проникнення на об'єкт противника; занурення агентів у структуру супротивника; знімання інформації з технічних каналів; проникнення в автоматизовані системи та ін.

До основних якісних характеристик інформації слід віднести: ***достовірність*** (коректність), ***об'єктивність***, ***однозначність***, ***достовірність джерела*** (чистота) та ***порядок інформації***.

Розглянемо кожну характеристику докладніше.

Достовірність (коректність) інформації – міра наближеності інформації до першоджерела чи точність передачі. Тут часто зустрічається той факт, що інформація, передана через третіх осіб в усній формі, мало відповідає як дійсності, а й вихідній інформації.

Об'єктивність інформації – міра відображення інформацією реальності. Тут важливо, що об'єктивність непроста: у будь-якій справі правд може бути безліч. Оцінювати об'єктивність інформації можна лише у ймовірнісних джерелах: «ймовірно…, ймовірно…, малоймовірно…» тощо.

Однозначність – поряд з об'єктивністю інформація має бути однозначною. Зауважимо, що достовірна інформація, навіть якщо вона є об'єктивною, не завжди є придатною для остаточних висновків та рішень.

Достовірність джерела (чистота) інформації – це ступінь наближеності джерела до місця створення інформації. Достовірність джерела часто підмінюється рівнем довіри, що суб'єктивно склався між вами. Абсолютно достовірної інформації від джерела немає: джерело може володіти лише інформацією, доступом до якої має (іноді авторитет джерела підміняє його реальні можливості); не володіючи спеціальними знаннями, джерело може стати жертвою дезінформації чи зловмисного обману з боку третьої особи.

Порядок інформації визначається в залежності від кількості передавальних ланок між джерелом та вами. Інформація може бути першого (найвищого) порядку, другого, третього і нижчого. У міру падіння висоти порядку знижується і достовірність.

3. Роль інформації для суспільства та окремої людини

Характерною ознакою сучасного етапу науково-технічного прогресу є стрімкий розвиток інформаційних технологій, їх використання як у повсякденному житті, так і в управлінні державою.

Інтенсивна інформатизація усіх сфер життєдіяльності суспільства є сьогодні одним із визначальних глобальних чинників подальшого соціально-економічного, інтелектуального та духовного розвитку людства. Водночас, світова спільнота вступає в новий етап своєї історії, котрий має всі підстави охарактеризувати його як еру інформаційних війн. Так, інформаційна складова є ключовим елементом гібридної війни Російської Федерації проти нашої держави. Це створює реальні загрози національній безпеці України, позаяк цілеспрямовано нищиться вітчизняна інформаційна інфраструктура на тимчасово окупованих територіях, проти України здійснюються кібернетичні атаки, блокуються канали поширення актуальної інформації щодо поточної соціально-політичної ситуації в країні, руйнівні інформаційні операції ведуться на тлі розгортання потужної пропагандистської кампанії проти України, спрямованої, зокрема, на перешкоджанням реалізації цивілізаційного вибору українського суспільства. Відтак, в умовах швидкого формування і розвитку інформаційного суспільства в Україні та глобального інформаційного простору, широкого використання інформаційно-комунікаційних технологій у всіх сферах життя особливого значення набувають ***проблеми інформаційної безпеки*** [[1]].

Процеси, що відбуваються в суспільному житті, можна охарактеризувати як посилення ролі та значення інформації як у суспільстві в цілому, так і в житті кожної окремої людини зокрема. Інформація отримує реальне матеріально-енергетичне, соціально-економічне, політичне і вартісне вираження. За цих умов одним з першочергових завдань, що постають перед правовою державою, є вирішення протиріччя між реально існуючими можливостями і зростаючими потребами особистості, суспільства і держави в якісних інформаційних ресурсах, продуктах та послугах і необхідністю забезпечення їх інформаційної безпеки. Політика у сфері інформаційної безпеки спрямована на досягнення такого рівня духовного та інтелектуального потенціалів країн, який є достатнім для розвитку державності і соціального прогресу.

Визнання проблеми інформаційної безпеки на міжнародному рівні обумовлюється такими чинниками глобалізації:

- у більшості розвинутих країн проводяться дослідження і розроблення нової інформаційної зброї, що дозволяє здійснювати безпосередній контроль над інформаційними ресурсами потенційного противника, а в необхідних випадках впливати на них
- кардинально змінилася оцінка доктрини інформаційної безпеки в цілому і позиції більшості країн світу, які усвідомили потенціал

[1]Указ Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» від 25.02.2017 № 47/2017: URL: www.president.gov.ua/documents/472017-21374 (дата звернення: 27.05.2018).

інформаційних загроз і необхідність створення відповідного міжнародного механізму для контролю інформаційного протиборства.

4. Поняття та зміст інформаційної безпеки як певної діяльності

Відтак, постає необхідність в окресленні поняття та змісту інформаційної безпеки як певної діяльності, спрямованої на створення достатніх умов для ***прогресивного розвитку*** національних інтересів в інформаційній сфері. У більш широкому плані йдеться про:

- забезпечення інформаційного суверенітету України;
- удосконалення державного управління інформаційною сферою, впровадження інноваційних технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;
- активне залучення засобів масової інформації до боротьби з корупцією, організованою злочинністю, сепаратизмом, тероризмом та іншими формами екстремістської діяльності, зловживанням службовим становищем, іншими явищами, які створюють сприятливі умови або безпосередньо загрожують національній безпеці України;
- неухильне дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання системи органів державного управління їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері та переслідування журналістів за політичні позиції;
- відповідальність ЗМІ за розповсюдження заздалегідь недостовірної інформації;
- інформаційне виховання громадян України;
- вжиття комплексних заходів щодо захисту національного інформаційного простору, протидії монополізації інформаційної сфери України, встановлення контролю над нею з боку будь-яких недержавних чи транснаціональних корпорацій.

Зазначимо, що розвиток інформаційних технологій є не лише важливою державною функцією, а й обов'язковою умовою забезпечення ефективного використання накопичених суспільством інформаційних ресурсів для створення розвиненого інформаційного середовища. Цій меті слугує організація функціонування системи інформаційної безпеки, складовими компонентами якої є національні інтереси в інформаційній сфері, загрози цим інтересам,сама інформаційна безпека як інструмент зі створення сприятливих умов для їх реалізації, які у сукупності становлять собою об'єкт управління органами державного управління, система забезпечення інформаційної безпеки, тобто суб'єкт управління, більше того, основні напрями політики національної безпеки в інформаційній сфері, а також внутрішнє та зовнішнє середовище. Зрозумілим є те, що інформаційна безпека забезпечується цілим комплексом заходів:

- Законодавчі. Використання законодавчих актів, що регламентують права та обов'язки фізичних та юридичних осіб, а також держави в галузі інформаційної безпеки;
- Морально-етичні. Створення та підтримка на об'єкті такої моральної атмосфери, у якій порушення регламентованих правил поведінки оцінювалося б більшістю співробітників різко негативно;
- Фізичні. Створення фізичних перешкод для доступу сторонніх осіб до об'єкта інформації, що охороняється;
- Адміністративні. Організація відповідного режиму секретності, пропускного та внутрішньооб'єктового режиму;
- Технічні. застосування електронних технічних та інших пристроїв для захисту інформації;
- Криптографічні та стеганографічні. Застосування шифрування та кодування для приховування оброблюваної та інформації, що передається, від несанкціонованого доступу;
- Програмні. Застосування програмних засобів для забезпечення інформаційної безпеки та розмежування доступу до інформації.

Відповідно вивченню цих заходів приділяється певна наукова увага.

Сучасні досягнення в галузі інформаційної безпеки дозволяють по праву віднести її до наукового напряму теорії інформації.

5. Інформаційна безпека як соціальна діяльність для розвитку і реалізації національних інтересів

Осягнення сутності предмета, уяснення змісту поняття «інформаційна безпека» є важливим завданнями наукового аналізу. ***Щодо інформаційної безпеки - це є поняття національної безпеки***, яке характеризує певний вид соціальної діяльності, ***основним змістом*** якої є створення сприятливих (необхідних і достатніх) умов для розвитку та реалізації національних інтересів.

Відповідно видове поняття «інформаційна безпека» різновид соціальної діяльності, який полягає в створенні державними і недержавними інституціями сприятливих умов для розвитку і реалізації національних інтересів в інформаційній сфері. Інформаційна безпека є складовим компонентом загальної проблеми інформаційного забезпечення ***розвитку*** людини, держави і суспільства. Вона орієнтована на захист значимих або вже згаданих суб'єктів інформаційних ресурсів, законних інтересів[2].

У найзагальнішому випадку інформаційна безпека — це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави.

Під інформаційним середовищем розуміють сферу діяльності суб'єктів, пов'язану зі створенням, перетворенням і споживанням інформації.

[2]В.А. ЛІПКАН, Ю.Є. МАКСИМЕНКО, В.М. ЖЕЛІХОВСЬКИЙ. ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ В УМОВАХ ЄВРОІНТЕГРАЦІЇ

Інформаційне середовище умовно поділяється (рис.1) на три основні предметні частини:

- створення і розповсюдження вихідної та похідної інформації;
- формування інформаційних ресурсів, підготовки інформаційних продуктів, надання інформаційних послуг;
- споживання інформації;

та дві забезпечувальні предметні частини:

- створення і застосування інформаційних систем, інформаційних технологій і засобів їхнього забезпечення;
- створення і застосування засобів і механізмів інформаційної безпеки.

Більш розгорнуте формулювання інформаційної безпеки — це стан захищеності потреб в інформації особистості, суспільства і держави, при якому ***забезпечується їх існування і прогресивний розвиток*** незалежно від наявності внутрішніх і зовнішніх інформаційних загроз.

Слід відзначити, що задоволення в будь-якій мірі потреб в інформації призводить до оволодіння відомостями про навколишній світ та процеси, що протікають в ньому, тобто інформованості особистості, суспільства та держави. Стан інформованості визначає ступінь адекватності сприйняття суб'єктами навколишньої дійсності і як наслідок — обґрунтованість рішень та дій, що приймаються.

В залежності від виду загроз інформаційній безпеці інформаційну безпеку можна розглядати наступним чином:

- як забезпечення стану захищеності особистості, суспільства, держави від впливу неякісної інформації;
- інформації та інформаційних ресурсів від неправомірного впливу сторонніх осіб;
- інформаційних прав і свобод людини і громадянина.

В інформаційному праві ***інформаційна безпека*** — це одна із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами.

Згідно з [3] Національними інтересами України в інформаційній сфері є:

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

[3]УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»

- захист українського суспільства від агресивного впливу деструктивної пропаганди, передусім з боку РФ;
- захист українського суспільства від агресивного інформаційного впливу Російської Федерації, спрямованого на пропаганду війни, розпалювання національної і релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України;
- всебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності у доступі до достовірної та об'єктивної інформації;
- забезпечення вільного обігу інформації, крім випадків, передбачених законом;
- розвиток та захист національної інформаційної інфраструктури;
- збереження і примноження духовних, культурних і моральних цінностей Українського народу;
- забезпечення всебічного розвитку і функціонування української мови в усіх сферах суспільного життя на всій території України;
- вільний розвиток, використання і захист мов національних меншин та сприяння вивченню мов міжнародного спілкування;
- зміцнення інформаційних зв'язків з українською діаспорою, сприяння збереженню її етнокультурної ідентичності;
- розвиток медіа-культури суспільства та соціально відповідального медіа-середовища;
- формування ефективної правової системи захисту особи, суспільства та держави від деструктивних пропагандистських впливів;
- створення з урахуванням норм міжнародного права системи і механізмів захисту від негативних зовнішніх інформаційно-психологічних впливів, передусім пропаганди;
- розвиток інформаційного суспільства, зокрема його технологічної інфраструктури;
- безпечне функціонування і розвиток національного інформаційного простору та його інтеграція у європейський і світовий інформаційний простір;
- розвиток системи стратегічних комунікацій України;
- ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації державної політики в інформаційній сфері;
- забезпечення розвитку інформаційно-комунікаційних технологій та інформаційних ресурсів України;
- захищеність державної таємниці та іншої інформації, вимоги щодо захисту якої встановлені законом;
- формування позитивного іміджу України у світі, донесення оперативної, достовірної і об'єктивної інформації про події в Україні до міжнародної спільноти;

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

Згідно з тим же самим документом актуальними ***загрозами*** національним інтересам та національній безпеці України в інформаційній сфері є:

- здійснення спеціальних інформоперацій, спрямованих на підрив обороноздатності, деморалізацію особового складу ЗСУ та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні;
- проведення державою-агресором спеціальних інформоперацій 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, недосконаліть 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.

Зауважимо, що для організації протидії загрозам інформаційній безпеці держави необхідно знати чинники, які сприяють виникненню ризиків і небезпек в ідеологічно-інформаційній сфері держави, з'ясувати їх сутність, уміти оцінювати та визначати ймовірність і рівень негативного впливу на суспільство й державу.

До головних чинників, що впливають на стан морально-ідеологічної стабільності та безпеки в Україні, належать[4]:

- відсутність цілісної системи інформаційно-аналітичного забезпечення органів державної влади й управління;
- руйнування інтелектуального потенціалу, неготовність наявної системи освіти до підтримання процесів випереджувального розвитку держави;

[4]ІСТОРІЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ПРОТИБОРСТВА: ПІДРУЧНИК / За загальною редакцією Є.Д.Скулиша

- повільність процесів усвідомлення прошарком колишньої радянської партійно-господарчої номенклатури, наукової й творчої інтелігенції, паростками нової буржуазії свого місця в суспільстві та формування власне української еліти, що призводить до неможливості сформувати керівними колами зрозумілої й привабливої для суспільства національної ідеї;
- низький загальний рівень розвитку інформаційної інфраструктури, що не виключає ймовірність експансії іноземних компаній на ринку інформаційних послуг; руйнування національного інформаційного простору та виникнення можливості його використання в антидержавних інтересах;
- недостатній професійний, інтелектуальний і творчий рівень вітчизняних виробників інформаційного продукту та послуг, їхня неконкурентоспроможність на світовому інформаційному ринку;
- інформаційна експансія провідних іноземних держав, розроблення й використання ними, міжнародними чи вітчизняними злочинними організаціями різних сучасних способів безпосереднього підриву;
- малоконтрольована діяльність окремих політичних сил, ЗМІ та осіб, спрямована на руйнування моральних цінностей, підрив морального й фізичного здоров'я нації; використання засобів масової інформації з позицій, протилежних інтересам громадян, політичних і громадських організацій, держави;
- утрата довіри до влади з боку значної частини населення внаслідок поширення компромату, застосування "брудних" політичних технологій, особливо під час виборчих кампаній;
- конкурентна боротьба за володіння ЗМІ, процес їхньої монополізації й концентрації інформаційної та політичної влади;
- маніпулювання громадською думкою (шляхом дезінформації, перекручування фактографічних даних, замовчування правдивих відомостей тощо).

Розглянемо детальніше найбільш значущі з чинників.

Відсутність цілісної системи інформаційно-аналітичного забезпечення органів влади та управління значно ускладнює прийняття ними зважених, науково обґрунтованих рішень, що породжує конфліктні ситуації у владних структурах і суспільстві.

Недостатнє інформаційно-аналітичне забезпечення діяльності характерне для всіх державних органів – як на центральному, так і на регіональному рівнях. Владні структури не мають достатніх можливостей завчасно прогнозувати розвиток подій у державі та навколо неї, належним чином ураховувати сприятливі й обмежувати несприятливі фактори, що визначають результативність прийнятих політичних рішень, здійснювати планування навіть на середньострокову перспективу.

Організація роботи інформаційно-аналітичних підрозділів дотепер не має системного характеру, а в періоди чергових скорочень чисельності державних органів діяльність деяких із таких підрозділів припиняється.

Руйнування інтелектуального потенціалу, неготовність системи освіти до підтримання процесів випереджувального розвитку країни призводить до того, що з огляду на рівень розвитку цієї галузі за кордоном і той факт, що багато держав світу приділяють особливу увагу інформаційній безпеці (створенню спеціальних органів і підрозділів для ведення інформаційних війн тощо), Україна й досі не має достатньої кількості кваліфікованих фахівців, які б змогли на належному рівні ефективно протидіяти щораз більшій інформаційній активності іноземних партнерів щодо її інформаційного простору.

На жаль, сучасне українське суспільство, зокрема соціальний прошарок, який має репрезентувати так звану національну українську еліту, поки що перебуває в стані морально-психологічного скніння, ідеологічного й політичного розколу. При цьому процес пошуку загальнонаціональних моральних та ідеологічних основ стратегії розвитку суспільства відбувається в умовах постійної жорсткої ідеологічної боротьби між іноземними конкурентами за геостратегічні позиції та вплив на правлячі кола України.

Низький загальний рівень інформаційної інфраструктури сприяє експансії іноземними компаніями ринку інформаційних послуг, що створює сприятливі умови для перерозподілу ефірного часу на користь іноземних програм, окремі з яких "засмічують" український інформаційний простір своїм баченням подій, пропагують власний спосіб життя та традиції, тим самим деструктивно впливаючи на суспільство й державу, руйнуючи морально-етичні основи генофонду української нації.

Недостатній професійний, інтелектуальний і творчий рівень вітчизняного виробника інформаційного продукту та послуг, його неконкурентоспроможність не лише на світовому ринку, а й в Україні, призводить до того, що українська аудиторія, природно, надає перевагу російським, американським, ізраїльським, польським, німецьким, французьким та іншим іноземним телесеріалам, розважальним й інформаційно-аналітичним програмам.

Недостатній контроль держави за дотриманням законів України політичними силами, ЗМІ й окремими особами, які займаються підприємницькою діяльністю в інформаційній сфері, спричиняє непоодинокі випадки надання ефірного часу теле- та радіопрограмам, спрямованим на руйнування моральних цінностей, свідомості української нації, підривання морального й фізичного здоров'я громадян.

У цьому випадку свідомо чи несвідомо ЗМІ створюють додатковий негативний вплив на психіку населення, "готуючи" її до проведення інших заходів прихованого вигідного іноземного впливу.

Утрата довіри до влади з боку значної частини населення відбувається, як уже зазначалося, внаслідок застосування "брудних" політичних технологій. Нині в Україні досить поширена практика оприлюднення

“замовних” статей із метою дискредитації окремих громадян і посадових осіб, про яких свідомо розголошуються неправдиві чи конфіденційні відомості. Неправдива інформація і так званий компромат активно поширюються через Інтернет. Для цього навіть створюються спеціалізовані веб-сайти. Розміщена на них інформація поширюється дуже швидко і може завдати моральної чи політичної шкоди громадянам України.

Потенційні можливості для поширення конфіденційної інформації про особу (без її згоди) мають відповідні банки даних, сформовані в довідкових службах, житлово-експлуатаційних конторах, бібліотеках, різних державних органах, лікарнях та інших установах. Наявність таких відомостей створює передумови для протиправних дій, зокрема шантажу громадян.

Отже, свідоме поширення неправдивої чи конфіденційної інформації стає важливим чинником інформаційно-ідеологічної безпеки, який завдає безпосередньої шкоди фізичним та юридичним особам у сфері забезпечення їхніх конституційних прав.

Нав’язування особі, суспільству бажаних іноземній стороні рішень у життєво важливих сферах суспільної та державної діяльності відбувається шляхом застосування великого арсеналу сил і засобів від ЗМІ до звичайних благодійних організацій, культурних обмінів між державами, а також різних місіонерських структур, що поширюють нетрадиційні релігійні вірування чи окультно-містичні традиції.

Ще одним чинником, який впливає на стан забезпечення інформаційної безпеки, є конкурентна боротьба за володіння ЗМІ та процеси їх монополізації й концентрації інформаційної та політичної влади. Фахівці зазначають, що в нинішніх умовах боротьба за вплив в електронних і друкованих мас-медіа, за контроль над кінокомпаніями, видавництвами та інформаційними агентствами спричиняє їх зосередження у руках однієї особи чи обмеженого кола людей. Саме це призводить до концентрації влади над споживачами, які одночасно є й виборцями, над політичними партіями та громадськими організаціями, профспілковими об’єднаннями (їм або може бути надана підтримка, або з ними боротимуться, або зовсім обійдуть увагою, начебто їх немає узагалі), над іншими видавцями, котрих можна загнати в глухий кут, журналістами, на яких можна “натиснути” тощо.

Злиття ЗМІ та виникнення монополістичних об’єднань у цій сфері, на нашу думку, призводить до:

- обмеження можливостей отримання інформації;
- здійснення впливу на свободу дій політичних партій;
- вигідного впливу на діяльність великих і малих видавництв.

Доктрина інформаційної безпеки України 2017 року визначає такі пріоритетні напрямки захисту інформаційного простору держави:

1. Щодо забезпечення інформаційної безпеки:
   - створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них;

- удосконалення повноважень державних регуляторних органів, які здійснюють діяльність щодо інформаційного простору держави, з метою досягнення адекватного рівня спроможності держави відповідати реальним та потенційним загрозам національним інтересам України в інформаційній сфері;
- законодавче врегулювання механізму виявлення, фіксації, блокування та видалення з інформаційного простору держави, зокрема з українського сегмента мережі Інтернет, інформації, яка загрожує життю, здоров'ю громадян України, пропагує війну, національну та релігійну ворожнечу, зміну конституційного ладу насильницьким шляхом або порушення територіальної цілісності України, загрожує державному суверенітету, пропагує комуністичний та/або націонал-соціалістичний (нацистський) тоталітарні режими та їхню символіку;
- визначення механізмів регулювання роботи підприємств телекомунікацій, поліграфічних підприємств, видавництв, телерадіоорганізацій, телерадіоцентрів та інших підприємств, установ, організацій, закладів культури та засобів масової інформації, а також використання місцевих радіостанцій, телевізійних центрів та друкарень для військових потреб і проведення роз'яснювальної роботи серед військ та населення; заборони роботи приймально-передавальних радіостанцій особистого та колективного користування і передачі інформації через комп'ютерні мережі в умовах запровадження правового режиму воєнного стану;
- оптимізація законодавчих механізмів реалізації зобов'язань України в межах Європейської конвенції про транскордонне телебачення щодо держав, які не є підписантами зазначеної Конвенції;
- створення і розвиток структур, що відповідають за інформаційно-психологічну безпеку, насамперед у Збройних Силах України, з урахуванням практики держав – членів НАТО;
- розвиток і захист технологічної інфраструктури забезпечення інформаційної безпеки України;
- забезпечення повного покриття території України цифровим мовленням, насамперед у прикордонних районах, а також тимчасово окупованих територій;
- розвиток цифрового мовлення, унеможливлення впливу на його інфраструктуру суб'єктів, що пов'язані з державою-агресором;
- побудова дієвої та ефективної системи стратегічних комунікацій;
- розвиток механізмів взаємодії держави та інститутів громадянського суспільства щодо протидії інформаційній агресії проти України;
- боротьба з дезінформацією та деструктивною пропагандою з боку Російської Федерації;
- посилення спроможностей сектору безпеки і оборони щодо протидії спеціальним інформаційним операціям, спрямованим на зміну конституційного ладу насильницьким шляхом, порушення

суверенітету і територіальної цілісності, підрив обороноздатності України, деморалізацію особового складу Збройних Сил України та інших військових формувань, загострення суспільно-політичної ситуації;

- виявлення та притягнення до відповідальності згідно із законодавством суб'єктів українського інформаційного простору, що створені та/або використовуються державою-агресором для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності;
- унеможливлення вільного обігу інформаційної продукції (друкованої та електронної), насамперед походженням з території держави-агресора, що містить пропаганду війни, національної і релігійної ворожнечі, зміни конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України, провокує масові заворушення;
- проведення розвідувальними органами України акцій сприяння реалізації та захисту національних інтересів України в інформаційній сфері, протидії зовнішнім загрозам інформаційній безпеці держави за межами України;
- недопущення використання інформаційного простору держави в деструктивних цілях або для дій, що спрямовані на дискредитацію України на міжнародному рівні;

2. Щодо забезпечення захисту і розвитку інформаційного простору України, а також конституційного права громадян на інформацію:

- стимулювання розвитку національного виробництва текстового і аудіовізуального контенту, зокрема шляхом створення системи квотування та проведення цільових конкурсів на надання грантів;
- забезпечення функціонування Суспільного телебачення і радіомовлення України, у тому числі його належного фінансування;
- створення системи мовлення територіальних громад, яка сприятиме розширенню комунікативних можливостей та зниженню конфліктності всередині громад;
- підтримка вітчизняної книговидавничої справи, зокрема перекладів іноземних творів, забезпечення ними навчальних закладів і бібліотек;
- розвиток правових інструментів захисту прав людини і громадянина на вільний доступ до інформації, її поширення, оброблення, зберігання та захист;
- комплексна підтримка розвитку механізмів саморегуляції засобів масової інформації на засадах соціальної відповідальності;
- підвищення медіа-грамотності суспільства, сприяння підготовці професійних кадрів для медіа-сфери з високим рівнем компетентності;
- удосконалення законодавчого регулювання інформаційної сфери відповідно до актуальних загроз національній безпеці;
- задоволення потреб населення тимчасово окупованих територій в об'єктивній, оперативній і достовірній інформації;

- повне покриття території України цифровим та інтернет-мовленням замість аналогового і надання рівних можливостей доступу кожному громадянину до інформаційних ресурсів мережі Інтернет;
- формування системи державної підтримки виробництва вітчизняного аудіовізуального продукту;
- пропагування, у тому числі через аудіовізуальні засоби, зокрема соціальну рекламу, основних етапів і досвіду державотворення, цінностей свободи, демократії, патріотизму, національної єдності, захисту України від зовнішніх і внутрішніх загроз;

3. Щодо відкритості та прозорості держави перед громадянами:
   - розвиток механізмів електронного урядування;
   - сприяння розвитку можливостей доступу та використання публічної інформації у формі відкритих даних;
   - інформування громадян України про діяльність органів державної влади, налагодження ефективної співпраці зазначених органів із засобами масової інформації та журналістами;
   - проведення реформи урядових комунікацій;
   - розвиток сервісів, спрямованих на більш масштабне та ефективне залучення громадськості до прийняття рішень органами державної влади та органами місцевого самоврядування;
   - сприяння формуванню культури суспільної дискусії;
4. Щодо формування позитивного міжнародного іміджу України:
   - ґрунтовне реформування системи представлення інформації про Україну на міжнародній арені;
   - розвиток публічної дипломатії, у тому числі культурної та цифрової;
   - активізація скоординованої інформаційної роботи закордонних дипломатичних установ України;
   - сприяння поширенню та розвитку системи іномовлення України;
   - створення та забезпечення функціонування правового механізму взаємодії державних органів з інститутами громадянського суспільства з метою інформаційної підтримки комерційної, гуманітарної, просвітницької, культурної та іншої діяльності таких інститутів за межами України;
   - постійний моніторинг пропаганди держави-агресора, розроблення та оперативна реалізація адекватних заходів протидії;
   - недопущення використання міжнародного інформаційного простору в деструктивних цілях або для дій, що спрямовані на дискредитацію України на міжнародному рівні;
   - реформування системи взаємовідносин з українською діаспорою шляхом забезпечення більш тісної співпраці та проведення ефективних заходів, зокрема в рамках комунікацій «від людини до людини»;
   - участь у міжнародних культурних заходах з метою представлення національної культури та ідентичності;

- запровадження міжнародних культурних фестивалів в Україні з метою популяризації української культури та розвитку комунікацій «від людини до людини».

Система забезпечення інформаційної безпеки передбачає формування відповідної системи протидії зазначеним вище загрозам. У загальному випадку можна виділити чотири основні складові цієї системи: нормативно-правову, організаційну, технологічну та кадрову.

Нормативно-правова складова повинна забезпечувати формування й удосконалення системи правових норм протидії загрозам інформаційній безпеці та механізмів їх реалізації. Вона утворюється сукупністю нормативних правових актів, інших нормативних документів, які регулюють відносини у сфері виявлення загроз безпеці індивідуальної, групової та масової свідомості громадян і протидії цим загрозам, що забезпечує реалізацію конституційних прав та свобод, їх законних обмежень, охорону психічного здоров'я громадян, збереження соціального спокою в суспільстві.

Організаційна складова системи забезпечення інформаційної безпеки має установлювати функціональну структуру громадських організацій і державних органів, що займаються реалізацією правових норм у цій сфері, й відносини між ними, а також між цими організаціями й органами, з одного боку, та громадянами – з іншого. При цьому найважливішою частиною організаційної складової системи мають бути відповідні структури громадянського суспільства.

Організаційна складова є важливою частиною загальної системи забезпечення інформаційної безпеки, конфігурація якої має бути позначена в Доктрині інформаційної безпеки країни. Система забезпечення інформаційної безпеки повинна будуватися на основі тісної взаємодії глави держави, органів законодавчої, виконавчої й судової влади, а також громадських організацій, що займаються установленою законом діяльністю в цій сфері.

Технологічна складова цієї системи повинна забезпечувати можливість вільного та безпечного інформаційного обміну між громадянами, членами груп, групових асоціацій і запобігання протиправному інформаційному впливу на них; своєчасне виявлення загроз інформаційній безпеці особи, суспільства та держави, оцінку можливого й завданого збитку цій безпеці та організацію ефективної протидії таким загрозам.

Кадрова складова має забезпечити формування й підтримання кадрового потенціалу суспільства та держави, необхідного для ефективного функціонування системи забезпечення інформаційної безпеки.

Варто виділити також найважливіші питання інформаційно-психологічної безпеки держави, які потребують нагального вирішення:

По-перше, розроблення основ державної політики в цій сфері, що зумовлено специфічністю об'єкта й предмета забезпечення безпеки. Держава за допомогою цивільного права повинна забезпечити запобігання найбільш суспільно небезпечним діянням у цій царині. Помилки в розмежуванні цих груп стосунків призводять як до недостатньої ефективності правового

захисту особистості, суспільства і держави, дискредитації влади, так і до відсутності належної уваги до створення суспільних інститутів, необхідних для вирішення проблеми.

По-друге, вдосконалення системи засобів масової інформації, що здійснює найсуттєвіший вплив на індивідуальну, групову та масову свідомість. З одного боку, відсутні досить ефективні механізми впливу суспільства на ЗМІ в інтересах захисту суспільної моральності, психічного здоров'я громадян, їхнього спокою, а з іншого – органи державної влади повільно проводять роботу з формування відкритих інформаційних ресурсів, що забезпечують громадянам можливість самостійного отримання достовірної та повної інформації про найбільш важливі події суспільного життя, діяльність органів влади щодо протидії наявним загрозам.

По-третє, виникають значні труднощі при оцінюванні втрати психічного здоров'я громадян. Вони пов'язані з відсутністю достатнього технологічного інструментарію для вирішення цього завдання; необхідного методичного апарату визначення та фіксації характеристик психіки конкретної людини, динаміки їх зміни, виявлення причин виникнення негативних тенденцій. Це особливо важливо для проведення судових експертиз за фактами неправомірної дії на психічну сферу людини та створення комплексних методик і засобів підвищення стійкості психіки до негативних інформаційних впливів, у тому числі через канали масової інформації.

Окремим аспектом інформаційної безпеки держави є створення системи підготовки кадрів для здійснення профілактичних робіт у цій сфері та проведенні експертиз і заходів щодо формування нормативного правового та технологічного забезпечення.

КОНТРОЛЬНІ ПИТАННЯ:

1. Якими чинниками глобалізації обумовлюється визнання проблеми інформаційної безпеки на міжнародному рівні?
2. Яке визначення можна дати "інформаційна безпеці" у найзагальнішому випадку?
3. На які частини можна умовно поділити інформаційне середовище?
4. Що відноситься до життєво важливих інтересів особи згідно з Національними інтересами України в інформаційній сфері?
5. Що відноситься до життєво важливих інтересів суспільства і держави згідно з Національними інтересами України в інформаційній сфері?
6. Які актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері існують?

ТЕМА 2. ЗАГРОЗИ ТА ДЖЕРЕЛА ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВИ

План

1. Поняття «загроза» для інформаційної безпеки
2. Дестабілізуючі фактори у сфері інформаційної безпеки
3. Класифікації загроз інформаційній безпеці
4. Джерела загроз інформаційній безпеці

1. Поняття «загроза» для інформаційної безпеки

Аналізові змісту поняття «інформаційна безпека» зазвичай дослідниками приділяється значна увага, у той час як такі поняття, як небезпека і загроза розглядаються дещо спрощено і здебільшого у звуженому плані, відірваному від контексту поняття «інформаційна безпека» [[567]].

Необхідність у розробленні поняття «загроза» визначається:

- відсутністю єдиного підходу до дослідження основних понять інформаційної безпеки;
- недостатньою розробленістю родового поняття «загроза» і питань його відмежування від інших споріднених понять, таких, як «небезпека», «виклик», «ризик», і відповідно видового «інформаційна загроза» і його відмежування від таких понять, як «інформаційна війна», «інформаційне протиборство», «інформаційний тероризм»;
- наявністю невирішеної проблеми формування категорійно-понятійного апарату теорії інформаційної безпеки;
- можливістю на підставі теоретичних розробок даного апарату формувати адекватну систему моніторингу та управління загрозами та небезпеками в інформаційній сфері.

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

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

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

---

[5] Мужанова Т.М. Інформаційна безпека держави. С. 40-43.

[6] Нестеренко Г. Інформаційна безпека. С. 17-24.

[7] Ліпкан В.А., Максименко Ю.Є., Желіховський В.М. Інформаційна безпека України в умовах Євроінтеграції. С. 118-129.

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

Небезпека містить у собі потенційну загрозу заподіяння шкоди тим чи іншим інтересам, для реалізації якої необхідне створення відповідних умов (накопичення можливостей і формування намірів), загроза ж є безпосередня можливість нанесення збитку, від початку здійснення якої її відділяє лише часовий інтервал, необхідний для прийняття рішення про реалізацію загрози.

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

- мають динамічний, змінний характер і включають події, зміни або дії;
- спричиняють шкоду або порушення нормального функціонування об’єкта (держави), і як наслідок є причиною збитків та втрат;
- виникають під дією певних чинників (зовнішніх та внутрішніх), і тому потребують комплексу заходів з боку держави для їх нейтралізації та усунення.

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

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.

Небезпечні інформаційні дії зазвичай розділяють *на два види*.

Перший пов’язаний зі втратою цінної інформації, що або знижує ефективність власної діяльності, або підвищує ефективність діяльності супротивника, конкурента. Якщо об’єктом такої дії є свідомість людей, то йдеться про розголошування державних таємниць, вербування агентів, спеціальні заходи й засоби для прослуховування, використання детекторів брехні, медикаментозних, біологічних та хімічних впливів на психіку людини. Безпеку від інформаційної дії цього виду забезпечують органи цензури, військової контррозвідки й інші суб’єкти інформаційної безпеки. Якщо ж джерелом інформації служать технічні системи, то йдеться вже про технічну розвідку, або шпигунство (прослуховування та перехоплення телефонних розмов, радіограм, сигналів інших систем комунікації), проникнення до комп’ютерних мереж, баз даних.

Другий вид інформаційної дії тісно пов'язаний з впровадженням негативної інформації, що не лише призводить до небезпечних помилкових рішень, але і змушує шкідливо діяти, що приводить суспільство до катастрофи. Інформаційну безпеку даного виду зобов'язані забезпечувати спеціальні структури інформаційно-технічної боротьби. Вони нейтралізують акції дезінформації, ослаблюють маніпулювання громадською думкою, ліквідовують наслідки комп'ютерних атак.

Розвиток і впровадження нових інформаційних технологій у різні сфери життєдіяльності суспільства, як і будь-яких інших науково-технічних досягнень, не лише забезпечують комфортність, але й іноді несуть небезпеку.

Найбільш значні групи *інформаційно-технічних небезпек*.

Перша група пов'язана з швидким розвитком нового класу зброї – інформаційної, що здатна ефективно впливати і на психіку, свідомість людей, і на інформаційно-технічну інфраструктуру суспільства. У відносно мирних умовах інформаційно-психологічні технології можуть застосовуватися в якості спеціальних механізмів управління кризами і провокації жорстокості на території супротивника.

Друга група інформаційно-технічних небезпек для особи, суспільства й держави – це новий клас соціальних злочинів, що ґрунтуються на застосуванні сучасних інформаційних технологій (махінації з електронними грошима, комп'ютерне хуліганство та ін.). Питання забезпечення інформаційної безпеки як однієї із важливих складових національної безпеки держави особливо гостро постає в контексті появи глобальної комп'ютерної злочинності й кібертероризма.

Третя група інформаційних небезпек – використання нових інформаційних технологій у політичних цілях. Яскравим прикладом є вибори Президента США у 2016 році, коли за допомогою інформаційних технологій розповсюджувалась дезінформація щодо кандидатки від демократичної партії Хіларі Клінтон.

2. Дестабілізуючі фактори у сфері інформаційної безпеки

Під *дестабілізуючими факторами у сфері інформаційної безпеки* розуміють такі явища та процеси природного і штучного походження, що породжують інформаційні загрози.

Джерелами дестабілізуючих факторів можуть бути як окремі особи, так і організації та їхні об'єднання. Джерелом дестабілізуючих факторів також може бути природне середовище.

Кожному джерелу властиві певні види дестабілізуючих факторів, які можна представити двома групами: міждержавні дестабілізуючі фактори і внутрішньодержавні дестабілізуючі фактори.

Одним із важливих дестабілізуючих факторів є агресивна політика інших держав або їх коаліції, в яких для формування інформаційних загроз створюються та функціонують спеціальні органи і служби.

Особливу групу джерел дестабілізуючих факторів складають інформаційні системи і засоби, оскільки вони одночасно є знаряддям

приведення в дію інформаційних загроз, каналом їх проникнення у свідомість особистості або суспільну свідомість, генератором спонтанних загроз, що виникають внаслідок технічних несправностей та інших причин.

Сукупність джерел разом із властивими їм видами дестабілізуючих факторів формують цілий спектр інформаційних загроз, що впливають на стан інформованості особистості, суспільства і держави. До них відносяться: викрадення, знищення, втрата, приховування, спотворення, розголошення, фальсифікація, компрометація корисної (істинної) інформації, а також фабрикування, розповсюдження і впровадження дезінформації.

До *внутрішньодержавних дестабілізуючих факторів* відносять:

- правовий вакуум у більшості питань забезпечення інформаційної безпеки;
- навмисне або ненавмисне порушення законодавства з питань інформаційної безпеки;
- політичні конфлікти;
- зловмисні дії злочинних елементів або груп;
- відмови, збої, технічні помилки інформаційних систем (засобів);
- природні явища (процеси), що ускладнюють одержання, передачу, прийом і зберігання інформації або руйнують інформаційні системи.

Міждержавні дестабілізуючі фактори – це конфлікти різноманітних масштабів і проявів (в економіці, політиці, ідеології, дипломатії і т. ін.).

Також фактори загроз інформаційній безпеці за видовою ознакою поділяють на політичні, економічні, організаційно-технічні.

Під *політичними факторами* загроз інформаційній безпеці розуміють:

- зміни геополітичної обстановки внаслідок фундаментальних змін у різноманітних регіонах світу, зведення до мінімуму ймовірності світової ядерної війни;
- інформаційна експансія розвинених країн, які здійснюють глобальний моніторинг світових політичних, економічних, воєнних, екологічних та інших процесів, та розповсюджують інформацію з метою здобуття односторонніх переваг;
- становлення нової державності в пострадянських країнах на основі принципів демократії, законності, інформаційної відкритості;
- знищення колишньої командно-адміністративної системи державного управління, а також системи забезпечення безпеки;
- порушення інформаційних зв'язків унаслідок утворення на території колишнього СРСР нових держав;
- прагнення пострадянських країн до більш тісного співробітництва із закордонними країнами в процесі проведення реформ на основі максимальної відкритості сторін;
- низька загальна правова та інформаційна культура сторін;
- перехід на ринкові відносини в економіці, поява на ринку великої кількості вітчизняних та зарубіжних комерційних структур — виробників та споживачів інформації, засобів інформатизації та

захисту інформації, включення інформаційної продукції в систему товарних відносин;

- критичний стан вітчизняних галузей промисловості, яка виробляє засоби інформатизації та захисту інформації;
- розширення кооперації із зарубіжними країнами в розвитку інформаційної інфраструктури.
- Основними *економічними факторами* загроз інформаційній безпеці є:
- перехід на ринкові відносини в економіці, поява на ринку великої кількості вітчизняних та зарубіжних комерційних структур – виробників та споживачів інформації, засобів інформатизації та захисту інформації, включення інформаційної продукції в систему товарних відносин;
- критичний стан вітчизняних галузей промисловості, які виробляють засоби інформатизації та захисту інформації;
- розширення кооперації із зарубіжними країнами в розвитку інформаційної інфраструктури.

Основними *організаційно-технічними факторами* загроз інформаційній безпеці є:

- недостатня нормативно-правова база у сфері інформаційних відносин, у тому числі в галузі забезпечення інформаційної безпеки;
- недостатнє регулювання державою процесів функціонування та розвитку ринку засобів інформатизації, інформаційних продуктів та послуг;
- широке використання у сфері державного управління та кредитно-фінансової сфери незахищених від витоку інформації імпортних технічних та програмних засобів для зберігання, обробки та передавання інформації;
- зростання обсягів інформації, яка передається відкритими каналами зв'язку;
- загострення криміногенної обстановки, зростання числа комп'ютерних злочинів, особливо в кредитно-фінансовій сфері.

Основні загрози інформаційній безпеці можна поділити на три групи:

- загрози впливу неякісної інформації (недостовірної, фальшивої дезінформації) на особу, суспільство, державу;
- загрози несанкціонованого і неправомірного впливу сторонніх осіб на інформацію й інформаційні ресурси (на виробництво інформації, інформаційні ресурси, на системи їхнього формування і використання);
- загрози інформаційним правам і свободам особи (праву на виробництво, поширення, пошук, одержання, передавання і використання інформації; праву на інтелектуальну власність на інформацію і речову власність на документовану інформацію; праву на захист честі й гідності тощо).

Аналіз та виявлення загроз інформаційної безпеки країни є важливою функцією її забезпечення. Розробка систем, форм та методів захисту інформації залежить саме від точності та систематичності вивчення потенційних загроз.

Загроза інформаційній безпеці є потенційною можливістю порушення режиму інформаційної безпеки.

3. Класифікації загроз інформаційній безпеці

Найчастіше загроза є наслідком наявності вразливих місць у захисті інформаційних систем, наприклад, неконтрольований доступ до персональних комп'ютерів або неліцензійне програмне забезпечення.

Історія розвитку та функціонування інформаційного середовища показує, що нові вразливі місця (загрози) з'являються постійно. Відповідно розробка засобів захисту інформаційної безпеки щодо усунення потенційних чи реальних загроз відбувається теж постійно. Як правило, засоби захисту інформації з'являються у відповідь на виникаючі загрози.

Такий підхід до забезпечення безпеки малоефективний, оскільки завжди існує проміжок часу між моментом виявлення загрози та її усуненням. Саме в цей період зловмисник може завдати непоправної шкоди інформації.

У зв'язку з цим більш прийнятним є інший спосіб захисту інформації – спосіб попереджувального захисту, що полягає в розробці механізмів захисту від можливих, передбачуваних і потенційних загроз.

Деякі загрози не можна вважати наслідком цілеспрямованих дій шкідливого характеру. Існують загрози, викликані випадковими помилками або техногенними явищами. Знання можливих загроз інформаційній безпеці, а також вразливих місць системи захисту, необхідне для того, щоб вибрати найбільш економічні й ефективні засоби забезпечення інформаційної безпеки.

Слід зауважити, що не існує однієї єдиної класифікації загроз інформаційній безпеці, кожна з існуючих може використовуватися в залежності від специфіки ситуації, тож нижче наведені різноманітні підходи до питання класифікації загроз, які застосовуються сьогодні.

За джерелами походження	
Природного походження	небезпечні геологічні, метеорологічні, гідрологічні явища, деградація ґрунтів чи надр, природні пожежі, масове руйнування (через природні катаклізми) каналів зв'язку тощо
Техногенного походження	транспортні аварії (катастрофи), пожежі, неспровоковані вибухи чи їх загроза, раптове руйнування каналів зв'язку, аварії на інженерних мережах і спорудах життєзабезпечення, аварії серверів та автоматизованих систем управління критичних об'єктів тощо
Антропогенного походження	вчинення людиною різноманітних дій з руйнування інформаційних систем, ресурсів, програмного

	забезпечення тощо. До цієї групи за змістом дій належать: ненавмисні, викликані помилковими чи ненавмисними діями людини; навмисні (інспіровані), результат навмисних дій людей
За повторюваністю вчинення	
Повторювані	загрози, які мали місце раніше
Продовжувані	неодноразове здійснення загроз, що складається з ряду тотожних загроз, які мають спільну мету
За сферами походження	
Екзогенні	джерело дестабілізації системи лежить поза її межами
Ендогенні	джерело дестабілізації системи перебуває у самій системі
За ймовірністю реалізації	
Вірогідні	загрози, які за наявності певного комплексу умов обов'язково настануть
Неможливі	загрози, які навіть за виконання певного комплексу умов ніколи не настануть. Такі загрози зазвичай мають більш декларативний, часто залякувальний характер
Випадкові	загрози, які за виконання певного комплексу умов кожного разу реалізуються по-різному
За рівнем визначеності	
Закономірні	загрози, які носять стійкий, повторюваний характер, що зумовлені об'єктивними умовами існування та розвитку системи. Так, наприклад, за умови відсутності системи інформаційної безпеки будь-який суб'єкт закономірно піддаватиметься інформаційним атакам
Випадкові	загрози, які можуть або трапитися або не трапитися за певних умов
За структурою впливу	
Системні	загрози, що впливають одразу на усі складові елементи системи
Структурні	загрози, що впливають на окремі структури системи
Елементні	загрози, що впливають на окремі елементи структури системи. Такі загрози мають постійний характер і можуть бути небезпечними лише за умови неефективності або непроведення їх моніторингу
За характером реалізації	
Реальні	активізація алгоритмів дестабілізації є неминучою і не обмежена часовим інтервалом і просторовою дією
Потенційні	активізація алгоритмів дестабілізації можлива за певних умов функціонування системи
Здійснені	загрози, які втілені у життя
Уявні	псевдореалізація механізмів дестабілізації, або ж активізація таких механізмів, що за деякими ознаками

	схожі з алгоритмами дестабілізації, але не є такими
За ставленням до них	
Об'єктивні	загрози, які підтверджуються сукупністю обставин і фактів, що об'єктивно характеризують навколишнє середовище. При цьому ставлення до них суб'єкта управління не відіграє вирішальної ролі через те, що об'єктивні загрози існують незалежно від волі та свідомості суб'єкта
Суб'єктивні	така сукупність чинників об'єктивної дійсності, яка вважається загрозою суб'єктом управління. У такому випадку визначальну роль у ідентифікації загрози відіграє воля суб'єкта управління, який і приймає безпосереднє рішення про надання статусу або ідентифікації тих чи інших подій в якості загроз безпеці

4. Джерела загроз інформаційній безпеці держави

Носіями загроз безпеці інформації є джерела загроз[8].

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

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

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

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

До зовнішніх джерел загроз інформаційній безпеці держави належать:

- іноземні політичні, економічні, військові, розвідувальні та інформаційні структури, діяльність яких спрямована проти інтересів держави в інформаційній сфері;
- іноземні держави;
- міжнародні, державні та приватні гравці, які беруть участь у міжнародній конкуренції за володіння та створення конкурентоспроможних інформаційних технологій та ресурсів;
- міжнародні терористичні організації, кримінальні структури;
- потенційні злочинці і хакери.

[8]Мужанова Т.М. Інформаційна безпека держави. Київ: ДУТ, 2019. С. 46–49.

Внутрішніми джерелами загроз інформаційній безпеці держави можуть бути:

- високопосадовці органів державної влади, політики, представники силових структур (з огляду на те, що вони володіють найбільшою кількістю конфіденційної інформації відповідно до займаного ними положення в державно-управлінській ієрархії);
- представники політичних партій, громадських організацій, ЗМІ;
- лідери громадської думки, наукова, культурна та мистецька еліта;
- представники релігійних організацій;
- потенційні злочинці і хакери.

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

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

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

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

Зовнішні джерела:

- діяльність іноземних політичних, економічних, військових, розвідувальних та інформаційних структур, спрямована проти інтересів держави в інформаційній сфері;
- прагнення ряду країн до домінування і утискання інтересів держави в світовому інформаційному просторі, витіснення її з зовнішнього і внутрішнього інформаційних ринків;
- загострення міжнародної конкуренції за володіння інформаційними технологіями та ресурсами;
- діяльність міжнародних терористичних організацій;

- збільшення технологічного відриву провідних держав світу і нарощування їх можливостей з протидії створенню конкурентоспроможних інформаційних технологій;
- діяльність космічних, повітряних, морських і наземних технічних та інших засобів (видів) розвідки іноземних держав;
- розробка низкою держав концепцій інформаційних війн, які передбачають створення засобів небезпечного впливу на інформаційні сфери інших країн світу, порушення нормального функціонування інформаційних і телекомунікаційних систем, збереження інформаційних ресурсів, отримання несанкціонованого доступу до них;
- культурна експансія з боку інших держав.

Внутрішні джерела:
- критичний стан вітчизняних галузей промисловості;
- несприятлива криміногенна обстановка, що супроводжується тенденціями зрощування державних і кримінальних структур в інформаційній сфері, отримання кримінальними структурами доступу до конфіденційної інформації, посилення впливу організованої злочинності на життя суспільства, зниження ступеня захищеності законних інтересів громадян, суспільства і держави в інформаційній сфері;
- недостатня координація діяльності державних органів державної влади, регіональних органів державної влади з формування та реалізації єдиної державної політики в галузі забезпечення інформаційної безпеки;
- недостатня розробленість нормативної правової бази, що регулює відносини в інформаційній сфері, а також недостатня правозастосовна практика;
- нерозвиненість інститутів громадянського суспільства і недостатній державний контроль за розвитком інформаційного ринку;
- недостатнє фінансування заходів щодо забезпечення інформаційної безпеки;
- недостатня економічна міць держави;
- зниження ефективності системи освіти і виховання, недостатня кількість кваліфікованих кадрів в галузі забезпечення інформаційної безпеки;
- недостатня активність органів державної влади в інформуванні суспільства про свою діяльність, в роз'ясненні прийнятих рішень, у формуванні відкритих державних ресурсів і розвитку системи доступу до них громадян;
- відставання від провідних країн світу за рівнем інформатизації органів державної влади і органів місцевого самоврядування, кредитно-

фінансової сфери, промисловості, сільського господарства, освіти, охорони здоров'я, сфери послуг та побуту;

- відсутність історичного, політичного та соціального досвіду життя у правовій державі, що торкається процесу практичної реалізації конституційних прав та свобод громадян, в тому числі в інформаційній сфері;
- посилення організованої злочинності та збільшення кількості комп'ютерних злочинів;
- постійне вдосконалення інформаційних систем та мереж зв’язку загалом, критичних інфраструктур зокрема;
- можливість концентрації ЗМІ в руках невеликої кількості власників і як наслідок формування ними інформаційного простору;
- зростання можливостей маніпулювання свідомістю широких мас населення за рахунок різноманітних технологій, формування віртуального простору;
- використання персональних даних особи на шкоду її інтересам, розширення прихованих можливостей збирання приватної інформації.

КОНТРОЛЬНІ ПИТАННЯ:

1. Які компоненти містить в собі загроза?
2. На які види поділяються небезпечні інформаційні дії?
3. Що розуміється під дестабілізуючими факторами у сфері інформаційної безпеки?
4. Що відноситься до внутрішньодержавних дестабілізуючих факторів? Що відноситься до міждержавних дестабілізуючих факторів?
5. На які групи поділяються джерела загроз інформаційній безпеці?
6. Що відноситься до антропогенних джерел загроз?
7. Що відноситься до техногенних джерел загроз?
8. Що відноситься до стихійних джерел загроз?

ТЕМА 3. ІНФОРМАЦІЙНИЙ ВПЛИВ ТА ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНІ ОПЕРАЦІЇ

План

1. Сутність поняття «інформаційний вплив»
2. Переконання та навіювання
3. Джерела загроз інформаційно-психологічній безпеці людини
4. Маніпулювання
5. Інформаційно-психологічний захист
6. Інформаційно-психологічні операції

1. Сутність поняття «інформаційний вплив»

Інформаційний вплив – це організоване цілеспрямоване застосування спеціальних інформаційних засобів і технологій для внесення деструктивних змін у свідомість особистості, соціальних груп чи населення (корекція поведінки), в інформаційно-технічну інфраструктуру об'єкта впливу та (чи) фізичний стан людини.

Інформаційний вплив варто поділяти на *інформаційно-технічний та інформаційно-психологічний*.

Інформаційно-технічний вплив (ІТВ) – це вплив на інформаційно-технічну інфраструктуру об'єкта з метою забезпечення реалізації необхідних змін у її функціонуванні (зупинка роботи, несанкціонований доступ до інформації та її перекручення (спотворення), програмування на певні помилки, зниження швидкості оброблення інформації тощо), а також вплив на фізичний стан людини. ІТВ становить загрозу безпеці інформаційно-технічної інфраструктури й фізичному стану людини.

Безпека інформаційно-технічної інфраструктури – це стан захищеності, який забезпечує її ефективне використання та захист від можливого ІТВ.

Безпека інформаційно-технічної інфраструктури поділяється на безпеку:

- машинно-технічних засобів (автоматизованих систем та мереж);
- програмного забезпечення;
- режиму захисту від несанкціонованого витоку інформації.

Інформаційно-психологічний вплив (ІПсВ) – це вплив на свідомість та підсвідомість особистості й населення з метою внесення змін у їхню поведінку і світогляд.

Обидва ці види впливів будуть ефективними тоді, коли їх здійснюють компетентні та забезпечені відповідними ресурсами суб'єкти. В той же час, на державі лежить відповідальність щодо нівелювання шкідливих чи загрозливих наслідків, що можуть нести за собою впливи, здійснювані ворожими, злочинними чи безвідповідальними суб'єктами.

Насамперед, важливо усвідомити, що ключові внутрішні і зовнішні інформаційні загрози народжуються на базовому рівні сприйняття інформації – індивідуальному. Саме людина з її потребами, переконаннями, психологічними особливостями, рівнем освіти та інтелекту піддається грандіозному впливу безлічі інформаційних імпульсів, значна кількість яких

носить деструктивний характер. “Загальним джерелом зовнішніх загроз інформаційній безпеці особистості є та частина інформаційного середовища суспільства, яка через різні причини неадекватно відображає дійсність. Тобто інформація, що вводить людей в оману, не дає можливості адекватно сприймати своє оточення і себе. Внутрішні джерела загроз інформаційній безпеці особистості закладені в самій біосоціальній природі психіки людини, в особливостях її формування та функціонування, в індивідуально-особистісних характеристиках індивіда, механізмах сприйняття та переробки інформації. З огляду на ці особливості, люди відрізняються мірою схильності до різних інформаційних впливів, можливостями аналізу та оцінки інформації, що надходить тощо ” [Отрешко В. Інформаційна безпека в контексті мовних пріоритетів українського державотворення/ В.Отрешко // Гілея: науковий вісник: збірник наукових праць.– К. : Видавництво “Гілея”, 2014]. Враховуючи такий “людиновимірний” рівень інформаційної безпеки, треба відмітити, що особливу роль в протистоянні деструктивним зовнішнім та внутрішнім інформаційним впливам має відігравати освіта громадян, яку здатна забезпечити тільки держава у плідному співробітництві з громадянським суспільством. Неосвічене населення легко підпадає під деструктивний вплив інформаційних загроз внутрішнього, зовнішнього і глобального характеру.

2. Переконання та навіювання

Базовими методами ІПсВ є ***переконання й навіювання***.

Переконання звернене до власного критичного сприйняття дійсності об’єктом впливу. Воно має певні алгоритми впливу:

- логіка переконання має бути доступною для інтелекту об’єкта впливу;
- переконання варто здійснювати, спираючись на факти, відомі об’єкту;
- переконлива інформація повинна містити узагальнювальні пропозиції;
- переконання має містити логічно несуперечливі конструкти;
- факти, що доносяться до об’єкта впливу, повинні мати відповідне емоційне забарвлення.

Навіювання, навпаки, спрямовується на об’єкти, які некритично сприймають інформацію. Його особливостями є:

- цілеспрямованість і плановість застосування;
- конкретність визначення об’єкта навіювання (селективний вплив на певні групи населення з урахуванням їхніх основних соціально-психологічних, національних й інших особливостей);
- некритичне сприйняття інформації об’єктом навіювання (навіювання засноване на ефекті сприйняття інформації як інструкції до дії без її логічного аналізу);
- визначеність, конкретність поведінки, що ініціюється (об’єкту необхідно дати інструкцію щодо його конкретних реакцій і вчинків, які відповідають меті впливу).

Навіювання або сугестія – це процес впливу на психіку людини, пов’язаний зі зниженням свідомості й критичності при сприйнятті навіяного

змісту, який не вимагає ні розгорнутого особистого аналізу, ні оцінки спонукання до певних дій. Суть навіювання полягає у впливі на відчуття людини, а через них – на її волю й розум.

Навіювання є основним способом маніпулювання свідомістю, прямим вторгненням у психічне життя людей. При цьому маніпулятивний вплив організується так, щоб думка, уявлення, образ безпосередньо входили у сферу свідомості та закріплювалися в ній як дані безперечні й уже доведені. Це стає можливим при підміні активного відношення психіки до предмета комунікації навмисно створеною пасивністю сприйняття, що так властиво релігійним виданням (розсіювання уваги поданням великої кількості інформації, активна форма її подання, штучне перебільшення престижу джерел).

ІПсВ спрямовується на індивідуальну або суспільну свідомість інформаційно-психологічними чи іншими засобами, що зумовлює трансформацію психіки, зміну поглядів, думок, взаємин, ціннісних орієнтацій, мотивів, стереотипів особи з метою вплинути на її діяльність і поведінку. Кінцевою його метою виступає досягнення певної реакції, поведінки (дії або бездіяльності) особистості, яка відповідає цілям ІПсВ.

Процес сприйняття індивідом ІПсВ, спрямованого на емоційну сферу свідомості, специфічний. Загалом, він більше згорнутий, ніж, наприклад, процес сприйняття пропагандистського впливу: в ньому функціонують тільки сприйняття й запам’ятовування, діяльність мислення виражена досить слабко. Інформацію особистість сприймає або не сприймає, сприймає цілком чи частково, але у формуванні певних висновків практично не бере участі. Процес ІПсВ на емоційну сферу свідомості включає довільне сприйняття та запам’ятовування й характеризується дуже зниженим рівнем усвідомлення змісту впливу. Осмислення отриманої інформації відбувається пізніше, при більш високій пізнавальній активності індивіда.

Потужність і ефективність маніпулятивного впливу залежить від наявності певних переваг у маніпулятора над адресатом. Раніше вже наголошувалося на прихованому від адресата характері маніпулятивного впливу, що відразу створює переваги маніпулятору. Є й інші переваги, які дають змогу маніпулятору використовувати специфічні прийоми впливу та підсилюють його ефект.

Рівень ефективності ІПсВ залежить від таких умов:

- *змісту матеріалу*: його складності, конкретності, суспільної важливості тощо. Наприклад, за рівних умов чим простіша інформація, тим більше шансів, що дії, на які вона спонукає, можуть виконуватися автоматично, особливо коли не суперечать переконанням об’єкта. Тобто, чим конкретніший заклик до дії, тим вищий ступінь автоматизму відповідної реакції;
- *психічного стану*, що характеризується наявністю високого рівня автоматизму відповідної реакції. Страх, пригніченість, апатія сприяють некритичному й підсвідомому сприйняттю впливу. Ступінь автоматизму у відповіді особи пов’язаний із рівнем усвідомленості та

критичності сприйняття інформації. Якщо вплив сприймається підсвідомо й некритично, то відповідь аудиторії може бути автоматичною;

- *часового інтервалу між впливами й відповідною реакцією*: із збільшенням часового інтервалу автоматизм реакції зменшується внаслідок підвищення критичності й розумової активності об'єкта (пояснюється включенням змісту отриманої інформації в систему знань особи й усвідомленням його).

3. Джерела загроз інформаційно-психологічній безпеці людини

Джерела загроз інформаційно-психологічній безпеці людини в міжособистісній комунікації під час здійснення на неї маніпулятивного впливу доцільно структурувати на три основні групи.

Перша група включає загрози, пов'язані з можливостями маніпулятора впливати на сам процес міжособистісної комунікації. Тобто, відповідно до своєї мети змінювати його хід, організацію, процедуру, інформаційний зміст, використовуючи для цього певні прийоми.

Друга група об'єднує загрози, пов'язані з можливостями використання маніпулятором зовнішніх для адресата чинників, і поділяється на такі підгрупи:

- умови зовнішнього соціального середовища (наприклад, можливість використання інших осіб для здійснення впливу; соціальних зв'язків, що склалися з адресатом і його оточенням тощо);
- особистий потенціал маніпулятора (скажімо, такі його статусні переваги, як рольова позиція, посада, вік, матеріальне становище, кваліфікація, освіта, здібності, знання, комунікативні навички, уміння й т. ін.);
- умови зовнішнього фізичного середовища (вибір місця та часу проведення міжособистісної комунікації, створення відповідної обстановки тощо).

Третя група включає загрози, пов'язані з можливостями використання маніпулятором внутрішніх, психологічних, індивідуально-особистісних характеристик адресата (зокрема його стану).

4. Маніпулювання

Застосовуючи відповідні прийоми впливу на різні психічні структури особистості адресата, маніпулятор досягає своєї мети. На відміну від міжособистісного, маніпулювання на політичному рівні знеособлене й передбачає вплив на широкі маси. Воля меншості (а то й окремої особи) в завуальованій формі нав'язується більшості. Маніпулювання свідомістю є системою ІПсВ із метою упровадження у свідомість певного світогляду, ціннісних установок, уявлень про мораль, моральність, нормативність тих чи інших форм поведінки.

Для маніпулювання використовуються такі методи, як перекручування, приховування та спосіб подання інформації.

Перекручування інформації варіює від відвертої брехні до часткових деформацій (підтасовування фактів або зміщення в семантичному полі поняття).

Приховування інформації найповніше проявляється як замовчування приховування визначених тем. Набагато частіше використовується метод часткового висвітлення чи диференційованого подання матеріалу.

Спосіб подання інформації нерідко відіграє вирішальну роль у тому, щоб зміст, який передається, був сприйнятий так, як необхідно його відправнику. Наприклад, велика кількість інформації в «сирому» чи несистематизованому вигляді дає змогу заповнити ефір потоками незначних відомостей, що ще більше ускладнює й без того безнадійні пошуки індивідом їхньої суті. Так само інформація, подана невеликими порціями, не дає можливості ефективно скористатися нею. В обох випадках заздалегідь знімається питання дорікання в приховуванні тих чи інших відомостей.

Найближчий до маніпулятивного впливу прийом особливого компонування тем, який начебто наводить одержувача інформації на цілком однозначні висновки. Важливу роль відіграє момент подання інформації.

Логіка маніпуляторів очевидна й закономірність однозначна: чим ширша аудиторія, на яку необхідно здійснити вплив, тим більш універсальними повинні бути мішені (на що спрямовувати зусилля). Спеціалізованість і точна спрямованість масового впливу можливі тоді, коли його організатору відомі специфічні якості потрібних верств населення чи груп людей. Відповідно, чим вужча передбачувана аудиторія, тим точнішим має бути підстроювання під її особливості. У випадках, коли таке підстроювання за будь-яких причин не проводиться, знову з’являються універсальні збудники: гордість, прагнення до задоволення, комфорту, бажання мати сімейний затишок, просування по службі, популярність, – цілком доступні й зрозумілі більшості людей цінності.

Більш «продвинуті» технології маніпулювання передбачають попередню підготовку думок або бажань, закріплення їх у масовій свідомості чи уявленнях конкретної людини для того, щоб можна було до них потім апелювати (наприклад, створення міфу про дбайливого президента або респектабельність компанії, переконання партнера в тому, що йому хочуть допомогти чи йому загрожує небезпека).

Роботизація. Особливо слід виокремити лейтмотив роботоподібності, який полягає в тому, що люди – об’єкти маніпулятивного оброблення – перетворюються на маріонеток, керованих владними силами за допомогою «ниточок» – засобів масової інформації. На соціально-рольовому рівні обговорюється залежність підлеглих від тиску організації, перетворення службовців на «прислужників». На міжособистісному рівні увага звертається на наявність запрограмованих дій у відповідь на ті чи інші впливи з боку партнерів у спілкуванні.

Окрім використання готових до «вживання» програм стереотипної поведінки, зусилля маніпуляторів спрямовані на уніфікацію способів мислення, оцінки й реагування великих мас людей, що призводить до

деіндивідуалізації та деперсоніфікації осіб, перетворення їх на податливих об'єктів маніпулювання.

Види змін в індивідуальній свідомості, які може спричинити ІПсВ:

- зміни психіки, психічного здоров'я людини. Оскільки в разі інформаційного впливу складно визначити межі норми й 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 й становлять небезпеку для усього суспільства, держави.

ІПсВ створюють загрозу інформаційній безпеці особи, суспільства та держави. Інформаційна безпека особи й суспільства є складовою інформаційної безпеки держави: її забезпечення займає особливе місце в державній політиці. Ця особливість визначається специфікою загроз та їхніх джерел, особливим характером принципів і завдань державної політики в цій сфері.

5. Інформаційно-психологічний захист

Об'єктом інформаційно-психологічного захисту (ІПсЗ) особи є стан її духовного та фізичного комфорту. Об'єкт захисту становлять і умови, фактори, які забезпечують розвиток усіх сфер життєдіяльності особи й суспільства, зокрема культури, науки, мистецтва, релігійних і міжнаціональних відносин. До об'єктів належать також мовне середовище, соціальні, ідеологічні, політичні орієнтири, суспільні й соціальні зв'язки, психофізичні фактори, що виявляються у вигляді фізичних, хімічних та інших впливів природного, антропогенного й техногенного походження; генофонд народів, які входять до складу населення держави тощо.

Найбільш важливими об'єктами ІПсЗ у сучасних умовах є індивідуальна та масова свідомість. Для особистості головними системотвірними якостями виступають цілісність (тенденція до стійкості) та розвиток (тенденція до зміни). При руйнуванні чи перекручуванні цих якостей особистість перестає існувати як соціальний суб'єкт. Це означає, що будь-який ІПсВ на особу має оцінюватися з позиції збереження чи руйнування її цілісності.

В сучасному інформаційному середовищі дуже важливу роль відіграють ЗМІ. Для ефективного ІПсЗ необхідно знати ознаки, які дозволяють виявити маніпулятивність інформаційного впливу через ЗМІ (за В.І. Полевим). Ці ознаки можна поділити на *організаційні* (притаманна системність та організованість) і *змістові*.

До організаційних належать:

1. Масове залучення фахівців із знанням мови держави – об'єкта впливу (журналістів, письменників, редакторів, теле-, радіоведучих тощо) іноземними суб'єктами.
2. Зосередженість компанії (організації, держави, інших суб'єктів) на інформаційному забезпеченні власної діяльності, а не на вирішенні проблем: знімають сюжет про безпечність виробництва та чудові умови праці замість того, щоб виділити кошти на утилізацію нечистот й очисні споруди.
3. Наявність у структурі організації інформаційно-аналітичних служб (прес-центр, інформаційна служба, власні видання, інтернет-сторінка).
4. Наймання фахівців із сфери піару, редакторів інформаційних служб, відомих телеведучих (*talkingheads*) тощо.
5. Трансляція та ретрансляція теле- і радіопрограм (передусім інформаційних) іноземного виробництва.
6. Залучення журналістів видання, каналу до участі в тренінгах, що проводять іноземні громадські організації (у процесі підготовки до виборів популярними є тренінги щодо аналізу джерел інформації; оброблення результатів соціологічних досліджень; збирання інформації про конкретних політиків; психологічних аспектів формування громадської думки; специфіки висвітлення економічної, соціальної та політичної тематики; технологій журналістських розслідувань і т. ін.).
7. Отримання фінансової допомоги (в обмін на замовну спрямованість матеріалів).
8. Формування власного «*agenda*» – переліку інформаційних повідомлень, які будуть висвітлені у ЗМІ, основних новин, порядку їх подання. Наочною формою реалізації цього організаційного заходу є підготовка та поширення так званих «темників».
9. Інформаційна ізоляція або запровадження цензури на інформацію, яка потрапляє до суб'єкта.
10. Притримування до певного часу (міждержавні офіційні переговори, закордонні візити, вибори), непоширення компрометуючої інформації, яка стала відомою ЗМІ.
11. Час виходу матеріалів – за відсутності можливості для відповіді або коли ця відповідь не буде почута (наприклад, 14 вересня 2005 р. о 19:30 в ефірі телеканалу "1+1" було оприлюднено інформацію про фінансування виборчої кампанії Ющенка Б. Березовським. У цей час президент Ющенко перебував за кордоном до 18 вересня 2005 р. на засіданні Генеральної Асамблеї ООН).
12. Інформація з маніпулятивними ознаками синхронно з'являється відразу в кількох джерелах (організувати це може лише єдиний координаційний центр). Відомі випадки, коли матеріал із покликанням на першоджерело виходив раніше, ніж його оприлюднювало першоджерело.
13. Акцентування уваги джерела на подіях, які є заздалегідь конфліктними в Україні. Ця ознака фіксується шляхом порівняння кількості повторів конфліктних тем у різних джерелах інформації (здійснюється за наперед

визначеним переліком конфліктних тем). Організація прес-конференцій із метою формування власного переліку інформаційних повідомлень, що варті висвітлення у ЗМІ.

14. Інформація з'являється в заздалегідь визначених рубриках із негативним контекстом: "невдаха року", "розчарування року", "сварка року"… (див. випуски новин телеканалу "Інтер" 26.12.2005 р., 27.12.2005 р.).
15. Оприлюднення інформації через Інтернет, який містить "спеціалізовані" загальнодоступні сайти для "зливу" компромату (наприклад, reporter.com.ua, compromat.ru, informacia.ru, Regnum.ru, vlasti.net тощо).
16. Джерелом інформації виступає особа (організація), діяльність якої пов'язана з іноземними спецслужбами (М.Мельниченко, Б.Березовський– о 19:30 14 вересня 2005 р. на "1+1" підтверджується інформація про фінансові зв'язки з Ющенком на тлі скандалу про фінансування виборчої кампанії).
17. Озвучувачем інформації є так звані "шоумени від політики": скандально відомі особистості (Д. Корчинський, Н. Вітренко, Н. Шуфрич, В. Жириновський).

До змістових ознак здійснення маніпулятивного інформаційного впливу належить:

1. Розгубленість, невизначеність, багатоваріантність та страх як загальний контекст інформації. Будь-яка особа психологічно прагне стабільності, визначеності, конкретних цілей і безпеки.
2. Кількість повторів ключових слів, які визначають суть повідомлення й можуть прив'язувати текст до негативних штампів: фашизм, нацизм, корупція, зрада, біль, терор і т. ін.
3. Присутність сенсації штучного походження (накшталт вибухи, катастрофи, злочини тощо, а не стихійні лиха чи явища природи). У хрестоматійному голлівудському фільмі про політичний піар "Хвіст крутить собакою" для відвернення уваги від неетичної поведінки президента США в мас-медіа був запущений міф про початок бойових дій в Албанії, який успішно протримався в ефірі до моменту згасання уваги до проступків президента.
4. Анонімність, використання псевдонімів авторами інформації: «за повідомленням нашого поінформованого джерела»; «в кулуарах влади ходять чутки», «джерело, яке побажало залишитись невідомим»...
5. Використання покликань на думку авторитетів: "як доведено науковцями", "не відповідає світовим стандартам", "експерти ФБР", "у той час як ще Аристотель (Маркс, Пушкін) зазначав" тощо. Посилання на авторитети використовується, коли треба без раціонального доведення підтвердити власну позицію.
6. Використання готових тверджень без аргументації (доведення): "Україна позбавлена виходів у світовий інформаційний простір", "у нас завжди так...", "Україна відстає від розвинутих країн у розвитку інформаційних технологій на кілька десятиріч", "Ющенко – американський шпигун".

7. Використання загальновживаних штампів: “демократичні країни”, “світовий тероризм”, “права людини”, “кланово-олігархічна система”, “антисеміт”, “бюрократ” тощо.
8. Оперування так званими “ідеальними поняттями”: свобода, демократія, справедливість, порядність, чесність, істина, правда, любов, Батьківщина, Бог, віра,святість,щастя.Джордж Бушусвоїйщорічній промові вКонгресіу2004 році 52 рази вжив слово “свобода” в різних поєднаннях, демаскуючи справжній зміст послання, авторське прочитання якого асоціюється з поняттями “перевага” (primacy), “війна”, “агресія”, “новий світовий порядок”.
9. Кількість прикметників стосовно обсягу тексту. Прикметники надають тексту емоційної забарвленості, тоді як новини повинні найточніше відображати факти, а не давати їм емоційну оцінку. Будь-який виступ, документ, рішення можна охарактеризувати таким чином, що їх текст буде мати характер темного, страшного, агресивного, а ці характеристики викликають негативні емоції. Вам потрібне негативне ставлення до нововведень? – Надрукуйте їх чорними літерами на червоному тлі.
10. Використання метафор (поетично, образно висловлена думка), гіпербол (перебільшень), порівнянь. Це, знову ж таки, свідчить про суб’єктивізм, емоційність (а не об’єктивність) оцінок.
11. Постановка запитань, які поступово підводять читача (глядача, слухача) до необхідної думки: “Скільки коштів бюджету США необхідно виділити на іракську кампанію?” замість “Чи є іракська кампанія легітимною? Чи підтримують громадяни цю кампанію?” Або “Які об’єкти газотранспортної системи України будуть передані в спільний російсько-український консорціум?” замість “Чи є допустимою зміна державної власності на об’єкти газотранспортної системи України?”.
12. Використання псевдонаукових термінів (на кшталт “кореляція детермінованих дефініцій”) призводить до втрати уваги чи навіть відлякування левової частки аудиторії.
13. Використання неологізмів (новостворених слів): цінності Майдану, кучмократія, нашизм, мегатерорист.
14. Використання синонімів із потрібним контекстом. Замість “війна” – “примус до миру”, “миротворча операція”, “умиротворення”; замість “блокада” – “ембарго”; замість “акції непокори”, “бунт” – “прояви протестів” тощо. І навпаки.
15. Невідповідність змістового (текст, звук) та відеоряду: повідомлення про діяльність радикального політичного угруповання показують на фоні картинки про зіткнення в Північній Ірландії або терористичної атаки 11 вересня2001 р. Тероризм – це завжди погано, отже, подія, про яку йдеться, – негативна.
16. Використання технічного прийому зйомки знизу, відомого як перспектива “жаби”, або показ об’єкта згори (перспектива “пташиного польоту”). Цей ракурс викликає антипатію до об’єкта, створює враження слабкості, порожності. Позитивна установка створюється за допомогою фронтальної

зйомки на рівні очей, оскільки психологами доведено, що це викликає симпатію до об'єкта, враження спокою, невимушеності.

Зазначений перелік не є вичерпним і повинен доповнюватись у процесі подальших досліджень у сфері інформаційної безпеки. Підкреслимо, наявність лише однієї з ознак ще не становить високу ймовірність того, що ми маємо справу з маніпулятивним інформаційним впливом як складовою спецоперації. Оцінюванню підлягає відповідність інформації відразу низці ознак. Об'єктивність та неупередженість оцінок на основі перелічених критеріїв може забезпечити або колектив фахівців-аналітиків, або застосування математичної теорії ймовірності.

Для оцінки змісту текстових повідомлень широко використовується контент-аналіз – формалізований метод вивчення текстової й графічної інформації, який полягає в переведенні інформації, що вивчається, в кількісні показники та її статистичному обробленні.

6. Інформаційно-психологічні операції

Інформаційні впливи на суспільство сьогодні набувають якісно нових форм: проводяться акції з використанням дезінформації, зливу компроматів, із замовчуванням та перекручуванням фактів [9].

У широкому сенсі під *інформаційно-психологічною операцією* розуміють сплановане використання засобів, форм і методів поширення інформації задля впливу на свідомість і поведінку людини.

Інформаційна війна, власне, складається з комплексу інформаційно-психологічних операцій. Одні сплановані агресором, який за допомогою дезінформації, зміщення чи заміщення акцентів у актуальних дискусіях, залякування, шокування намагається досягти своєї переваги в тих чи інших політичних, фінансово-економічних, соціальних питаннях. Інші ж розробляються як відповідь на деструктивний вплив. На неправдиву інформацію з боку нападника можна зреагувати якісним інформаційним продуктом, який здатний подолати інформаційний голод чи, навпаки, прибрати надлишок інформації.

У вужчому значенні інформаційно-психологічні операції розглядаються як інструмент, «зброя», технологія, що лише супроводжує бойові дії, гарячі фази збройних конфліктів або передує їм. У цьому сенсі вони застосовуються переважно для деморалізації і дезорієнтації противника чи, навпаки, зміцнення морального духу населення.

Таким чином, *інформаційно-психологічні операції* – обов'язкова складова війни. Однак пам'ятаймо, що вони цілком можуть розроблятися й проводитися і в мирний час. Такі операції складаються з політичних, військових та ідеологічних заходів, мета яких – зміна поведінкових і емоційних установок певних груп людей та окремих осіб з тих чи тих питань

---

[9] Марків О. Інформаційно-психологічні операції: поняття, види, способи використання в умовах гібридної війни / О. Марків // // Гібридна війна і журналістика. Проблеми інформаційної безпеки / за заг. ред. В.О. Жадька. – Київ: Вид-во НПУ імені М. П. Драгоманова, 2018. - С. 229-245.

у бажаному напрямку. Інформаційні операції використовуються як один із напрямів політики національної безпеки провідних країн світу.

На думку В. Горбуліна, термін "інформаційні операції" дає змогу точніше, ніж традиційний термін "інформаційні війни", дослідити місце та роль інформаційного протиборства як компонента глобальних протистоянь. <Його зміст> охоплює та розкриває інформаційний вплив на масову свідомість(як на ворожу, так і на дружню), вплив на інформацію, доступну супротивникові та необхідну йому для прийняття рішень, а також на інформаційно-аналітичні системи супротивника. Загалом інформаційні операції охоплюють також дії, спрямовані на фізичне ураження (знищення) автоматизованих систем, виведення з ладу засобів комп'ютерно-телекомунікаційної інфраструктури тощо».

В.М. Петрик у статті «Інформаційні операції в системі стратегічних комунікацій» пропонує розрізняти два поняття – акція інформаційного впливу і спеціальна інформаційна операція.

Акція інформаційного впливу – це поширення неповної, неточної, упередженої, недостовірної інформації, яке здійснюється одноразово і в дуже стислі терміни(1-3 дні). Спеціальна інформаційна операція, на думку науковця, має такі особливості: спланованість, скерованість на чітко визначену аудиторію, більша, порівняно з акцією, тривалість(від одного тижня і понад місяць); лавиноподібний характер зростання повідомлень на певну тему; сенсаційний, тенденційний і емоційний способи їх обговорення. У межах інформаційно-психологічної операції може бути проведено кілька акцій інформаційного впливу.

Отже, ***інформаційно-психологічна операція*** – це розробка і реалізація за продуманим планом інформаційно-психологічних впливів на життєві установки та поведінку людей для досягнення заздалегідь визначених цілей, зазвичай – прийняття якихось управлінських рішень.

Основне завдання інформаційних операцій(за В. Горбуліним) полягає в маніпулюванні масовою свідомістю з такими цілями, як, наприклад: внесення в суспільну свідомість і свідомість окремих людей визначених ідей і поглядів; дезорієнтація людей та їхня дезінформація; ослаблення усталених переконань людей, основ суспільства; залякування мас.

Ведучи мову про завдання інформаційних операцій слід зазначити: їхня реалізація не завжди може приводити до прогнозованих наслідків. Така природа віртуальних впливів.

По-перше, нереально врахувати всі соціальні, політичні, релігійні, історичні, економічні, психологічні, ментальні, культурні чинники, а також особливості сприймання інформації різними за національною належністю, віком, соціальним становищем та іншими характеристиками аудиторіями. Таким чином, неможливо точно передбачити ефект впливу, оскільки він залежить від безлічі не лише об'єктивних, а й суб'єктивних факторів, а також швидко змінюваної політичної кон'юнктури.

По-друге, потрібно враховувати і такий фактор, як наявність «імунітету» до певних інформаційних впливів у певному соціальному середовищі.

Канали впливу, використовувані від найдавніших часів і дотепер для реалізації інформаційних операцій дуже різноманітні: від оприлюднення і поширення листівок, плакатів до трансляції на багатомільйонну аудиторію промов політиків і лідерів думок, коментарів експертів, новин через програми телерадіомовлення та Інтернет-ресурси, соціальні мережі.

До основних видів інформаційно-психологічних операцій відносять ***наступальні та оборонні***. Хоча, як зазначає В. Горбулін, «на практиці більшість інформаційних операцій є змішаними». ***За метою і спрямованістю*** розрізняють також інформаційно-психологічні операції, які націлені 1) на прийняття потрібних агресорові управлінських рішень; 2) на компромат; 3) на пошкодження, виведення з ладу; 4) на дестабілізацію політичної чи економічної ситуації. ***За часом проведення*** зазвичай йдеться про короткострокові (1-2 тижні), середньострокові (2-4 тижні) і довгострокові (понад місяць).

Оскільки однією з найважливіших ознак інформаційно-психологічних операцій є їхня спланованість і продуманість у межах заздалегідь створеного плану, важливо усвідомлювати, якими є основні етапи їхнього розгортання, інакше кажучи – яким є сам план. У науці сьогодні немає одностайності в цьому питанні, тому для порівняння наведемо кілька запропонованих дослідниками схем.

В. Горбулін описує два алгоритми проведення інформаційно-психологічних операцій – для наступальних і оборонних (табл.1).

Таблиця 1. Порівняння етапів інформаційно-психологічних операцій наступу і оборони за В. Горбуліним [10]

Наступ	**Оборона**
Оцінка необхідності проведення операції	
1. Визначення мети, прогноз досяжності, ступеня впливу. 2. Збір інформації.	1. Аналіз можливих вразливостей (цілей). 2. Збір інформації про можливі операції. 3. Визначення можливих «замовників» інформаційних впливів: а) визначення сфер спільного інтересу об'єкта і потенційних «замовників»; б) ранжирування потенційних замовників за їхніми інтересами.
Планування	
1. Стратегічне планування наступальної операції (явне або неявне)	1. Стратегічне планування оборонної операції (явне або неявне): а) визначення критеріїв інформаційних впливів; б) моделювання інформаційних впливів з урахуванням зв'язків об'єкта; динаміки впливу; «особливих» (критичних) точок впливу; в) прогнозування наступних кроків;

[10]Горбулін В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія/ В.П. Горбулін, О.Г. Додонов, Д.В. Ланде. – Київ: Інтертехнологія, 2009. – 164 с.

	г) розрахунок наслідків. 2. Тактичне планування контроперацій.
Виконання	
1. Знаходження або створення інформаційного приводу. 2. Розкручування інформаційного приводу(пропаганда). 3. Оперативна розвідка. 4. Оцінка впливу. 5. Перешкода інформаційній протидії. 6. Коригування інформаційного впливу.	1. Виявлення та«згладжування» інформаційного приводу. 2. Контрпропаганда. 3. Оперативна розвідка. 4. Оцінка інформаційного середовища. 5. Коригування інформаційної протидії.
Завершальна фаза	
1. Аналіз ефективності. 2. Використання позитивних результатів інформаційного впливу. 3. Протидія негативним результатам.	

Інший підхід до фіксації етапів проведення інформаційно-психологічних операцій пов’язаний із урахуванням не лише наступального чи оборонного характеру останніх, а ще й із тими засобами, які в межах запланованих акцій використовуються. Причому тут наступ і оборона розглядаються як компоненти однієї й тієї самої операції.

Перша фаза – «експансія» (наступ) з метою забезпечення власної переваги на всіх фазах військової спецоперації через вплив на інформаційні процеси противника. Тут використовуються такі спеціальні засоби:

- технічні (максимальний захист власної інформації щодо плану, характеру і шляхів здійснення операції; радіоелектронна боротьба, атаки комп’ютерних мереж);
- психологічні (засоби введення в оману противника про хід операції; схиляння населення й перетворення поведінки особового складу ворога на вигідну для себе);
- публічні (інформування(без дезінформації!) громадськості про свої цілі й дружні війська; налагодження зв’язків з командуванням на території противника з метою створення сприятливих умов для проведення операції).

Друга фаза – власне «оборонна інформаційна операція», сукупність взаємозалежних заходів щодо захисту інформаційного середовища, розкриття ознак нападу, відновлення боєздатності й організації відповідних протидій з нейтралізації нападу. Тут використовуються всі ті засоби, що й під час інформаційного наступу, а також додаються протипропаганда, контррозвідка, фізичний захист інформаційної інфраструктури.

Оборона має забезпечувати адекватну відсіч загрозам, включно із загрозами терористичного та асиметричного характеру. Для прикладу, в антитерористичних спеціальних операціях переможний результат, що очевидно, може бути досягнутий не застосуванням новітніх високотехнологічних озброєнь, а шляхом інформаційної експансії. «Війни на випередження» відбуваються завдяки активізації інформаційно-

психологічного протиборства й диверсійно-розвідувальної діяльності держави.

В.М. Петрик подає в своєму дослідженні схему інформаційно-психологічної операції з огляду на ознаки, які помітні в інформаційному просторі під час її проведення. Зокрема, науковець стверджує: «Спеціальні інформаційні операції здійснюються за приблизно однаковою схемою: 1. Створення передумов (інформаційний етап) передбачає створення інформаційного приводу – конкретної або вигаданої події, яка використовується для спеціальної інформаційної операції. 2. «Розкрутка» інформаційного приводу передбачає поступове зростання напруги(кількості повідомлень та їх сенсаційності, тенденційності, емоційності і, як правило, недостовірності). 3. Загострення напруги… 4. Вихід із операції» [11].

У своїй книзі «Війна та антивійна» Е. Тоффлер наводить приклади прийомів, які найчастіше використовується для впливу на інших: звинувачення в звірячості; гіперболізація ставок; демонізація та дегуманізація опонента; поляризація; «божественні санкції»; метапропаганда, яка дискредитує пропаганду іншої сторони.

Сьогодні найпопулярнішими методами, які застосовуються в межах інформаційно-психологічних операцій, є пропаганда, дезінформація, психологічний тиск, розповсюдження чуток, диверсифікація громадської думки. Зазвичай вони є надійною «зброєю» пропаганди, інформаційної агресії, маніпулювання, інформаційного тероризму.

Розглянемо кожен із методів на прикладах сучасних інформаційно-психологічних операцій.

Пропаганда в межах інформаційно-психологічних операцій застосовується як спеціальний метод впливу на думки, емоції, настанови чи поведінку будь-якої окремої групи людей з метою набуття переваг, прямих чи непрямих.

Пропаганда [**https://ojs.dpu.edu.ua/index.php/irplegchr/article/view/63/61**] – 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.

Форми проведення пропаганди:

- пропаганда способу життя (соціологічна) – натуральний показ досягнень, переваг, перспектив конкретної держави тощо;
- формулювання та створення нових ідей;
- коректування наявних думок.

[11] Петрик В. Сутність і особливості проведення спеціальних інформаційних операцій та акцій інформаційного впливу / В. Петрик // Сучасні інформаційні технології у сфері безпеки та оборони. – 2009. – №3(6). – С. 71-75.

Пропаганда поділяється на види: ***позитивна*** й ***негативна*** [**https://ojs.dpu.edu.ua/index.php/irplegchr/article/view/63/61**].

Мета ***позитивної пропаганди*** – сприяти соціальній гармонії, злагоді, вихованню людей у дусі загальноприйнятих цінностей. Позитивна пропаганда виконує виховну та інформаційну функції у суспільстві. Вона здійснюється на користь тих, кому адресована, а не обмеженого кола зацікавлених осіб; не допускає обману та приховування фактів. У цьому її відмінність від негативної. Позитивна пропаганда не містить маніпулятивної мети, тому використовується не для проведення спеціальних інформаційних операцій, а для захисту населення від них.

Мета негативної пропаганди – розпалювання соціальної ворожнечі, ескалація соціальних конфліктів, загострення суперечностей у суспільстві, пробудження похітливих інстинктів у людей тощо. Це дозволяє роз‟єднувати людей, робити їх слухняними щодо волі пропагандиста. Технологія створення «образу ворога» дає можливість згуртувати натовп навколо пропагандиста, нав’язати людям потрібні переконання та стереотипи. Основна функція негативної пропаганди – створення ілюзорної, паралельної реальності з «хибною» системою цінностей, переконань, поглядів. При цьому активно використовується низька критичність та навіюваність мас із метою маніпулювання останніми на користь обмеженої групи осіб.

Виділяють декілька видів пропаганди.

Біла пропаганда — відверто нелояльна до адресата пропаганда, яка ведеться будь-якими засобами масової інформації (державними, комерційними, громадськими тощо) офіційними каналами без приховування її спрямованості та джерела.

Звичайно, що для досягнення успіху однієї білої пропаганди недостатньо. Тому, поряд із білою, використовується ***чорна пропаганда*** — нелояльна до адресата пропаганда, яка ведеться неофіційними каналами, у тому числі через можливості спецслужб, від імені вигаданих чи спеціально створених під відповідними легендами за допомогою методів маскування підпільних груп і опозиційних елементів.

Звичайно, що може існувати і проміжний елемент, так звана ***сіра пропаганда*** — нелояльна до адресата пропаганда, яка ведеться будь-якими засобами масової інформації офіційними каналами, але з приховуванням її спрямованості та справжнього джерела.

Яскравим прикладом ведення пропагандистських кампаній вважають діяльність Йозефа Геббельса, який проголосив такі принципи пропаганди:

1) пропаганда має бути спланована і вестися з однієї інстанції;

2) тільки авторитет може визначити, має бути результат пропаганди істинним чи фальшивим;

3) чорна пропаганда використовується, коли біла неможлива або вона не має належного ефекту;

4) пропаганда має характеризувати події та людей влучними фразами чи гаслами;

5) для кращого сприйняття пропаганда має викликати інтерес в аудиторії і передаватися через привабливе увазі середовище комунікацій.

Дезінформація – це метод, який передбачає введення об'єкта впливу в оману щодо справжності намірів для спонукання його до запрограмованих дій. Розрізняють такі види дезінформації [[12]]:

- тенденційне викладення фактів (упереджене висвітлення інформації щодо подій за допомогою спеціально підібраних правдивих даних);
- дезінформування «від зворотного» (надання правдивих відомостей у перекрученному вигляді чи в такій ситуації, коли вони сприймаються об'єктом спрямувань як неправдиві);
- термінологічне «мінування» (викривлення первинної правильної суті принципово важливих, базових термінів і тлумачень загально-світоглядного та оперативно-прикладного характеру).
- «сіре» дезінформування (використання синтезу правдивої інформації з дезінформацією);
- «чорне» дезінформування (передбачає використання переважно неправдивої інформації).

Психологічний тиск – цілеспрямований вплив на психіку людини шляхом залякування, погроз із метою схилення до певної запланованої моделі поведінки. До форм психологічного тиску відносять: доведення до об'єкта відомостей про реальні чи неіснуючі загрози та небезпеки; прогнози щодо репресій, переслідувань, убивств тощо; шантажування; здійснення вибухів, підпалів, масових отруєнь, захоплення заручників, інші терористичні акції.

Яскравим прикладом психологічного тиску у війні рф проти України є обстріли житлових будинків, лікарень, шкіл, дитячих садків, магазинів та інших будівель невійськового призначення.

Поширення чуток – діяльність із поширення різноманітної інформації (найчастіше неправдивої) серед широких мас населення переважно за допомогою неофіційних каналів із метою дезорганізації громадськості та держави або їх окремих закладів чи організацій.

Чутки можна ***класифікувати за трьома параметрами***: експресивними (емоційні стани, виражені в змісті чутки, і відповідні типи емоційних реакцій), інформаційними (ступінь достовірності сюжету чутки) та за ступенем впливу на психіку людей.

Так, ***за експресивною характеристикою*** визначають чутки-бажання, чутки залякування й роз'єднувальні агресивні чутки:

- Чутки-бажання. Інформація поширюється з метою викликати розчарування з приводу нездійснених очікувань і деморалізацію об'єкта впливу.
- Чутки-залякування. При їх поширенні в особи ініціюється стан тривоги, непевності. Це можуть бути чутки про смертельну

[12] Петрик В. Сутність інформаційної безпеки держави, суспільства та особи

суперзброю, якою володіє противник (сторона, що поширює чутки), про нестачу продовольства, зараження місцевості, питної води тощо.

- Роз'єднувальні агресивні чутки. Поширювана інформація має на меті внести розлад у суспільство, порушити соціальні зв'язки.

За ***інформаційною характеристикою*** чутки поділяються на абсолютно недостовірні, недостовірні, недостовірні з елементами правдоподібності та правдоподібні.

У сучасних умовах чутки поширюються переважно через соціальні мережі й мають такі наслідки: поширення паніки, емоційна пригніченість, прийняття неправильних рішень.

У соцмережах поширюються великі обсяги недостовірної (фейкової) інформації: неперевірені «фотофакти», «відео очевидців», «коментарі учасників» тощо. Загалом через соцмережі поширюються ті самі міфи й стереотипи, які створює російська пропаганда; також культивується емоційний стан тривоги, постійної готовності до захисної агресії.

Найчастіше поширюються рф чутки з демонізації українських військових, руйнування інфраструктури населених пунктів, знущання над мирним населенням українськими військами. Яскравими прикладами поширення чуток у війні рф проти України є: розповсюдження інформації про захоплення військами рф Києва. Ці чутки розповсюджувалися через мережу «Інтернет», а рідше в офіційних ЗМІ рф.

Чутки самопоширювані. Їхня природа ґрунтується на інформації, яку важко втримати. Достатньо створити відповідну чутку та запустити її в обіг у потрібному місці в слушний час. «Людський поголос» зробить решту. Практично немає ефективних засобів протидії чуткам. На офіційному рівні зупинити їх неможливо: це викликає протилежний ефект: чим численніші намагання їх спростувати, тим більша упевненість у їхній достовірності. Єдиний можливий спосіб подолання чуток – цілковите їх ігнорування. Через певний час напруження спадає, зайва активність в обговоренні уже неактуальних новин згасає, інтерес до порушеної в чутках проблеми зникає.

Диверсифікація громадської думки – розгалуження уваги правлячої еліти держави на різні штучно акцентовані проблеми з метою відволікання від вирішення першочергових завдань суспільно-політичного та економічного розвитку для нормального функціонування суспільства й держави.

Як бачимо, вплив інформаційних операцій країн-агресорів на систему міжнародних відносин настільки вагомий, що варто розробляти ефективні стратегії протидії, враховуючи гнучкість і непередбачуваність інформаційної зброї, а також концепції інформаційних війн.

Заходи протидії інформаційним операціям та заходи оборони можуть використовуватися як у межах операцій-відповідей на агресію, так і в межах кампаній реалізації глобальних стратегій безпекової політики держави.

Для прикладу розглянемо думки експертів щодо цього питання.

В. Гусаров [13] описує такі заходи:

1. створення та тиражування друкованих матеріалів; створення та транслювання телевізійних і радіопередач на позначений район;
2. передавання необхідних повідомлень через звукові засоби; використання мережі Інтернет в інтересах операції;
3. забезпечення можливості залучення організацій державної та недержавної форм власності з метою створення і трансляції рекламних роликів на телебаченні та в радіоефірах;
4. залучення операторів мобільного зв'язку для забезпечення передачі текстових, фотографічних, звукових та аудіовізуальних повідомлень пропагандистського характеру за допомогою мобільних телефонів.

В. Панченко [14] відзначає, що в інформаційній війні виправдовуються:

1. інформаційно-роз'яснювальна робота з населенням окупованих територій;
2. дискредитація діяльності незаконних терористичних угруповань та їх ватажків;
3. формування морально-психологічної стійкості українського суспільства до диверсійних та терористичних актів;
4. дискредитація дій ворожого уряду(порушення національного та міжнародного законодавства, необґрунтовані втрати серед військовослужбовців);
5. дискредитація ворожих каналів масової інформації, які поширюють фейки про події в Україні, маніпулюють історичними фактами;
6. наголошення на легітимності дій українського уряду;
7. мобілізація українського суспільства навколо ідеї захисту національної державності, боротьби з корупцією, розвитку економічного потенціалу України;
8. об'єктивне широкомасштабне інформування світової спільноти про події, що відбуваються в Україні, в тому числі шляхом створення іншомовних каналів поширення інформації, через дипломатичні можливості, експертне середовище;
9. формування нетерпимості до порушення норм міжнародного права, терористичних засобів політичної боротьби.

КОНТРОЛЬНІ ПИТАННЯ:

1. Що розуміється під "інформаційним впливом"? Чим відрізняється інформаційно-технічний вплив від інформаційно-психологічного?
2. Які методи є базовими для інформаційно-психологічного впливу?
3. Від чого залежить рівень ефективності інформаційно-психологічного впливу?
4. Які зміни можуть наступати в індивідуальній свідомості під дією інформаційно-психологічного впливу?

---

[13] Гусаров В. Сили інформаційних операцій Росії: якою має бути відповідь України?

[14] Панченко В.М. Інформаційні операції в системі стратегічних комунікацій / В. М. Панченко // Стратегічні комунікації. – 2016. – №4. – С. 72-79.

5. Що таке інформаційно-психологічна операція? Яке основне завдання інформаційних операцій?
6. Наведіть алгоритм проведення інформаційно-психологічних операцій для наступальних дій?
7. Наведіть алгоритм проведення інформаційно-психологічних операцій для оборонних дій?
8. Які можна виділити прояви інформаційної агресії в інформаційно-психологічних операціях?
9. Що таке інформаційний тероризм? Наведіть приклади.
10. Що таке дезінформація? Які види дезінформації існують?
11. Що таке психологічних тиск? Наведіть приклади методів психологічного тиску.

ЛІТЕРАТУРА

Базова

1. Інтегрована методологія виявлення, аналізу та нейтралізації загроз у сфері національної безпеки і оборони: монографія / С.В.Мілевський, С.С.Погасій, О.А.Лаптєв, В.А.Савченко, А.Г. Салій А.А.Кобозєва, П.В.Жук, Є.О.Меленті. – Харків: НТУ «ХПІ»; Львів: «Новий Світ-2000», 2026. – 424 с.
2. В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. — К.: КНТ, 2006. — 280 с. (Серія: Національна і міжнародна безпека).
3. Т.М.Мужанова. Інформаційна безпека держави. Навчальний посібник. – Київ: ДУТ. 2019. – 131 с.
4. Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. 102 с.
5. Горбулін В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія/ В.П.Горбулін, О.Г. Додонов, Д.В. Ланде. – Київ: Інтертехнологія, 2009. – 164 с.
6. Світова гібридна війна: український фронт. Монографія. За заг. ред. В.П. Горбуліна. К.: НІСД, 2017. 496 с.

Допоміжна

1. Марків О. Інформаційно-психологічні операції: поняття, види, способи використання в умовах гібридної війни / О. Марків // // Гібридна війна і журналістика. Проблеми інформаційної безпеки / за заг. ред. В.О. Жадька. – Київ: Вид-во НПУ імені М. П. Драгоманова, 2018. - С. 229-245.
2. Петрик В. Сутність і особливості проведення спеціальних інформаційних операцій та акцій інформаційного впливу / В. Петрик // Сучасні інформаційні технології у сфері безпеки та оборони. – 2009. – № 3(6). – С. 71-75.
3. Новицька Н. П. Петрик В. М., Кудико В. М. Пропаганда, диверсифікація громадської думки, психологічний тиск та поширення чуток як методи ведення спеціальних інформаційних операцій РФ проти України. - Ірпінський юридичний часопис: науковий журнал. 2022. Вип. 2 (9).
4. Панченко В.М. Інформаційні операції в системі стратегічних комунікацій / В. М. Панченко // Стратегічні комунікації. – 2016. – № 4. – С. 72-79.

Законодавча база

Доктрина інформаційної безпеки України. Затверджено Указом Президента України від 25 лютого 2017 року № 47/2017.
https://www.president.gov.ua/documents/472017-21374

Інтернет ресурси

1. Стратегія і тактика гібридних війн в контексті військової агресії Росії проти України. http://bintel.com.ua/uk/article/gibrid-war/
2. Антонов А.В., Бзот В.Б., Жилін Є.І. Україно-російський воєнний конфлікт: сутність, передумови та зміст агресії. Частина 1. https://informnapalm.org/2782-4gw-1/