Міністерство освіти і науки України

Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Інститут спеціального зв'язку та захисту інформації

В. А. Ананьїн, В. В. Горлинський, А. В. Гангал

ІНФОРМАЦІЙНА БЕЗПЕКА

МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Курс лекцій

Рекомендовано Вченою радою ІСЗЗІ КПІ ім. Ігоря Сікорського
як навчальний посібник для здобувачів ступеня магістр
за освітніми програмами Комп'ютерні системи і технології спеціального зв'язку та Спеціальні системи електронних комунікацій
спеціальностей 122 Комп'ютерні науки та 172 Електронні комунікації та радіотехніка за освітніми програмами

Електронне мережеве навчальне видання

Київ
ІСЗЗІ КПІ ім. Ігоря Сікорського
2025

УДК 004.056.5

Автори: *Ананьїн Валерій Опанасович*, д-р філос. наук, проф.
Горлинський Віктор Вікторович, канд. філос. наук, доц.
Гангал Артур Васильович, канд. філос. наук, доц.

Рецензент *Могилевич Д.І., д-р т. н., проф.,*
завідувач Спеціальної кафедри №3 ІСЗЗІ КПІ ім. Ігоря Сікорського

Відповідальний редактор *Ананьїн Валерій Опанасович*, д-р філос. наук, проф.

Рекомендовано Вченою радою ІСЗЗІ КПІ ім. Ігоря Сікорського
(протокол № 1 від 26. 09.2024 р.)

Інформаційна безпека. Менеджмент інформаційної безпеки держави [Електронний ресурс]: курс лекцій: навч. посіб. для здобувачів ступеня магістра за освітніми програми Комп'ютерні системи і технології спеціального зв'язку та Спеціальні системи електронних комунікацій спец. 122 Комп'ютерні науки 172 Електронні комунікації та радіотехніка / В. О. Ананьїн, В. В. Горлинський, А. В. Гангал. ІСЗЗІ КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,73 Мбайт). – Київ : ІСЗЗІ КПІ ім. Ігоря Сікорського 2025. – 140 с.

У навчальному посібнику викладено змістовні положення навчальної дисципліни "Менеджмент інформаційної безпеки держави" з урахуванням спрямованості підготовки сучасних військових фахівців у сфері спеціального зв'язку, захисту інформації та кібербезпеки. Розкрито загальні засади, завдання і складові менеджменту інформаційної безпеки держави з урахуванням досвіду, отриманому підрозділами Держспецзв'язку в ході виконання завдань за призначенням. Навчальний посібник призначений для здобувачів вищої освіти ступеня магістр за спеціальностями 122 Комп'ютерні науки, 172 Електронні комунікації та радіотехніка ІСЗЗІ КПІ ім. Ігоря Сікорського, а також для використання в освітньому процесі та службовій діяльності аспірантами і науково-педагогічними працівниками. Навчальний посібник буде також корисним для фахівців Державної служби спеціального зв'язку та захисту інформації України.

УДК 004.056.5

ЗМІСТ

“Хто думає про науку, той любить її,
а хто її любить, той ніколи не перестає вчитися …”
Григорій Сковорода

ПЕРЕДМОВА

Під час вивчення курсу “Менеджмент інформаційної безпеки держави” увага акцентується на теоретичному значенні дисципліни, яка сприяє формуванню основ соціального мислення.

Конспект лекцій підготовлено відповідно до програми курсу “Менеджмент інформаційної безпеки держави” та слугує для організації самостійної роботи курсантів з оволодіння теоретичним матеріалом навчальної дисципліни.

Предметом навчальної дисципліни є питання інформаційної безпеки держави що функціонує, а також система форм і методів організації захисту особового складу від негативного інформаційно-психологічного впливу.

Метою навчальної дисципліни є формування у курсантів наступних компетентностей:

- Здатність удосконалювати й розвивати свій інтелектуальний і культурний рівень, будувати власну траєкторію професійного розвитку й кар’єри;
- Здатність генерувати нові ідеї й нестандартні підходи до їх реалізації (креативність);
- Здатність до ефективних комунікаційних взаємодій, в тому числі засобами інформаційних технологій;
- Здатність визначати, транслювати цілі в професійній і соціальній діяльності;
- Здатність розв’язувати світоглядні, соціально- й особистісно значимі проблеми.
- Здатність застосовувати знання у практичних ситуаціях;
- Здатність проводити дослідження на відповідному рівні;
- Здатність до абстрактного мислення, аналізу та синтезу.

Програмні результати навчання, на формування та покращення яких спрямована дисципліна:

- Провадити дослідницьку та інноваційну діяльність у сфері інформаційної безпеки або кібербезпеки, а також у сфері технічного та криптографічного захисту інформації у кіберпросторі;
- Аналізувати, розробляти й супроводжувати систему управління інформаційною безпекою та кібербезпекою організації на базі стратегії і політики інформаційної безпеки;
- Аналізувати, розробляти й супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, операційних процесів у сфері інформаційної та кібербезпеки в цілому;
- Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
- Виконувати аналіз внутрішнього та зовнішнього середовища, використовувати методи та принципи менеджменту для прийняття управлінських рішень;
- Підвищувати ефективність службової діяльності на основі впровадження нових форм і методів керівництва та системи менеджменту якості;
- Формувати і постійно застосувати системне мислення під час оволодіння професією і в практичній діяльності.

Під час підготовки цього конспекту лекцій автори – укладачі використовували роботи В. Алещенка, В. Петрика, С. Гнатюка, М. Присяжнюка В. Остроухова, О. Корченка, М. Шелеста, С. Казмірчука, Ю. Ткача, Є. Іванченка, Д. Кулеби та інших вітчизняних авторів.

Автори висловлюють щиру вдячність авторам навчальних посібників, рецензенту та колегам по роботі, всім тим, хто посприяв виходу в світ цього конспекту лекцій.

Розподіл підготовленого навчального матеріалу: В. О. Ананьїн (передмова, теми 1–3, додат. матер.); В. В. Горлинський (теми 4–6, глосарій); А. В. Гангал (теми 7–8).

РОЗДІЛ І
БЕЗПЕКА В УМОВАХ ГЛОБАЛЬНИХ ТРАНСФОРМАЦІЙ СУЧАСНОГО СВІТУ

Тема 1. Предмет та завдання навчальної дисципліни "Менеджмент інформаційної безпеки держави".

Лекція 1. Заняття 1.1. Вступ до дисципліни "Менеджмент інформаційної безпеки держави".

Навчальні питання.

1 Мета, завдання, значення і місце навчальної дисципліни у підготовці фахівців.

2. Перелік компетентностей, які формуються у курсантів навчальною дисципліною.

1. Питання. Мета, завдання, значення і місце навчальної дисципліни у підготовці фахівців

Навчальна дисципліна "Менеджмент інформаційної безпеки держави", передбачена освітньо-професійною програмою підготовки здобувачів вищої освіти магістр.

Предметом навчальної дисципліни *є інформаційна безпека держави, що функціонує, а також система форм і методів організації захисту особового складу від негативного інформаційно-психологічного впливу.*

Успішне вирішення завдань навчальної дисципліни базується на засвоєні курсантами знань та умінь, сформованих у них, в результаті вивчення таких навчальних дисциплін: "Філософія", "Морально-психологічне забезпечення підрозділів Держспецзв'язку", "Педагогіка і психологія військових колективів" та ін.

Навчальні дисципліни, які забезпечуються цією навчальною дисципліною – "Сталий інноваційний розвиток", "Інтелектуальна власність та патентознавство" та інші.

Зміст навчальної дисципліни

Семестр 1-й.

Розділ І. Безпека в умовах глобальних трансформацій сучасного світу.

Тема 1. Мета та завдання навчальної дисципліни "Менеджмент інформаційної безпеки держави".

Тема 2. Національна безпека держави як соціальна проблема.

Розділ ІІ. Інформаційна безпека держави.

Тема 3. Інформаційна безпека як складова національної безпеки держави.

Тема 4. Гендерні аспекти інформаційної безпеки.

Розділ (змістовий модуль) ІІІ. Загрози безпеки держави, суспільства, людини в інформаційній сфері.

Тема 5. Загрози національної безпеки держави в інформаційній сфері.

Тема 6. Загрози людині та суспільству в інформаційній сфері.

Розділ ІV. Менеджмент по захисту інформаційної безпеки України.

Тема 7. Сутність та завдання менеджменту інформаційної безпеки.

Тема 8. Актуальні питання підготовки фахівців у сфері інформаційної безпеки та кібербезпеки.

2. Питання. Перелік компетентностей, які формуються у курсантів навчальною дисципліною

Метою навчальної дисципліни є формування у курсантів наступних загальних компетентностей:

- ❖ Здатність застосовувати знання у практичних ситуаціях;
- ❖ Здатність проводити дослідження на відповідному рівні, застосовувати знання у практичних ситуаціях;
- ❖ Здатність до абстрактного мислення, аналізу і синтезу;
- ❖ Здатність удосконалювати й розвивати свій інтелектуальний і культурний рівень, будувати власну траєкторію професійного розвитку й кар'єри;
- ❖ Здатність генерувати нові ідеї й нестандартні підходи до їх реалізації (креативність);
- ❖ Здатність до ефективних комунікаційних взаємодій, в тому числі засобами інформаційних технологій;
- ❖ Здатність визначати, транслювати цілі в професійній і соціальній діяльності;
- ❖ Здатність розв'язувати світоглядні, соціально й особистісно значимі проблеми.

Програмні результати навчання, на формування та покращення яких спрямована дисципліна:

- Провадити дослідницьку та інноваційну діяльність у сфері інформаційної безпеки або кібербезпеки, а також у сфері технічного та криптографічного захисту інформації в кіберпросторі;
- Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та кібербезпекою організації на базі стратегії і політики інформаційної безпеки;
- Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, операційних процесів у сфері інформаційної безпеки та кібербезпеки в цілому;
- Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб;
- Оцінювати ефективність та практичну цінність результатів наукових і практичних досліджень та інновацій;
- Виконувати аналіз внутрішнього та зовнішнього середовища, використовувати методи та принципи менеджменту для прийняття управлінських рішень;
- Підвищувати ефективність службової діяльності на основі впровадження нових форм і методів керівництва та системи менеджменту якості;
- Формувати і постійно застосовувати системне мислення при оволодінні професією та в практичній діяльності.

Завдання на самостійну роботу

1. Об’єкт, предмет та мета навчальної дисципліни “Менеджмент інформаційної безпеки держави”.
2. Методологічні засади навчальної дисципліни “Менеджмент інформаційної безпеки держави”.

Питання до самоконтролю

1. Значення і місце навчальної дисципліни у підготовці фахівців Держспецзв’язку.
2. Компетентності, які формуються у курсантів навчальною дисципліною.

Рекомендована до теми література

1. Менеджмент інформаційної безпеки: навч. посіб. для студентів спеціальності 125 “Кібербезпека” /О. Г. Корченко, М. Є. Шелест, С. В. Казмірчук, Ю. М. Ткач, Є. В. Іванченко. Ніжин: ФОП Лук’яненко В. В. ТПК “Орхідея”, 2019. 408 с. https://ir.stu.cn.ua/handle/123456789/19244 (дата звернення 13.05.2024).

2. Про інформацію: Закон України від 02 жовтня 1992 року № 2658-XII Верховна Рада України. Відомості Верховної Ради України. 1992. № 48. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення 13.05.2024).

3. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року “Про Стратегію інформаційної безпеки”. URL: https://zakon.rada.gov.ua/laws/show/n0080525-21#Text . (дата звернення: 29.06.2024).

4. Рішення Ради національної безпеки і оборони України “Про План реалізації Стратегії кібербезпеки” від 30 грудня 2021 року. Указ Президента України від 1 лютого 2022 року № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text (дата звернення: 14.02.2024).

5. Закон України “Про основні засади забезпечення кібербезпеки України” від 05 жовтня 2017 року № 2163-VII. URL: https:// https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 14.02.2024).

Тема 2. Національна безпека держави як соціальна проблема.

Лекція 2. Заняття 2.1. Національна безпека України у системі сучасних геополітичних координат.

Навчальні питання.

1. Сутність та задачі національної безпеки.

2. Види національної безпеки.

1. Питання. Сутність та задачі національної безпеки

Трансформаційні процеси, що відбуваються в країнах світу, викликають багато питань і змушують соціальну науку переосмислити безліч проблем. Важливою складовою сучасних суспільств є *феномен сталого та безпечного розвитку в умовах глобальних та кардинальних змін у світі*. Однією з актуальних для України, як і для інших держав, є проблема забезпечення її безпеки в сучасних умовах. Це обумовлено необхідністю нового розуміння напряму світового розвитку та проблеми безпеки залежно від обставин, що безперервно змінюються.

По-перше, науково-технічний прогрес створив умови для прискорення процесів глобалізації та інформаційної революції, становлення взаємопов'язаного, взаємозалежного світу. Вони впливають на всі сторони життя суспільства, в тому числі і на його безпеку.

По-друге, у зовнішньополітичній обстановці, що склалася в сучасному світі, відбуваються динамічні зміни, що суттєво впливають на розвиток міжнародної системи безпеки та реформування національних політик з питань безпеки.

По-третє, бурхливе зростання національної самосвідомості народів, прагнення зберегти свою самобутність за допомогою своєї держави призвели до поширення конфліктів на етноконфесійній основі на усій земній кулі.

По-четверте, процеси глобалізації не зменшують протистояння між народами та державами, а ще більше посилюють його.

По-п'яте, усе більших масштабів набуває міжнародний тероризм, який призводить до масової загибелі мирного населення.

По-шосте, екстраординарного значення набули глобальні проблеми, які є результатом тривалого історичного розвитку суспільства, зумовленого суперечливим процесом взаємодії людини, суспільства і природи, у ході якого виникають проблеми, пов'язані зі шкодою, що завдають люди природі.

Безпека, як загальний атрибут суспільного буття, має різні смисли і значення, згідно з множиною об'єктів, стосовно яких використовується поняття. Вона має модуси:

- стану, властивості, здатності, характеристики;
- розуміється й відповідно оцінюється як передумова, потреба, умова, фактор, норма життєдіяльності, правило, вимога, інтерес, суспільне благо;
- може розумітися як система, підсистема, структура, організація, механізм, зв'язки та елементи природного, соціального і технічного характеру.

Безпека є актуальним показником якості предметів.

***Безпека**, у загальному розумінні, означає надійне існування будь-якого об'єкта за наявності всіляких йому загроз.*

Практично загрози існують завжди, мова може йти лише про їхнє посилення, достатню нейтралізацію. Для характеристики такого стану використовується загальноприйняте в міжнародному спілкуванні поняття "безпека", що традиційно визначається як "положення, при якому кому-небудь або чому-небудь не загрожує небезпека". В даний час зміст цього поняття вийшов за рамки, що використовувались раніше.

Вперше в політичному лексиконі поняття "національна безпека" було вжито у **1904** році в посланні президента США ***Т. Рузвельта*** Конгресові, де він обґрунтовував підпорядкування зони Панамського каналу інтересам національної безпеки США.

У концептуально-теоретичному оформленні основні ідеї сучасного розуміння безпеки вперше були сформульовані в *"Законі про національну безпеку", прийнятому в США у 1947 році.* На його основі була створена Рада національної безпеки, до складу якої було включено президента, віце-президента, держсекретаря та міністра оборони США. Апаратом РНБ керував помічник Президента з національної безпеки.

Безпека (національна безпека*)* – *визначений ступінь захищеності особистості, суспільства, держави від внутрішніх і зовнішніх загроз, що дозволяє їм існувати і постійно стало розвиватися*.

В залежності від того хто або що виступає об'єктом захисту, ззовні або зсередини випливають загрози, розглядають безпеку:

***а) зовнішню** (національну, регіональну, глобальну);*

б) внутрішню *(особистості, соціальної групи, влади, держави, суспільства).*

Безпека цих об'єктів забезпечується, в першу чергу, за рахунок сил і засобів, що маються у держави (коаліції держав) і реалізується за допомогою цілеспрямованої зовнішньої (внутрішньої) політики.

Основними підсистемами безпеки, виходячи з об'єктів захисту, є:

- безпека особистості;
- безпека суспільства;
- безпека держави.

Система безпеки – це продукт конкретного суспільства, в якому відбиваються його специфічні риси. Під час розгляду системи безпеки важливо зрозуміти, що жодна соціальна система не виникає на порожньому місці. Вона використовує матеріал для свого становлення від попередніх систем або систем, що існують поруч з нею. Незважаючи на складність рішення проблеми безпеки, в останні роки у світовій політиці спостерігається тенденція до створення *регіональної,* а в перспективі і *глобальної системи безпеки*.

Для кожного соціального суб'єкта існує певний *набір критичних параметрів життєдіяльності*, порушення яких призводить до самоліквідації суб'єкта (особистості, держави, суспільства, міжнародної організації тощо). Дані критичні параметри характеризують область його життєво важливих інтересів. Для кожного суб'єкта вони будуть різні, але серед них обов'язково буде присутня безпека в тому або іншому вигляді:

для особистості це: умови фізичного розвитку, здоров'я, воля, статок, можливість реалізувати себе та ін.;

для суспільства це: збереження своєї системи цінностей, історична пам'ять, соціокультурна ідентичність та ін.;

для держави це: збереження себе як самостійного суб'єкта зовнішньої і внутрішньої політики.

Національна безпека як система, формується і функціонує в результаті цілого ряду умов об'єктивного і суб'єктивного характеру. До них, як правило, відносяться:

- ❖ рівень економічного і соціально-політичного розвитку суспільства;
- ❖ соціальна стабільність суспільства;
- ❖ матеріальні і людські ресурси;

❖ міжнародний статус країни та інші.

Виходячи з цього, доцільно говорити про наявність цілого ряду чинників, що істотно впливають на безпеку країни.

До *формуючих чинників національної безпеки* відносяться:

- геополітичний;
- соціально-політичний;
- економічний;
- етнонаціональний.

Геополітичним чинником є *сукупність географічних параметрів, які визначають відповідну політику держави стосовно забезпечення її життєво важливих інтересів на певному етапі розвитку*.

Соціально-політичний *чинник* *в безпеці країни виражає механізм і гостроту протікання політичних процесів у суспільстві, рівень його стабільності.*

Економічний чинник є найважливішим у формуванні системи безпеки. Мова йде про взаємозв'язок потенціалу країни з реалізацією своїх інтересів у внутрішній і зовнішній сферах із забезпечення безпеки. Національна безпека й економічна могутність країни нероздільні.

Етнонаціональний чинник зберігає в собі специфіку етнонаціональних протиріч і механізми їхнього розв'язання, які значною мірою виражені соціальною стабільністю та рівнем консолідації суспільства.

Виходячи з розглянутих ознак, слід вважати базовими елементами системи безпеки наступні:

- соціальні процеси і зв'язки в суспільстві;
- соціальні групи людей;
- ідеї як виразники певних потреб і інтересів різних соціальних груп;
- соціальні інститути, що забезпечують безпеку.

Система як цілісне явище може забезпечити безпеку об'єкта, але в той же час жоден з її елементів, як би він не був розвинутий, не дає гарантії захисту.

2. Питання. Види національної безпеки

Основні види безпеки

Політична безпека – це стан захищеності політичних інтересів особи, соціальних груп і держав від внутрішніх та зовнішніх загроз, а також система заходів щодо забезпечення цієї захищеності.

Економічна безпека – визначений рівень розвитку і стану економічної та фінансової системи, при якому гарантовані стабільний соціально-економічний розвиток та стійкість до несприятливих внутрішніх і зовнішніх впливів.

Соціальна безпека є рівнем регулювання соціальних процесів з метою реалізації соціальних пріоритетів, збалансування соціальних пропорцій і недопущення соціальних деформацій, що призводять до соціально-політичної нестабільності та ускладнюють соціально-економічний розвиток держави.

Інформаційна безпека – це рівень захищеності та стійкість основних сфер життєдіяльності (економіки, сфери управління, військової справи тощо) щодо небезпечних, дестабілізуючих інформаційних впливів.

Науково-технологічна безпека – це стан захищеності наукового потенціалу держави, наявних в країні конкурентоспроможних технологій, а також недопущення та усунення наслідків технологічної недосконалості господарської діяльності.

Воєнна безпека – це стан захищеності прав та свобод громадян, базових інтересів та цінностей суспільства і суверенної держави від можливих зазіхань із застосуванням воєнної сили.

Екологічна безпека – це допустимий рівень негативного впливу природних і антропогенних факторів екологічної небезпеки на навколишнє середовище і людину.

Демографічна безпека – захищеність генофонду народу від різних негативних впливів і створення сприятливих умов для його існування, розвитку і самореалізації.

Моделі міжнародної безпеки

1. Однополярна модель безпеки. Однополярна модель передбачає посилення системи НАТО, де провідною країною є США.

2. Союз великих держав. Модель міжнародної безпеки як союз декількох великих держав (“Концерт держав”), які могли б узяти на себе відповідальність за підтримку стабільності у світі.

3. Багатополярна модель (ЄС, США, Китай, Індія, Японія та ін.).

4. Глобальна модель міжнародної безпеки. На думку дослідників, міжнародна безпека може бути дієвою тільки на глобальному рівні, коли всі актори світового товариства беруть участь у її створенні.

Види міжнародної безпеки

1. Колективна безпека. Поняття "колективна безпека" з'явилося у світовому політичному лексиконі та дипломатичної практики ще на межі 1920-30-х рр., коли починалися спроби створити механізм запобігання нової світової війни (в основному на базі Ліги Націй).

Головними елементами колективної безпеки є наявність групи держав, які об'єднані загальною метою захисту себе.

2. Всезагальна безпека. Вперше поняття "всезагальна безпека" з'явилося 1982 році у доповіді Комісії ООН з питань безпеки та роззброєння. Інституційну основу загальної безпеки повинні складати не тільки та не стільки військово-політичні альянси, скільки глобальні організації типу ООН.

3. Кооперційна безпека. Кооперційна безпека віддає перевагу мирним, політичним засобам вирішення спірних питань, в той же час не виключає застосування військової сили.

Системи безпеки

- Глобальна система безпеки.
- Регіональна система безпеки.
- Національна безпека.

Європейська інтеграція України у систему безпеки передбачає:

- у політичному вимірі – це створення надійних механізмів політичної стабільності, демократії та безпеки;
- в економічному вимірі – це шлях модернізації економіки України, залучення іноземних інвестицій і новітніх технологій;
- в соціальному вимірі – забезпечення соціальної стабільності, досягнення високих соціальних стандартів держав – членів ЄС.

Національні інтереси України – *це життєво важливі матеріально-інтелектуальні і духовні цінності українського народу, визначальні потреби суспільства і держави, реалізація яких гарантує державний суверенітет України та її розвиток.*

Завдання на самостійну роботу:

1. Сутність, задачі національної безпеки.
3. Об'єкти національної безпеки.
2. Види національної безпеки.

4. Значення знання концептуальних засад національної безпеки для фахівців Держспецзв'язку.

Питання до самоконтролю:

1. Сутність та задачі національної безпеки.
2. Об'єкти національної безпеки.
3. Види безпеки у сучасному суспільстві.

Семінар 2. Заняття 2/2. Національна безпека як соціальна система

1. Сутність та задачі національної безпеки.
2. Підсистеми безпеки.
3. Об'єкти національної безпеки.
4. Види безпеки у сучасному суспільстві.
5. Рівні безпеки за їхньою масштабністю.
6. Значення знання концептуальних засад національної безпеки для фахівців Держспецзв'язку.

Семінар 3. Заняття 2/3. Національна безпека України: сутність, структура

1. Задачі національної безпеки України.
2. Основні принципи забезпечення національної безпеки України.
3. Пріоритети національних інтересів України.
4. Об'єкти національної безпеки України.
5. Суб'єкти національної безпеки України.
6. Умови достатнього рівня оборонної могутності України.
7. Воєнна організація України.

Рекомендована до теми література

1. Ананьїн В.О., Горлинський В.В., Пучков О.О. Міжнародна безпека та євроатлантична інтеграція України: навч. посіб. Київ: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2020. 231 с.

2. Рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України", Указ Президента України від 14 вересня 2020 року № 37/2022. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 8.02.2024).

РОЗДІЛ ІІ. ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ

Тема 3. Інформаційна безпека як складова національної безпеки держави

Лекція 3. Заняття 3.1. Інформаційна безпека в системі національної безпеки України.

Навчальні питання.

1. Інформаційна безпека: сутність, структура та об’єкти захисту.

2. Суб’єкти та об’єкти інформаційного впливу.

1. Питання. Інформаційна безпека: сутність, структура та об’єкти захисту

За час свого існування людство пережило багато інформаційних революцій, вони стали причиною перетворень суспільних відношень через значні зміни у сфері обробки інформації.

З кожним роком інформаційні системи ускладнюються, інформаційна безпека й політика набувають все більш глобального характеру. У XXI ст. виникло багато проблем, пов’язаних з інформаційною безпекою.

Головною умовою роботи службовця Держспецзв’язку повинні бути знання про інформаційну безпеку, її структурні складові та критерії.

Інформація – це не тільки товар, а й інструмент маніпуляції суспільством, думкою громадян, створенню конфліктів. Отже, як людина потребує захисту від інформації, так і інформація потребує захисту від людини.

*Особливо зростає роль інформаційної безпеки **(ІБ)*** у сфері високих технологій, бо саме цифрова інформація стає одночасно і сировиною, і продуктом, що виробляють, обробляють, продають та, на жаль, частіше крадуть.

У науковій літературі відсутній єдиний погляд на зміст поняття “інформаційна безпека”. Існує необхідність уточнення поняття **ІБ,** яке сприятиме осмисленню перспективних змін інформаційної безпеки та дозволить повніше розкрити її зміст та надання йому більш широкого й системного характеру.

Розглянемо основні поняття, визначення і терміни.

Інформація (від латинського слова "informacio" – роз'яснення, виклад) – це відомості (або їх сукупність) про предмети, явища і процеси оточуючого нас світу.

Однією з перших є статистична теорія інформації, розроблена ***К. Шенноном*** і викладена в серії його робіт у **1948** році. Саме він ввів термін "інформація", яку розумів у вузькому технічному аспекті.

Отже, під інформацією нині розуміють:

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

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

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

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

Властивості інформації:

- об'єктивність;
- повнота;
- актуальність;
- доступність;
- достовірність;
- корисність;
- зрозумілість.

Види інформації (Закон України "Про інформацію"):

❖ *статистична інформація* – офіційна документована державна інформація, що дає кількісну характеристику подій та явищ;

❖ *масова інформація* – публічно поширювана друкована та аудіовізуальна інформація;

❖ *інформація про діяльність державних органів влади та органів місцевого і регіонального самоврядування*;

❖ *правова інформація* – сукупність документованих або публічно оголошених відомостей про право;

❖ *інформація про особу* – сукупність документованих або публічно оголошених відомостей про особу;

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

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

❖ *екологічна інформація;*

❖ *інформація про товар (роботу, послугу);*

❖ *науково-технічна інформація;*

❖ *податкова інформація.*

Інформаційна безпека є складовою національної безпеки. Але особливістю інформаційної безпеки є те, що вона, як невід'ємна частина, входить до інших складових національної безпеки: економічної, воєнної, політичної безпеки тощо.

Роль інформаційної безпеки та її місце в системі національної безпеки держави стає все значнішою. Це відбувається внаслідок таких чинників:

- національні інтереси, загрози їм і забезпечення захисту від цих загроз у всіх галузях національної безпеки виражаються, реалізовуються і здійснюються через інформацію та інформаційну сферу;
- особа та її права, інформація та інформаційні системи і права на них - це основні об'єкти не тільки інформаційної безпеки, а й основні елементи всіх об'єктів безпеки в усіх її галузях;
- вирішення завдань національної безпеки пов'язане з використанням інформаційно-комунікаційних засобів та технологій, як основних на сучасному етапі;
- проблема національної безпеки має яскраво виражений інформаційний характер.

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

Інформаційна безпека – *Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні*

наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації. (Закон України "Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" від 09.01.2007 р. № 12, ст. 13).

Основні об'єкти ІБ:

- ❖ особистість;
- ❖ суспільство;
- ❖ держава.

Суб'єкти забезпечення інформаційної безпеки:

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

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

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

Види інформаційної безпеки:

– особиста (безпека конкретної особи);

– суспільна (безпека суспільства);

– державна (безпека окремої держави);

– міжнародна (безпека багатьох держав, світового співтовариства загалом).

Інформаційна безпека особи – це стан захищеності психіки та здоров'я людини від деструктивного інформаційного впливу, який призводить до неадекватного сприйняття нею дійсності та (або) погіршення її фізичного стану.

Інформаційна безпека суспільства – можливість безперешкодної реалізації суспільством та окремими його членами своїх конституційних прав, пов'язаних із можливістю вільного одержання, створення й поширення інформації, а також ступінь їхнього захисту від деструктивного інформаційного впливу.

Інформаційна безпека держави. Серед головних складових інформаційної безпеки держави виділяють:

- ✓ обсяг інформаційного продукту, що виробляється в державі і державою;
- ✓ здатність мереж витримувати зростаюче інформаційне навантаження;
- ✓ можливість держави керувати розвитком вироблення та розповсюдження інформації;

✓ можливість доступу народонаселення до усіх можливих інформаційних джерел, а також відкритість більшості з них.

Слід зазначити, що інформаційна безпека особи, суспільства та держави тісно пов'язані між собою. Інформаційна безпека суспільства та його окремих осіб залежить від рівня:

- інтелектуальності, спеціальної теоретичної й практичної підготовки;
- критичного мислення, морального і духовного вдосконалення;
- гармонійного розвитку особи в суспільстві;
- технічних засобів захисту.

Принципи забезпечення інформаційної безпеки:

- законність;
- баланс інтересів особи, суспільства і держави;
- системність;
- єдиноначальність;
- права власності в процесі забезпечення інформаційної безпеки;
- науковий підхід до організації;
- комплексний підхід;
- безперервність;
- інтеграція з міжнародними системами безпеки;
- економічна ефективність.

Функції забезпечення ІБ:

❖ розробка методів аналізу загроз, оцінки рівня інформаційної безпеки і систем її забезпечення;

❖ організація і здійснення діяльності із захисту інформації;

❖ експлуатація технічних засобів захисту інформації;

❖ аудит і контроль функціонування системи інформаційної безпеки.

Шляхи розв'язання проблеми інформаційної безпеки

❖ створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів; підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань;

❖ удосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії

комп’ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;

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

Державним органом, діяльність якого пов’язана із забезпеченням кібербезпеки в Україні і який призначений для забезпечення функціонування і розвитку державної системи урядового зв’язку, Національної системи конфіденційного зв’язку, формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, електронних комунікацій, є ***Державна служба спеціального зв’язку та захисту інформації України***.

Відповідно до ст. 31 Закону України Про електронні комунікації, від 16.12.2020 р., № 1089-IX, визначено норми права щодо *забезпечення безпеки електронних комунікаційних мереж, як складової інформаційної безпеки*.

Безпека мереж і послуг, відповідно до ст. 2 Закону, – це здатність електронних комунікаційних мереж і послуг протистояти діям, що становлять загрозу доступності, цілісності чи конфіденційності таких мереж і послуг, а також даних, що зберігаються, передаються чи обробляються, та пов’язаних із ними послуг, що надаються або доступ до яких здійснюється через електронні комунікаційні мережі чи послуги

2. Суб’єкти та об’єкти інформаційного впливу

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;
- можливість нанесення збитку інтересам безпеки.

Небезпека обмежується наявністю тільки одного з цих компонентів.

Загроза має персоніфікований, конкретно адресний характер, що припускає наявність очевидних суб’єкта (джерела) загрози і об’єкта, на який

спрямовано її дію. *На відміну від загрози небезпека носить гіпотетичний, часто безадресний характер, її суб'єкт і об'єкт явно не виражені.*

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;
- порушується нормальне функціонування, здійснюється руйнація або стримується розвиток технічних об'єктів інформаційної безпеки.

Загрози інформаційній безпеці поділяють на два види:

- соціальні (обмеження чи неспроможність особи та суспільства загалом реалізувати ключові інтереси в інформаційній сфері);
- технічні (порушення функціонування та виведення з ладу інформаційної інфраструктури та інформаційних ресурсів зокрема).

Фахівці з інформаційної безпеки пропонують декілька підходів до класифікації загроз інформаційній безпеці.

Їх можна поділити на такі основні групи:

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

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

– загрози обмеженню інформаційних прав особистості, механізмам їх реалізації.

Відповідно до іншого підходу виділяють декілька типів інформаційних загроз, серед яких політичні, економічні, суспільні, військові та науково-технічні. *Є й інші підходи до класифікації загроз інформаційній безпеці.*

Носіями загроз безпеці інформації є джерела загроз.

Джерелами загроз можуть виступати:

– суб'єкти (особистість, група, організація, держава);

– об'єктивні прояви.

Причому, джерела загроз можуть бути:

– всередині держави – внутрішні джерела;

– 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).

Суб'єктами забезпечення інформаційної безпеки є:

- Президент України.
- Верховна Рада України.
- Кабінет Міністрів України.
- Національний банк України.
- Державний комітет телебачення і радіомовлення України.
- Визначені законодавством центральні органи виконавчої влади, державні адміністрації та органи місцевого самоврядування.
- Прокуратура України та інші органи охорони правопорядку, судові органи, які віднесені до суб'єктів забезпечення національної безпеки України.
- Центральний орган виконавчої влади зі спеціальним статусом з питань інформаційної безпеки.
- Державна служба спеціального зв'язку та захисту інформації України.
- Служба безпеки України.
- Служба зовнішньої розвідки України.
- Державна прикордонна служба України.
- Збройні Сили України та інші військові формування, утворені відповідно до законів України.
- Державні і недержавні засоби масової інформації, підприємства, заклади, установи та організації різних форм власності, що здійснюють інформаційну діяльність.
- Наукові установи і навчальні заклади України, які здійснюють наукові дослідження та підготовку фахівців за різними напрямами інформаційної діяльності, в галузі інформаційного права та інформаційної безпеки.
- Громадяни України та інші особи, за їх згодою, громадські організації та інші інститути громадянського суспільства.

Завдання на самостійну роботу

1. Стратегія формування єдиного інформаційного простору держави.
2. Інформаційна політика держави.
3. Геополітичні особливості сучасного інформаційного простору.
4. Стратегія розвитку єдиного інформаційного простору України.

Питання до самоконтролю

1. Інформаційна безпека в системі національної безпеки держави.

2. Геополітичні особливості сучасного інформаційного простору.

3. Інформаційна безпека держави: сутність, задачі.

4. Структура інформаційної безпеки держави.

5. Діяльність спецслужб України у сфері забезпечення ІБД.

Семінар 3. Заняття 3.2. Інформаційна безпека держави: сутність, структура.

Навчальні питання.

1. Інформаційна безпека в системі національної безпеки держави.

2. Інформаційна безпека держави: сутність, задачі.

3. Стан інформаційної безпеки держави.

4. Структура інформаційної безпеки держави.

5. Об’єкти інформаційної безпеки держави.

6. Суб’єкти забезпечення інформаційної безпеки держави.

Семінар 4. Заняття 3.3. Інформаційна безпека України (ІБУ).

Навчальні питання.

1. Геополітичні особливості сучасного інформаційного простору.

2. Основні задачі забезпечення інформаційної безпеки України.

3. Життєво важливі інтереси в інформаційній сфері України.

4. Об’єкти захисту інформаційної безпеки України.

5. Основні групи загроз ІБУ.

6. Основні принципи забезпечення ІБУ.

7. Система функції забезпечення ІБУ.

8. Діяльність спецслужб України у сфері забезпечення ІБД.

Семінар 5. Заняття 3.4. Стратегія формування та розвитку єдиного інформаційного простору України.

Навчальні питання.

1. Єдиний інформаційний простір України: сутність, значення.

2. Стратегія формування єдиного інформаційного простору держави.

3. Засоби масової інформації як засіб впливу на інформаційний простір.

4. Протидія діяльності зарубіжних державних та недержавних організацій інформаційному впливу.

5. Структура інформаційного впливу.

6. Об’єкти інформаційного впливу.

7. Діяльність спецслужб України у сфері забезпечення ІБД.

Рекомендована до теми література

1. Інформаційна безпека: підручник /В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін; під. ред. В. В. Остроухова. Київ: Вид-во Лира-К, 2021. 412 С.

2. Золотар О. О. Інформаційна безпека людини: теорія і практика: монографія. Київ : ТОВ Видавничий дім “АртЕк”, 2018. 446 с. URL: http://ippi.org.ua/sites/default/files/informaciyna_bezpeka_lyudini_print.pdf (дата звернення: 29.06.2024).

3. Мужанова Т. М. Інформаційна безпека держави: навч. посіб. Київ: ДУТ, 2019. 131 С. URL: https://nubip.edu.ua/sites/default/files/u34/posibnik_ibd_muzhanova_2019.pdf (дата звернення: 04.01.2024).

4. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року “Про Стратегію інформаційної безпеки”. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text . (дата звернення: 29.06.2024).

5. Про інформацію : Закон України від 02 жовтня 1992 року № 2658-XII Верховна Рада України. Відомості Верховної Ради України. 1992. № 48. URL: https://zakon.rada.gov.ua/laws/show/2657-12Text (дата звернення 13.05.2024).

6. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017, № 2163-VII. URL: https:// https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 14.02.2024).

7. Про електронні комунікації. Закон України, від 16.12.2020 р., № 1089-IX, URL: https://zakon.rada.gov.ua/laws/show/1089-20#n2246 (дата звернення 13.05.2024).

8. Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки. Закон України від 09.01.2007. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text (дата звернення 13.05.2024).

Тема 4. Гендерні аспекти інформаційної безпеки.

Лекція 4. Заняття 4.1. Гендерні аспекти інформаційної безпеки.

Навчальні питання.

1. Питання. Гендерні стереотипи та комунікативні моделі у сучасному суспільстві.

2. Питання. Гендерні особливості інформаційного впливу.

1. Питання. Гендерні стереотипи та комунікативні моделі у сучасному суспільстві

У науковий обіг поняття "гендер" першим ввів американський психолог **Роберт Столлер** у 1968 році. Культурні й соціальні аспекти статевої ідентичності Р. Столлер назвав словом "гендер".

Поняття "гендер" остаточно ввійшло в науковий дискурс у 80-х роках минулого століття.

Гендер є загальнонауковою категорією, принципи гендерного аналізу можуть бути використані у будь-якій з наукових дисциплін.

Гендер – один із базових вимірів соціальної структури суспільства, який разом з іншими соціально-демографічними та культурними характеристиками (раса, клас, вік) організовує соціальну систему.

Гендер – *це сукупність соціальних та культурних норм, які суспільство наказує виконувати людям залежно від їхньої біологічної статі.*

Гендерна соціалізація – це процес засвоєння людиною соціальної ролі, визначеної для неї суспільством від народження, залежно від того, чоловіком чи жінкою вона народилась.

Гендерні ролі – норми та правила поведінки жінок і чоловіків в суспільстві.

Соціальна комунікація, сучасні технології й способи маніпулювання свідомістю в сучасному суспільстві мають явний або схований гендерний компонент.

Гендерні відносини фіксуються у вигляді культурно обумовлених стереотипів.

Гендерні стереотипи – *уявлення про соціальні ролі чоловіків і жінок.*

У сучасних інтернет-ресурсах багато уваги приділяється гендерній проблематиці а саме, службі жінок в армії та ін.

Гендерна культура – *це система уявлень, які формують соціокультурні аспекти статі, визначають їхні ролі й моделі поведінки у різних сферах життя.*

Гендерна культура виконує наступні функції:

- *світоглядну,*
- *аксіологічну,*
- *нормативно-регулятивну,*
- *адаптаційну,*
- *гуманістичну,*
- *комунікативну,*
- *виховну* та ін.

Зміст гендерної культури як соціального явища суспільного життя розкривається у забезпеченні умов для всебічного розвитку особистості, гармонійної соціалізації, самореалізації, гуманізації людини й суспільства.

Цінностями гендерної культури (знання, уміння, навички вихованців) є:

❖ гендерна грамотність, як система отримання необхідних знань у сфері гендерних досліджень;

❖ сформована мотивація до рівноправної участі чоловіків і жінок у суспільному житті та реалізації своїх гендерних прав і свобод;

❖ гендерна самоосвіта, як набуття власного досвіду з гендерної збалансованості;

❖ гендерна чуйність, як здатність особистості усвідомлювати та моделювати вплив соціального середовища;

❖ повага до особливостей та індивідуальних проявів особистості незалежно від її статі.

Гендерні стереотипи в контексті інформаційного впливу представлено *гендерними схемами* (*Сандра Бем 1981*), які відкладаються у свідомості людей.

Гендерні схеми

- **Праймінг** (фіксована установка);
- **Схема власної статі –** схема, що складається зі сценаріїв дій, які відповідають гендеру;
- **Ефект стійкості** – полягає в тому, що якщо людина навіть і запам’ятає інформацію, яка суперечить схемі, це ще не означає, що вона обов’язково змінить свої стереотипи;

- **Ілюзорна кореляція** – перебільшений зв’язок між гендером і певними властивостями;
- **Помилка обґрунтування оцінки** – тенденція не звертати уваги на порівняно часті випадки з реального життя.

Комунікація – *обумовлений процес передачі й сприйняття інформації за умов міжособистісного й масового спілкування через канали з допомогою різноманітних комунікативних засобів.*

Основна модель комунікації, створена Аристотелем ще у IV столітті до Н. Х. структура моделі мала такий вигляд: *"оратор – мова – аудиторія"*.

Нині дуже багато моделей комунікації.

Основні комунікаційні моделі

Модель Лассуела

Одним з перших, хто зайнявся питанням дослідження сучасної комунікації, був американський політолог Гарольд Лассуелл. У 1948 році він представив абсолютно нову модель комунікації, що складається з 5W (п’яти елементів масової комунікації):

- ✓ джерело інформації;
- ✓ інформація;
- ✓ спосіб передачі інформації;
- ✓ одержувач інформації;
- ✓ ефект комунікації.

Модель була заснована на досвіді ведення пропаганди у військових підрозділах під час Другої світової війни.

Модель Шеннона-Уивера

Комунікативний процес у даній моделі носить лінійний, односпрямований характер, зворотний відсутній, значну увагу приділяють не якості, а кількості інформації. Вона відбиває переважно технічні способи комунікації, а людина входить у неї лише як "джерело" чи "приймач" інформації.

Модель Дефлюера

У моделі Дефлюера враховано основний недолік лінійної моделі Шеннона-Уивера – відсутність чинника зворотний зв’язок. Він замкнув ланцюжок прямування інформації джерела до мети лінією зворотний зв’язок,

що повторює весь шлях у напрямку, включаючи трансформацію значення під впливом "шуму".

Ця модель є першою, яка впроваджує у комунікаційний процес, як двосторонній зворотний зв'язок, так і цільову аудиторію.

Модель Осгуда-Шрама

У цій моделі відображена реакція комуніканта на повідомлення джерела, як зворотний зв'язок. Саме зворотний зв'язок робить комунікацію двостороннім процесом (діалогом), дозволяючи кожній із сторін коригувати свої дії та цілі.

У даній моделі наголошено на необхідності виконання учасниками комунікації трьох взаємопов'язаних процесів: кодування, декодування та інтерпретація повідомлення, без чого процес комунікації не може вважатися таким, що відбувся.

Модель Лазарсфельда

Це модель двоступеневого потоку комунікації. В результаті досліджень було встановлено, що немає прямого впливу на аудиторію. Вплив на аудиторію опосередковується міжособистісною комунікацією, тобто від засобів масової комунікації ідеї поширюються до "лідерів думок", а вже через них – до всієї аудиторії.

Подальший розвиток цієї моделі пов'язаний з виявленням "факторів-посередників", спираючись на те, як відбувається вплив на людину.

Модель Романа Якобсона

У моделі Якобсона беруть участь адресант і адресат, від першого до другого надсилається повідомлення, яке реалізовано за допомогою коду. Контекст пов'язаний зі змістом повідомлення, поняття контакту – з регулятивним аспектом комунікації.

У сучасному суспільстві широко діє модель *Лазарсфельда.*

2. Питання. Гендерні особливості інформаційного впливу

На сьогодні інформаційно-комунікаційні технології створюють унікальні можливості для виявлення та розвиток людського потенціалу. Вони здійснюють значний вплив на сталий розвиток суспільства, розширення можливостей чоловіків і жінок, а також дозволяють останнім брати активну участь у

суспільному житті і соціально-економічному розвитку країни, висловлювати свої думки та активно пропагувати свою життєву позицію.

Завдяки технічним можливостям інформаційного обміну мережі Інтернет останніми роками активно використовуються для залучення світової спільноти до жіночих проблем, досягнення фактичної рівності.

Наприклад, створюючи веб-сайти (сторінки) тієї або іншої жіночої організації або лідера жіночого руху, можна отримати додаткові можливості для мобілізації добровольців, які готові надати підтримку тим або іншим соціальним акціям, для збору фінансової допомоги недержавним організаціям і жіночим рухам, для проведення маркетингових операцій на соціальному ринку з метою пошуку своєї ніші.

На сьогодні завдяки використанню найважливішого демократизуючого аспекту – Інтернету, створенню безпечних інтерактивних просторів, захищених від несанкціонованого доступу, жінки можуть вільно висловлювати свою думку і конфіденційно обмінюватися інформацією в цілях боротьби з дискримінацією за статевою ознакою, заохочення прав людини і жінок.

Відзначимо, що розвиток інформаційних та телекомунікаційних технологій чинить серйозну дію на розповсюдження та діяльність жіночих рухів в галузі інформації та комунікації. Зросли можливості для поширення на державному, національному, регіональному і глобальному рівнях новинної інформації, що надається жінкам, велика частина якої у минулому була обмеженою за ступенем охоплення. Гендерний фактор поширюється на все більш широкий простір комунікації.

Дослідження гендерних особливостей технологій інформаційно-психологічного впливу в сучасному суспільстві дозволяє зробити наступні висновки.

1. Гендерні теорії належать сьогодні до пріоритетної галузі наукових досліджень.

2. Інформаційна безпека в сучасному суспільстві неможлива без обліку гендерного компонента інформаційної діяльності.

3. У комунікативному просторі сучасного суспільства відбувається переосмислення гендерних стереотипів.

4. У сфері соціально-правових основ інформаційної безпеки формується нова гендерна парадигма.

5. Інтернет-ресурси є відображенням гендерної ситуації в суспільстві.

6. Категорія "гендер" має певну специфічність в Інтернет-комунікації.

Засоби масової інформації не лише інформують суспільство про події, але й створюють, підтримують, а інколи й спростовують стереотипні уявлення про моделі поведінки чоловіків і жінок в різних життєвих сферах – спілкуванні, кар'єрі, родинних та службових стосунках.

З огляду на це, образи жінок і чоловіків, поширювані в медіа, неодноразово аналізувались гендерними дослідниками в різних ракурсах та контекстах. Як показують результати досліджень, найпопулярнішими соціальними образами жінок, наявними в гендерному дискурсі друкованих ЗМІ, є жінка-мати – 19%, жінка-сексуальна подруга – 17%, працівниця – 13%, активістка – 12% та жінка-політик – 10%.

За результатами згаданих досліджень, такими образами є чоловік батько, бізнесмен, маргінал, зірка, спортсмен, красень, професіонал, експерт, сексуальний друг (партнер), творець, політик, хворий та працівник.

Завдання на самостійну роботу

1. Гендерні особливості інформаційного впливу.
2. Роль інтернет-ресурсів у популяризації гендерної проблематики.

Питання до самоконтролю

1. Гендерні стереотипи та комунікативні моделі.
2. Гендерні особливості інформаційного впливу.

Семінар 6. Заняття 4.2. Гендер в епоху інформаційного суспільства.

Навчальні питання.

1. Гендер: становлення наукової галузі в сучасному суспільстві.
2. Гендерні стереотипи та комунікативні моделі.
3. Гендерні особливості інформаційного впливу.
4. Роль інтернет-ресурсів у популяризації гендерної проблематики.
5. Питання гармонізації гендерних відносин в сучасному українському суспільстві.
6. Гендерна культура особистості фахівця: сутнісні аспекти.
7. Особливості соціалізації жінок у воєнній сфері суспільства.

Рекомендована до теми література

1. Гендерний розвиток у суспільстві: конспект лекцій. Київ: ПЦ “Фолізит”, 2005. 351с.

2. Путівник ґендерної інтеграції у Збройних силах України : Формування ґендерної компетентності військового професіонала / Укладачі: В. Арнаутова, В. Лукічов, Т. Нікітюк. 2020. 228 с. https://www.osce.org/uk/project-coordinator-in-ukraine/479044 (дата звернення 29.06.2024).

3. Інформаційна безпека (соціально-правові аспекти): підручник. / Остроухов В. В., Петрик В. М. Присяжнюк М. М. та ін.; за заг. ред. Є. Д. Скулиша. Київ: КИТ, 2010. 776 с.

4. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / за заг. ред. В. Б. Толубка. Київ: ДУТ, 2015. 288 с.

5. Самчук Р. Постмодерні виміри гендерної ідентичності / Р. Самчук //Наукові записки Національного університету “Острозька академія”. 2014. Вип. 15(2). С. 311-315.

6. Методичні рекомендації з інтеграції ґендерних підходів у систему підготовки фахівців для сектору безпеки і оборони України. https://ukraine.unwomen.org/uk/digital-library/publications/2021/11/guidelines-on-integrating-gender-approaches-in-training-specialists (дата звернення 26.05.2024).

7. Збірник інформаційно-методичних матеріалів Каллум Уотсон “Гендерні питання в секторі безпеки” Центр ДКЗС, ОБСЄ/БДІПЛ, ООН Жінки. URL: https://www.osce.org/files/f/documents/a/b/468957.pdf (дата звернення 29.06.2024).

РОЗДІЛ ІІІ. ЗАГРОЗИ БЕЗПЕЦІ ДЕРЖАВИ, СУСПІЛЬСТВУ, ЛЮДИНІ В ІНФОРМАЦІЙНІЙ СФЕРІ

Тема 5. Загрози національній безпеці держави в інформаційній сфері.

Лекція 5. Заняття. 5.1. Поняття та види загроз безпеці держави в інформаційній сфері.

Навчальні питання.

1. Загальна характеристика зовнішніх та внутрішніх загроз в інформаційній сфері

2. Інформаційна зброя.

3. Спеціальні інформаційні операції (СІО).

1. Питання. Загальна характеристика зовнішніх та внутрішніх загроз в інформаційній сфері

В умовах глобальної інтеграції та жорсткої міжнародної конкуренції ареною боротьби інтересів держав стає інформаційний простір.

Сучасні інформаційні технології дають змогу державам реалізовувати власні інтереси без застосування воєнної сили або завдавати значної шкоди безпеці конкурентної держави.

Розвиток глобального процесу інформатизації суспільства породило нову глобальну соціотехнологічну проблему – проблему інформаційної безпеки людини, суспільства, держави.

Комплексний характер загроз безпеки в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту інформаційного простору в умовах вільного обігу інформації.

Актуальні загрози національній безпеці України в інформаційній сфері визначені в наступних документах:

- ❖ Стратегія національної безпеки України (*Указ Президента України від 14 вересня 2020 року № 392*);
- ❖ Доктрина інформаційної безпеки України (*Указ Президента України від 28 лютого 2017 року № 47/2017*);
- ❖ Стратегія інформаційної безпеки. (*Указ Президента України від 28 грудня 2021 року № 685/2021*).

Інформаційна загроза – *потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою ускладнення реалізації національних інтересів України.*

Загрози, як правило, мають комплексний характер, відтак їхні прояви дуже різноманітні.

Зовнішні загрози залежать передусім від незалежних і неконтрольованих факторів, на які важко вплинути, тому досягти такого стану, в якому б цих загроз не було, практично неможливо. Також важко скласти список усіх загроз "на всі часи", оскільки вони змінюються, а ще частіше приховуються.

Зовнішні загрози в інформаційній сфері:

- здійснення спеціальних інформаційних операцій спрямованих на дестабілізацію суспільно-політичної та соціально-економічної ситуації в країні;
- проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі;
- інформаційна експансія державою-агресором та контрольованих нею структур;
- інформаційне домінування держави-агресора на тимчасово окупованих територіях.

Внутрішні загрози в інформаційній сфері:

- недостатня розвиненість національної інформаційної структури;
- неефективність державної інформаційної політики;
- недостатній рівень медіа-культури суспільства;
- недостатній рівень медіаграмотності (медіакультури) в умовах стрімкого розвитку цифрових технологій;
- поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів.
- обмежені можливості реагувати на дезінформаційні кампанії;
- несформованість системи стратегічних комунікацій;
- низька спроможність забезпечення населення послугами з доступу до Інтернету.

2. Питання. Інформаційна зброя

За останні 15 років витрати США на розробку і придбання засобів інформаційного протиборства виросли в 4 рази і займають нині перше місце серед витрат на всі військові програми.

Інформаційна зброя – *сукупність технік і технологій інформаційного впливу на інформаційну інфраструктуру та інформаційне поле певної території чи держави, на психіку, свідомість її населення задля дестабілізації інформаційного простору з подальшим нанесенням шкоди суспільно-політичній системі та збройним силам.*

Ознаки інформаційної зброї:

- прихованість – досягнення мети без привернення до себе уваги;
- масштабність – поширення шкоди на будь-які території та сфери життєдіяльності;
- універсальність – одні й ті самі техніки та технології використовуються для знищення як військових, так і цивільних структур.

Об'єктами інформаційної зброї є комп'ютерні системи, системи зв'язку, засоби масової інформації та психіка людини.

За об'єктами впливу інформаційну зброю поділяють на класи:

- *інформаційно-технічний* – зброя, що впливає на цивільну, державну та військову інформаційну інфраструктуру;
- *інформаційно-психологічний* – зброя, що впливає на морально-психологічний стан окремої особистості, групи людей і суспільства в цілому.

Інформаційно-технічну зброю розрізняють, як:

- алгоритмічну;
- програмну;
- апаратну.

Інформаційну алгоритмічну зброю використовують для виведення з ладу або зміни алгоритму функціонування програмного забезпечення інформаційних систем, ресурсів і мереж.

Інформаційна програмна зброя – шкідливі програми, призначені для руйнування та спотворення кодів інших програм, блокування й підміни масивів інформації, а також нейтралізації тестових програм і систем захисту інформаційних ресурсів.

Інформаційна апаратна зброя здатна до тимчасового або повного виведення з ладу окремих компонентів радіоелектронних систем і джерел їхнього живлення, дезорганізації обміну інформації в межах певного середовища розповсюдження сигналів, а також прихованого збору інформації внаслідок її перехоплення.

Інформаційно-психологічну зброю поділяють на:

✓ *пропагандистську* – поширення дезінформації, фейків, запуск медіавірусів, що спотворюють реальність, підмінюють її новою, сконструйованою ворогом;

✓ *психогенну* – фізичний вплив на мозок людини звуком, кольором, зовнішніми обставинами, що дезорієнтує її;

✓ *психоаналітичну* – вплив на підсвідомість людини терапевтичними засобами, що програмує на потрібні ворогу вчинки чи поведінку;

✓ *нейролінгвістичну* – використання спеціальних лінгвістичних програм, спрямованих на зміну емоційно-вольового стану і світогляду особистості;

✓ *психотропну* – застосування медичних препаратів, хімічних або біологічних речовин задля зміни біохімічних характеристик процесів, що перебігають у нервовій системі людини.

3. Питання. Спеціальні інформаційні операції (СІО)

Спеціальні інформаційні операції (СІО) – *сплановані дії, спрямовані на ворожу, дружню або нейтральну аудиторію, які передбачають вплив на її свідомість і поведінку за допомогою використання організованої інформації та інформаційних технологій для досягнення певної мети.*

Види СІО:

- операції, спрямовані проти суб’єктів, які ухвалюють рішення;
- операції, спрямовані на компрометацію, завдання шкоди опонентам;
- операції, спрямовані на економічну чи політичну дестабілізацію.

Термін проведення СІО:

- довгостроковий (більш місяця);
- середньостроковий (два-чотири тижні);
- короткостроковий (один-два тижні).

Основні методи СІО:

❖ *Дезінформування* (передбачає обман чи введення об'єкта СІО в оману щодо справжності намірів).

Форми дезінформування:

- тенденційне викладення фактів;
- дезінформування "від зворотнього";
- термінологічне "мінування";
- "сіре" дезінформування.

❖ *Пропаганда*

Форми проведення пропаганди:

- пропаганда способу життя (соціологічна) – показ досягнень, перспектив тощо конкретної держави;
- використання ЗМІ та друкованих наукових і художніх видань;
- коректування існуючих думок, формулювання та створення нових ("резонансна").

❖ *Диверсифікація громадської думки*

Форми диверсифікації громадської думки:

- дестабілізація обстановки в державі чи окремих її регіонах;
- активізація різними міжнародними установами кампанії проти політичного курсу правлячої еліти держави та окремих її лідерів;
- ініціювання антидемпінгових кампаній та іншого роду скандальних судових процесів, застосування міжнародних санкцій з інших причин.

❖ *Психологічний тиск*

Форми психологічного тиску:

- доведення до об'єкта відомостей про реальні чи неіснуючі загрози та небезпеки;
- прогнози щодо репресій, переслідувань, убивств тощо;
- шантаж;
- здійснення вибухів, підпалів, масових отруєнь, захоплення заручників, інші терористичні акти.

❖ *Поширення чуток.*

Класифікація чуток:

- експресивні (емоційні стани, пов'язані зі змістом чутки, і відповідні типи емоційних реакцій);

- інформаційні (ступінь вірогідності сюжету чутки);
- за ступенем впливу на психіку людей.

Етапи СІО.

1. *Інформаційний етап* створення інформаційного приводу – конкретної або вигаданої події, яка використовується в СІО.

2. *"Розкручування" інформаційного приводу* – поступове зростання напруження.

3. *Загострення напруження*, що є основною частиною СІО (полягає у досягненні цілей операції).

4. *Вихід із операції / етап закріплення* – забезпечення плавного завершення СІО після досягнення поставленої мети.

Завдання на самостійну роботу.

1. Інформаційна зброя, особливості та класифікація.
2. Інформаційна війна.
3. Спеціальні інформаційні операції в інформаційній політиці.

Питання до самоконтролю.

1. Інформаційна зброя, особливості та класифікація.
2. Інформаційна війна.
3. Спеціальні інформаційні операції в інформаційній політиці.

Семінар 7. Заняття. 5.2. Загрози безпеки держави в інформаційній сфері.

Навчальні питання.

1. Загальна характеристика зовнішніх загроз держави.
2. Загальна характеристика внутрішніх загроз держави.
3. Спеціальні інформаційні операції в інформаційній політиці.
4. Класифікація психологічних операцій.

Семінар 8. Заняття. 5.3. Інформаційна зброя, особливості та класифікація.

Навчальні питання.

1. Інформаційний простір, як театр сучасних воєнних дій.
2. Класифікація сучасної інформаційної зброї.
3. Основні показники та особливості інформаційної зброї.
4. Види інформаційної зброї.
5. Основні способи й методи застосування інформаційної зброї.

Семінар 9. Заняття. 5.4. Інформаційна війна: сутність і зміст.

Навчальні питання.

1. Сутність та задачі інформаційної війни.

2. Об’єкти посягань інформаційної війни.

3. Сучасні теоретичні підходи до використання понять “інформаційна боротьба” та “інформаційна війна”.

4. Види інформаційної боротьби.

5. Форми інформаційної війни.

Рекомендована до теми література

1. Інформаційна безпека: підручник. / В. В. Остроухов, М. М. Присяжнюк, О.І. Фармагей та ін.; під. ред. В. В. Остроухова. Київ: Видавництво Ліра, 2021. 412с.

2. Інформаційна безпека (соціально-правові аспекти): підручник. / Остроухов В. В., Петрик В. М. Присяжнюк М. М. та ін.; за заг. ред. Є. Д. Скулиша. Київ: КИТ, 2010. 776 с.

3. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В . Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. В. Б. Толубка. Київ: ДУТ, 2015. 288 с.

4. Левченко О. В. Класифікація інформаційної зброї за засобами ведення інформаційної боротьби. /Сучасні інформаційні технології у сфері безпеки та оборони. 2014. № 2. С. 142–146.

ІНСТИТУТ ПЕРСПЕКТИВНОГО ВИВЧЕННЯ ІНФОРМАЦІЙНИХ ВІЙН (IASIW)

https://web.archive.org/web/20070709005214/http://www.psycom.net/iwar.1.html

Тема 6. Загрози людині та суспільству в інформаційній сфері.

Лекція 6. Заняття 6.1. Загрози особистісній безпеці від деструктивних інформаційних впливів.

Навчальні питання.

1. Інформаційно-психологічна безпека особи.

2. Характеристика інформаційно-психологічного впливу.

1. Питання. Інформаційно-психологічна безпека особи

Одне із головних завдань сучасної держави – гарантування інформаційної безпеки особи, яка характеризується захищеністю її психіки та свідомості від небезпечних інформаційних впливів: маніпулювання, дезінформування, образ, спонукання до самогубства тощо.

Інформаційна безпека особистості – *це стан людини, в якому його особистості не може бути завдано істотної шкоди шляхом здійснення впливу на навколишній інформаційний простір.*

Під інформаційно-психологічною безпекою *розуміють стан захищеності громадян, окремих груп та соціальних верств, масових об'єднань людей і населення загалом від негативних інформаційно-психологічних впливів.*

Інформаційно-психологічна безпека особистості *– це захищеність психіки й свідомості людини від небезпечних інформаційних впливів: маніпулювання свідомістю, дезінформування, спонукання до образ, самогубства тощо.*

Інформаційно-психологічна безпека особи (у вузькому розумінні) – *це стан захищеності психіки людини від негативного впливу, який здійснюється шляхом упровадження деструктивної інформації у свідомість і (або) у підсвідомість людини, що призводить до неадекватного сприйняття нею дійсності.*

Інформаційно-психологічна безпека особи (в широкому розумінні) – це:

по-перше, належний рівень теоретичної та практичної підготовки особистості, за якого досягається захищеність і реалізація її життєво важливих інтересів та гармонійний розвиток незалежно від наявності інформаційних загроз;

по-друге, здатність держави створити умови для гармонійного розвитку й задоволення потреб особистості в інформації незалежно від наявності інформаційних загроз;

по-третє, гарантування, розвиток і використання інформаційного середовища в інтересах особистості;

по-четверте, захищеність від різного роду інформаційних небезпек.

Об'єктом *інформаційно-психологічного захисту особи є стан її духовного, морального та фізичного комфорту.*

Об'єктом захисту є також умови та фактори, які забезпечують розвиток усіх сфер життєдіяльності особистості й суспільства, зокрема культури, науки, мистецтва, релігійних і міжнаціональних відносин.

До об'єктів належать також:

- ✓ мовне середовище;
- ✓ соціальні, ідеологічні, політичні орієнтири;
- ✓ суспільні та соціальні зв'язки;
- ✓ психофізичні фактори, що проявляються у вигляді фізичних, хімічних та інших впливів природного, антропогенного і техногенного походження;
- ✓ генофонд народів, які населяють державу, тощо.

Інформаційно-психологічна безпека особи є складовою частиною інформаційної безпеки держави і займає особливе місце в державній політиці під час її забезпечення. Ця особливість визначається специфікою загроз і їхніх джерел, особливим характером принципів та завдань державної політики у цій сфері. Найбільш важливими об'єктами інформаційно-психологічного захисту в сучасних умовах є індивідуальна і масова свідомість.

Для особистості головними системоутворювальними рисами є цілісність (тенденція до стійкості) та розвиток (тенденція до зміни).

Внаслідок руйнування або перекручування цих рис особистість перестає існувати як соціальний суб'єкт. Це означає, що будь-який інформаційно-психологічний вплив на особистість має оцінюватися з позиції збереження чи руйнування її як цілого. Складність забезпечення інформаційно-психологічної безпеки визначається декількома факторами.

Так, до політичних факторів відносять:

- ❖ зміну геополітичної обстановки внаслідок фундаментальних змін у різних регіонах;
- ❖ формування нових національних інтересів;
- ❖ становлення державності на основі демократичних принципів, законності, інформаційної відкритості;
- ❖ руйнування усталеної системи командно-адміністративного державного управління;

❖ інформаційна експансія розвинутих країн, які здійснюють глобальний інформаційний вплив, з метою поширення світогляду, політичних і духовних цінностей та ідеалів західного світу;

❖ посилення міжнародної співпраці на основі максимальної відкритості сторін;

❖ низький рівень політичної, правової та інформаційної культури в суспільстві.

До соціально-економічних факторів відносять:

❖ труднощі переходу до ринкової економіки;

❖ продовження інфляційних процесів та падіння життєвого рівня населення;

❖ зростання безробіття, майнова поляризація;

❖ поширення злочинності, криміналізація суспільних відносин;

❖ погіршення показників здоров'я нації;

❖ зростання міжетнічної напруги.

Духовні фактори також мають значення, а саме:

❖ криза державної ідеології;

❖ деформація системи норм, установок та цінностей, що проявляється у неадекватності оцінки інформаційно-психологічного впливу;

❖ поява нових форм та засобів впливу на індивідуальну, групову й масову свідомість;

❖ поява й ріст нових форм міфологічної свідомості;

❖ недооцінка національних і культурно-історичних традицій та проникнення в суспільну свідомість шаблонів західної масової культури;

❖ послаблення важливих соціокультурних інститутів держави, науки, освіти, виховання та культури;

❖ недовершеність та недосконалість системи етичних норм в сфері інформаційної діяльності.

Для усвідомлення сутності та змісту завдань інформаційно-психологічного захисту особи і суспільства від деструктивного впливу в умовах сучасного інформаційно-психологічного протиборства необхідно зрозуміти *механізми інформаційно-психологічного впливу на поведінку індивіда (особистості),* а також на прийняття рішень на будь-якому рівні суспільних і державних структур, у будь-якій сфері їхньої діяльності. Для цього необхідно ввести поняття механізму вербального інформаційного впливу, розуміючи при цьому, що в його основі лежить закономірність усвідомленого сприйняття

інформації, саме її змісту. Цей механізм за своєю суттю є загальним і реалізує загальні закономірності інформаційних процесів у соціальному середовищі.

Під впливом змісту інформаційних потоків, які людина сприймає, акцентів на окремих його фрагментах, інших факторів у неї формується спосіб мислення, її світогляд, система цінностей та інтересів, які з часом збагачуючись і розвиваючись в той чи інший бік, виступають під час аналізу поточної інформації вже у вигляді своєрідного морально-семантичного фільтра.

Від орієнтації й усталеності цього фільтра суттєво залежать вчинки та поведінка людини в тій чи іншій ситуації. На змістовні та якісні характеристики фільтра впливають *історичні, національно-етнічні чинники, система освіти, релігійні та філософські течії, ідеологічна пропаганда, інші складові інформаційного середовища.* Зрозуміло, що значну роль при цьому відіграють засоби масової інформації (періодичні видання, радіомовлення та телебачення, Інтернет).

Наступним важливим моментом у процесі вербального впливу є поведінка особи в конкретній ситуації, визначення позиції, прийняття нею адекватного рішення тощо. У цьому випадку за наявності "якісного" фільтра також велике значення має якість інформування, яке передбачає своєчасність, повноту, всебічність і достовірність наявної інформації. Забезпечення цих факторів є запорукою адекватної поведінки людини.

Разом з цим, якщо не виконується хоча б одна із вимог до інформації, адекватність оцінки ситуації людиною гарантувати не доводиться. До того ж, якщо інформація містить грамотно продуману та організовану дезінформацію, яка є правдоподібною, людина навіть за наявності "якісного" фільтра може приймати рішення, адекватні змісту наявної інформації, але неадекватні щодо реальної ситуації. За допомогою навмисно спотвореної, вибірково неповної інформації і цілеспрямованої дезінформації можна впливати не лише на рішення, що приймаються людиною, та на її поведінку, але й на елементи фільтра (систему цінностей, духовні й матеріальні інтереси і потреби, релігійні та філософські погляди тощо), корегуючи їх в бажаному напрямку, тобто на формування її як особистості (аналітика, вченого, керівника, політика тощо).

Механізми невербального інформаційного впливу на людину ґрунтуються на використанні закономірностей сприйняття людиною інформації через підсвідомість.

Відомо, що підсвідомість (а опосередковано і свідомість) може програмуватися зовнішнім, неконтрольованим людиною інформаційним

впливом. Наприклад, чим тонша психічна організація людини, тим більше вона емоційно вразлива. На сьогодні не існує достатніх гарантій захисту особи від загроз, пов'язаних з порушенням інформаційної та інформаційно-психологічної безпеки особистості.

Загрози неусвідомлюваного інформаційно-психологічного впливу:

- штучного щеплення їй синдрому залежності;
- розроблення, створення та застосування спеціальних засобів;
- маніпуляції суспільною свідомістю з використанням спеціальних засобів впливу;
- деструктивний вплив на психіку людини природних комплексів, антропогенних зон, генераторів фізичних полів та випромінювань.

У сучасних умовах спостерігається активна розробка та впровадження новітніх форм, способів і технологій інформаційно-психологічного впливу на індивідуальну, групову та масову свідомість.

До таких джерел, каналів і технологій впливу на свідомість, психологію та поведінку людини можна було б віднести наступні:

Канали і технології впливу на свідомість та психологію людини:

- ЗМІ та спеціальні засоби інформаційно-пропагандистської спрямованості;
- глобальні комп'ютерні мережі та програмні засоби швидкого поширення в мережах інформаційних і пропагандистських матеріалів;
- засоби та технології, що нелегально модифікують інформаційне середовище, на підставі якого людина приймає рішення;
- засоби створення віртуальної реальності;
- чутки, міфи і легенди;
- засоби підпорогового семантичного впливу;
- засоби генерування акустичних та електромагнітних полів.

Джерелами загроз інформаційного простору є:

- ✓ суперечності певних інтересів, систем цінностей, цілей між особистістю та суспільством, державою;
- ✓ наявність в однієї зі сторін (особистості або держави) стосовно іншої домагань, претензій або інших спонукань до конфлікту.

Найбільш небезпечним джерелом загроз цим інтересам вважається суттєве розширення можливостей маніпулювання свідомістю людини через

створення навколо неї індивідуального віртуального інформаційного простору, а також можливість використання технологій впливу на її психічну діяльність.

Однією з характерних тенденцій, яка склалася в сучасних умовах не тільки в Україні, а й у світі, є випереджувальний розвиток форм, способів, технологій і методів впливу на свідомість (підсвідомість), і психічний стан людини порівняно з організацією протидії негативним, деструктивним психологічним впливам, інформаційно-психологічним захистом особистості й суспільства загалом. Йдеться про можливі деформації у системі масового інформування й поширення дезінформації, які ведуть:

- ❖ до потенційних порушень суспільної стабільності;
- ❖ до завдання шкоди здоров'ю і життю громадян унаслідок пропаганди чи агітації, що збуджують соціальну, расову, національну чи релігійну ненависть і ворожнечу;
- ❖ до діяльності тоталітарних сект, що пропагують насильство й жорстокість.

Ці впливи, усвідомлені чи неусвідомлені, як свідчить життєва практика, можуть призводити й призводять до серйозних порушень психічного й фізичного здоров'я, відхилення від норм поведінки, до зростання ризикованих соціальних й особистісних ситуацій. Під час розгляду інформаційно-психологічного впливу, як загрози, вочевидь йдеться про негативні наслідки його реалізації, які можуть проявлятись у двох аспектах:

1) система відносин особистості, зокрема стосовно держави;

2) руйнування цілісності самої особистості.

Водночас особистість (її психіка та свідомість), піддається різноманітним маніпуляційним впливам, що є інформаційними за своєю природою, і їх результати можуть прямо загрожувати фізичному чи психічному здоров'ю людини. Саме такі впливи часто протягом багатьох років формують морально-психологічну атмосферу в окремих прошарках суспільства, підживлюють кримінальне середовище і сприяють зростанню психічних захворювань у суспільстві. Проповідництво деструктивних релігійних вчень, поширення містичних й езотеричних знань і практик, магії, шаманства тощо можуть бути прикладом таких впливів, що призводять до соціальної особистісної дезадаптації, а в ряді випадків – до руйнування психіки людини.

Серйозну небезпеку для особистості викликає поширення за допомогою мережі Інтернет порнографії, непристойної інформації, що ображає суспільну

мораль, порушує сформовані в суспільстві стандарти моралі. Хоча й вважається, що за допомогою Інтернету гарантується більша конфіденційність й анонімність, ніж під час відвідування кінотеатрів або магазинів з відкритою чи підпільною порнолітературою й відеофільмами.

2. Питання. Характеристика інформаційно-психологічного впливу

Інформаційно-психологічний вплив (ІПсВ) **—** *вплив на свідомість особи і населення з метою внесення змін у їхню поведінку та (або) світогляд.*

Види ІПсВ:

❖ **Психогенний вплив** – *(це психічний або фізичний вплив якихось явищ або подій на мозок, свідомість людини в результаті якого спостерігається порушення вищої нервової діяльності: з'являється відчуття страху та паніки).*

Це обумовлено неузгодженістю функціональних систем психофізіологічної організації, тобто ламанням стереотипів під час впливу різко зміненої афферентації з боку різних рецепторів.

Чим вища в часі така неузгодженість і чим менше підготовлена людина до впливу цього психогенного чинника, тим більше виражені психічні порушення.

Такий стан може виникати під впливом голографічних малюнків. Багато країн домоглися в цій галузі досить великих успіхів, приміром, створено проекти лазерної графіки з поверхні землі та з космічної платформи.

❖ **Нейролінгвістичний вплив** – *вид психологічного впливу, що припускає використання спеціальних прийомів, спрямованих на створення позитивної мотивації, психологічної корекції внутрішніх джерел поведінки і світогляду особистості людини.*

Нейролінгвістичний вплив орієнтований на ідентифікацію та зміну переконань особистості під час впливу на її світоглядні й емоційно-почуттєві стани (характеристики, що дозволяють удосконалювати, програмувати стан і поведінку людини в умовах практичної діяльності).

Основним об'єктом такого виду впливу на людину є її психіка і контрольована нею діяльність, а основним засобом впливу виступають соціально продумані програми вербального і невербального впливу, що дозволяють змінювати світогляд та цінності особистості.

❖ **Психоаналітичний (психокорекційний) вплив** – *це вивчення (аналіз) підсвідомості людини і вплив на неї шляхом, що виключає опір на рівні свідомості (здійснюється у стані гіпнозу).*

Однак сучасні технологічні досягнення дозволяють усунути опір з боку свідомості й у нормальному стані. Це можна зробити за допомогою як психоаналізу, так і психокорекції. Під час першого здійснюється математичний аналіз реакцій організму, що виникають під час миттєвого візуального перегляду або звукового читання різних "стимулів": слів, образів, фраз.

У такий спосіб можна абсолютно точно визначити наявність у підсвідомості людини визначеної інформації й виміряти її значимість для конкретної особистості, знайти сховану мотивацію. Проаналізувавши отриману інформацію, у разі необхідності, можна здійснювати психокорекцію (психорегуляцію), основним діючим фактором, якої також, служать ключові слова, образи, запахи (слова можуть перетворюватися за допомогою спектрального мовного сигналу). Найбільш зручною є звукова регуляція психіки, за якої словесні навіювання в закодованій формі виводяться на будь-який носій звукової інформації (музику, мову або шум). Наприклад, людина може слухати музику, у якій утримується схована (не сприймана на свідомому рівні) команда, що постійно впливає на підсвідомість слухача.

❖ **Психотронний вплив** (парапсихологічний, екстрасенсорний) — *вплив, що може здійснюватися за допомогою передачі енергії мислення через позачуттєве сприйняття, яке охоплює опосередковане свідомістю і процесами сприйняття дистанційної взаємодії між живими організмами й навколишнім середовищем.* Телевізійні та інші масові сеанси екстрасенсорного впливу засвідчують реальну можливість впливу на особистість. Досить часто при цьому використовуються технічні засоби, що сприяють посиленню впливу, передачі й контакту з індивідом. Цей вплив на об'єкт може бути пов'язаний з придушенням волі до опору, деморалізацією. Відомі факти роботи над створенням генератора частотного кодування психіки, високочастотних і низькочастотних генераторів, засобів впливу соціальною інформацією та ін., які здатні викликати необхідні процеси в психіці людини, а отже, впливати на її свідомість і поведінку.

Парапсихологія — це галузь науки, що вивчає пси-комунікації, тобто досліджує ті дистантні зв'язки живого організму з навколишнім середовищем,

які одержали назву "екстрасенсомоторних" (оскільки вони діють на все, крім органів чуття і мускульних зусиль). Поняття "пси" містить у собі екстрасенсорну перцепцію, тобто позачуттєве сприйняття і психокінез, під яким розуміється вплив на предмети й хід психічних процесів без мускульних зусиль або використання технічних засобів. Загалом же принципової різниці між предметами дослідження парапсихології і психотроніки немає. Відмінність прослідковується лише під час порівняння методів, засобів і цілей дослідження. Психотроніці властиве прагнення переважно до технічних і технологічних підходів і рішень, до розробки технічних аналогів досліджуваних феноменів, наприклад, психотронних генераторів, а отже, концентрації великих зусиль на роботах прикладного характеру. Процес екстрасенсорного впливу значно полегшується під час використання системи комунікацій: телефонного зв'язку, радіотрансляційних мереж тощо.

❖ **Психотропний вплив** – *вплив на мозок і поведінку особи шляхом введення в її організм різних препаратів (зокрема фармацевтичних препаратів, запахів), засвоєння яких відбивається на вищій нервовій діяльності*. Вплив препаратів на психіку людини добре відомий і вивчається вже досить тривалий час. З урахуванням останніх досягнень не тільки в психології, але й "суміжних" науках (біології, нейро- і психофізіології, кібернетиці, психофармакології тощо) розробляються і продовжують удосконалюватися методи підпорогового впливу, методи психологічної індоктринації та конверсії, засоби місцевого психічного контролю і психопрограмування.

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

Процес прийняття індивідом ІПсВ, спрямованого на емоційну сферу свідомості, специфічний. Загалом він більш згорнутий, ніж, наприклад, процес прийняття пропагандистського впливу: в ньому функціонують тільки сприйняття і запам'ятовування, діяльність мислення виражена дуже слабо. Інформацію особистість сприймає або не сприймає, сприймає цілком або частково, але у формуванні певних висновків майже не бере участі. Процес

інформаційно-психологічного впливу на емоційну сферу свідомості включає довільне сприйняття та запам'ятовування і характеризується дуже зниженим рівнем усвідомлення про зміст впливу. Осмислення отриманої інформації відбувається пізніше, за більш високої пізнавальної активності індивіда.

Рівень ефективності ІПсВ залежить від:

- *Змісту матеріалу: його складності, конкретності, суспільної значимості тощо*. Наприклад, за рівних умов, чим простіша інформація, тим більше шансів на те, що дії, до яких вона спонукає, можуть виконуватися автоматично, а 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 неусвідомленому сприйняттю впливу. Ступінь автоматизму у відповіді особистості пов'язаний з рівнем усвідомленості та критичності сприйняття інформації. Якщо вплив приймається 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 особистості й усвідомленням його).

Небезпечний ІПсВ на індивідуальну свідомість може призвести до двох видів взаємозалежних змін:

1. Зміни психіки, психічного здоров'я людини. Оскільки, у випадку застосування інформаційного впливу складно визначити межі норми і патології, показником змін може бути втрата адекватності щодо відображення світу у свідомості й індивідуальному ставленні до світу. Можна говорити про деградацію особистості, якщо форми відображення дійсності спрощуються, реакції грубішають і здійснюється перехід від вищих потреб (у самоактуалізації, соціальному визнанні) до нижчих (фізіологічних, побутових).

2. Зміни в цінностях, життєвих позиціях, орієнтирах, світогляді особистості. Такі зміни спричиняють антисоціальні вчинки і становлять небезпеку вже для всього суспільства і держави.

Важлива особливість інформаційно-психологічного впливу на індивідуальну свідомість полягає в тому, що людина може не помічати його і не усвідомлювати як загрозу.

Поведінкою особи керує її мозок, свідомість. Усе, що спонукає людину до діяльності, має проходити через її мислення. Отже, ІПсВ з метою зміни поведінки особистості в бажаному напрямку має домогтися відповідної зміни в її свідомості.

Завдання на самостійну роботу

1. Роль ЗМІ в маніпулюванні свідомістю людини.
2. Методи маніпулювання свідомістю людини.
3. Дезінформація як засіб впливу на людину.
4. "Вікна Овертона" у маніпулятивних технологіях.
5. Біометрія як механізм захисту від соціальної інженерії.
6. Кібертероризм як загроза інформаційній безпеці.
7. Комп'ютерна злочинність як загроза інформаційній безпеці.

Питання до самоконтролю

1. Сутність інформаційно-психологічної безпеки особи.
2. Види інформаційно-психологічного впливу.
3. Загрози особистості від деструктивних інформаційних впливів.
4. Роль ЗМІ в маніпулюванні свідомістю людини.

Семінар 10. Заняття. 6.2. Поняття та сутність інформаційного впливу на суспільство та особистість.

Навчальні питання.

1. Сутність інформаційно-психологічної безпеки особи.
2. Загрози особистості від деструктивних інформаційних впливів.
3. Інформаційне середовище та його вплив на людину.
4. Види інформаційно-психологічного впливу.
5. Роль ЗМІ в маніпулюванні свідомістю людини.

Семінар 11. Заняття. 6.3. Інформаційний вплив на суспільство та особистість.

Навчальні питання.

Інформаційний вплив на суспільство та особистість.

1. Інформаційно-психологічна безпека особи.
2. Види загроз особистості від деструктивних інформаційних впливів.
3. Інформаційне середовище та його вплив на людину.
4. Види інформаційно-психологічного впливу.

Рекомендована до теми література

1. Інформаційна безпека: підручник. / В. В. Остроухов, М. М. Присяжнюк, О.І. Фармагей та ін.; під. ред. В. В. Остроухова. Київ: Видавництво Ліра, 2021. 412с.

2. Теорія та практика сучасного інформаційно-психологічного протиборства: навчальний посібник. /В. В. Петрик, С. О. Гнатюк, М. М. Присяжнюк та ін. Полтава, 2022. 328 с.

3. Золотар О. О. Інформаційна безпека людини: теорія і практика: монографія. Київ : ТОВ Видавничий дім "АртЕк", 2018. 446 с. URL: https://ippi.org.ua/sites/default/files/informaciyna_bezpeka_lyudini_print.pdf (дата звернення: 29.06.2024).

4. Богданов О. М., Петрик В. М. Соціальна інженерія (сучасні технології та шляхи захисту): навч. посіб. Київ: ІСЗЗІ КПІ імені Ігоря Сікорського, 2018. 80 с.

5. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки". URL: https://zakon.rada.gov.ua/laws/show/n0080525-21#Text . (дата звернення: 29.06.2024).

6. Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року "Про створення Центру протидії дезінформації": Указ Президента України від 19 березня 2021 року № 106/2021. URL: https://zakon.rada.gov.ua/laws/show/n0015525-21#Text (дата звернення: 29.06.2024).

Лекція 7. Заняття 6.4. Сутність та зміст сугестивних технологій маніпулятивного впливу.

Навчальні питання.

1. Наукові особливості сугестивних явищ.

2. Поняття та напрями реалізації сугестивних технологій.

1. Питання. Наукові особливості сугестивних явищ.

Історично людство супроводжувало одне з найбільш універсальних явищ, пов'язаних із психікою людини – **сугестія (навіювання).**

Сугестія або навіювання – *це психологічний вплив на свідомість людини, при якому відбувається некритичне сприйняття нею переконань та установок.*

- *Суть навіювання полягає у впливі на відчуття людини, а через них – на її волю та розум.*
- *Психологічна дія може бути позитивною або негативною, що впливає на ефект, який виявляється на людину.*

***Сугестор** – людина, яка маніпулює (навіює).*

***Сугерend** – об'єкт навіювання(адресат).*

Сугестор – джерело навіювання (сугестії) залежно від ситуації та своїх особливостей сугестор може використовувати чотири варіанти поведінки:

- "безперечний авторитет";
- інтелектуальний;
- емоційний;
- пасивний.

Якщо раціональний вплив – це звернення до логіки, розуму і фактів, то сугестивний вплив – це вплив, що обходить свідомий контроль, що йде в обхід розуму через прямі або опосередковані навіювання. Зазвичай це звернення до емоцій, несвідомих, живих вражень. Сугестивний вплив здійснюється або через прямі навіювання, або через ритуали.

Сугестія відіграє ключову роль у психотерапії з таких причин:

1. Розвиток нових переконань.

Психотерапевт може переформатувати переконання людини та допомогти їй розвинути нові, більш позитивні та конструктивні способи мислення.

2. Активація внутрішніх ресурсів.

Сугестія здатна стимулювати внутрішні ресурси та здібності, які допоможуть впоратися з проблемами чи травмами.

3. Посилення мотивації.

Психотерапевт може використовувати сугестію для зміцнення віри людини у власні здібності та можливості.

4. Зниження симптомів.

Сугестія впливає на фізіологічні та емоційні процеси, що може допомогти впоратися із симптомами тривоги, депресії чи панічних атак.

Сугестія пронизує багато сфер буття: за будь-якого виду діяльності, свідомо чи несвідомо, людина піддається впливу.

Сугестія різноманітна у використанні та багатолика у своїх проявах. Смаки й уподобання, особливості поведінки дуже часто продиктовані неусвідомлюваним навіюванням. На ньому частково заснований вплив на свідомість електронних засобів масової комунікації, моди, звичаїв, обрядів. Навіювання – один із способів формування віри.

Проблема причинності сугестивних впливів привертала увагу багатьох учених. Наукова література містить матеріали, що дають змогу не лише ознайомитися з явищем сугестії, але й становлять основу розкриття його сутності, виявлення причин його виникнення та функціонування.

Здавна під час пояснення феномену сугестії визнавалася значна сила слова. Серед мислителів минулого можна *назвати Арістотеля, Сократа, Платона, Цицерона* та інших, як творців ораторського мистецтва та мовного переконання.

Ускладнення форм суспільного буття, формування нових ідеалів, норм і культурних цінностей зумовлюють необхідність використання наукових знань у поясненні багатьох суспільно-соціальних явищ. У зв’язку з цим появу робіт (*А. Слободяник, Е. Феїзов, Д. Дубровський, Л. Грімак, П. Буль* та ін.), що включають аналіз соціальних явищ – носіїв сугестивного впливу, слід розглядати як важливий крок до задоволення відповідної суспільної потреби.

Роботи *Г. Шиллера, Д. Райгородського, С. Кара-Мурзи, І. Черепанової, О. Романова, Є. Доценко, К. Каландарова, Г. Почепцова* та інших розкривають суть сугестивних явищ у структурі маніпулятивної й прагматичної діяльності.

У їхніх працях пояснюються причини уразливості людської свідомості, розшифровуються замасковані засоби масового впливу на психіку людей.

Механізми впливу на психіку людини та її свідомість лежать в основі технологій маніпулювання свідомістю, але ці механізми відповідають маніпулюванню тільки в тому випадку, якщо воно майстерно приводить до прихованого збудження в людини намірів, якими вона до цього не володіла.

Суб'єкт маніпулювання прагне, щоб об'єкт впливу сам визнав той чи інший вчинок, що йому навіюється, єдино правильним для себе. Для досягнення цього маніпулятор вдається не до засобів примушення, а до засобів переконання, які полягають в умисному обмані або навіюванні (сугестії).

У сучасній інтерпретації *"сугестія – це процес впливу на психічну сферу людини, пов'язаний із зниженням критичності під час сприйнятті та реалізації змісту, що навіюється"*

Навіювання (сугестія) може бути зроблено за допомогою:

- директивного гіпнозу;
- недирективного гіпнозу;
- ритуальних дій;
- емоційного впливу оточуючих (групи);
- казок, метафор.

Вважається, що інформація, засвоєна за допомогою навіювання, важко піддається осмисленню та корекції.

Засоби сугестії поділяють на:

- *текстові* (зміст та форма подання тексту, графіка, шрифти);
- *мовленнєві*, які натомість бувають:
  - ✓ вербальні (фрази, слова, наголоси та інтонації);
  - ✓ паралінгвістичні (висота, тон, тембр голосу);
  - ✓ невербальні (міміка, жести, проксеміка, особливості поведінки учасників відеоряду).

Використовують різні класифікації сугестії:

1) зовнішня (гетеросугестія) й самонавіювання (аутосугестія);

2) навіювання пряме чи відкрите, опосередковане чи закрите;

3) навіювання контактне й дистанційне, тощо.

2. Питання. Поняття та напрями реалізації сугестивних технологій

Є кілька сугестивних підходів у здійсненні психологічного впливу з метою маніпулювання свідомістю людей:

1. Психоаналітично орієнтований підхід, який використовує "підсвідомість" із метою маніпулювання свідомістю. Із середини XX століття масове застосування психоаналізу в рекламі стало основою діяльності торгових компаній; слово "підсвідомість" – девізом і змістом нового напряму в рекламі.

2. Гіпнотичний підхід використовує трансовий стан. У гіпнотичних підходах широко застосовуються результати досліджень, сплеск яких спостерігався в США після Другої світової війни, коли чітко намітився інтерес до маніпулювання свідомістю, особливо у сфері реклами.

Техніки наведення трансового стану, які використовуються в рекламній справі:

- ❖ показ трансової поведінки персонажів під час зустрічі з рекламою;
- ❖ застосування вікової регресії – обігруються стосунки бабусі та внуків та ін.;
- ❖ використання природних трансових станів;
- ❖ перевантаження свідомості в сюжетах фільмів через показ двох персонажів, які одночасно говорять, швидке й хаотичне чергування картинок у кадрі з поєднанням прискореного мовлення тощо;
- ❖ використання повної невизначеності, непередбаченості;
- ❖ звернення до авторитету та інші.

3. Підхід за допомогою еріксонівського гіпнозу передбачає застосування мовних стратегій для нейтралізації здатності до опору навіювання.

Суть еріксонівського гіпнозу полягає в тому, що в ньому практично не віддають прямих наказів, лише дещо коментують, про щось запитують, радяться з партнером у спілкуванні. Разом із тим, усі вживані мовні стратегії дають змогу одержувати результат (наказ виконується) й уникнути свідомого опору наказу.

4. Підхід нейролінгвістичного програмування (НЛП).

У технології НЛП широко застосовується найвище на сьогодні досягнення комп'ютерних технологій – віртуальна реальність.

У кожної людини свій власний спосіб створення "карти" реальності: в *картинках, звуках* або *відчуттях*.

Існують три типи сприйняття дійсності.

- Перший тип – *візуальний, зоровий*. Людина візуального типу сприймає і організовує свій досвід та мислення в основному за допомогою зорових образів, їй краще "один раз побачити, ніж сто разів почути".
- Другий тип – *аудіальний, слуховий*. Індивід уявляє й описує світ в аудіальних, слухових образах.
- Третій тип – *тактильний,* тобто сприймається й оцінюється світ насамперед за допомогою відчуттів.

Комплексне донесення сенсорної інформації через зорову, слухову й тактильну модальність дає змогу проникати в глибинні пласти людської психіки, змінювати окремі елементи самого образу в потрібному напрямі та, зрештою, ефективно маніпулювати свідомістю віртуального користувача.

Найвищим досягненням комп'ютерних технологій є віртуальна реальність. Це якісно новий крок у сугестивних технологіях.

Комплексне донесення сенсорної інформації через зорову, слухову й тактильну модальності дає можливість проникати в глибинні пласти людської психіки, змінювати окремі елементи самообразу в потрібному напрямі та зрештою ефективно маніпулювати свідомістю віртуального користувача.

Швидкий розвиток комп'ютерних технологій віртуальної реальності створює загрозу появи "техногенного наркотику" – сильнішого й гнучкішого для управління свідомістю людини, ніж відомі нині наркотичні препарати.

За допомогою комп'ютерних ігор у контексті з ігровою захоплюючою фабулою можна також вирішувати завдання сугестії при повному усвідомленні гравцем своїх дій, трансформуючи його психіку в заданому програмно підтримуваному напрямі.

Незважаючи на складність класифікації навіювань, у сугестивно-психологічній літературі в структурі сугестивного впливу розрізняються наступні базові види навіювання, пов'язані з етапом утилізації стану підвищеної сугестивності сугеренда:

1) *прямі навіювання;*

2) *непрямі навіювання* припускають розуміння сугерендом мети сугестивного впливу, чітко вказуючи на очікувану дію або психологічну

реакцію з його боку. Переважно вони належать до свідомого досвіду цього сугеренда й, зазвичай, дають конкретні вирішення проблем, а також детальні інструкції про те, як реагувати на рекомендації й питання сугестора.

Цей вид сугестії відповідно до її психологічної природи може розглядатися у двох аспектах:

а) в аспекті впливу на емоції, установки, неусвідомлювані мотиви сугеренда (у формі сугестивних настанов сугестора);

б) в аспекті впливу на складові поведінки сугеренда (у формі сугестивних команд і наказів сугестора).

Розглянемо найважливіші змістовні особливості різних форм **прямого навіювання.**

❖ "*Позитивні навіювання*".

Ці навіювання найбільш популярні, прості й безвідмовні. Вони будуються таким чином, щоб допомогти усвідомити сугеренду, що він може досягти бажаних станів, переживань, відносин. Оскільки слова сугестора орієнтують сугеренда на актуалізацію певного досвіду, конкретне позитивне навіювання конструюється таким чином, щоб стимулювати певні бажані або необхідні реакції.

Приклади: 1) "Ви можете згадати ту мить, коли пишалися собою"; 2) "Ви в змозі знайти в собі сили, про існування яких навіть не підозрювали".

❖ "*Негативні навіювання*".

За допомогою даних навіювань можна актуалізувати бажану реакцію сугеренда, рекомендуючи йому не реагувати тим способом, що від нього насправді очікується. Якщо застосовувати негативні навіювання з урахуванням контексту комунікації й характеру сугеренда, вони можуть виявитися винятково корисними.

Приклади: 1) "Ви не повинні тепер думати із симпатією про свою школу"; 2) "Спробуйте не думати про те, хто з ваших друзів завтра не прийде на вечірку".

❖ "*Конкретні навіювання*".

Дані навіювання містять детальні описи почуттів, спогадів, думок або фантазій, які повинні бути актуалізовані в сугеренда в процесі навіювання. При цьому наведення численних деталей, що стосуються кожного елемента досвіду,

який навіюється, може викликати бажаний сугестивний ефект більш повно, тривало й надійно.

Приклади: 1) “Подумайте на хвилинку про червону троянду, про її м’які, оксамитові пелюстки, її ніжний запах”; 2) “Чи пам’ятаєте ви, як приємно відкусити спілий апельсин, коли рот наповнюється слиною, а по пальцях тече солодкий ароматний сік?”

Однак кожне конкретне навіювання може стати в той же час і джерелом потенційної невдачі. Таке можливо, тому що велика кількість деталей, які приводить сугестор, збільшують імовірність переживань сугеренда, що йдуть врозріз зі змістом навіювань сугестора.

❖ “*Загальні навіювання*”.

На відміну від конкретних навіювань, у загальних навіюваннях відсутні деталі, що дає сугеренду можливість вільно вибирати елементи суб’єктивного досвіду, які асоціюються з абстрактним змістом навіювання. У межах сугестивного процесу вони дають сугеренду шанс використовувати власний досвід та інформацію для деталізації й реалізації змісту навіювання. Таким чином, навіювання, яке може здатися занадто узагальненим, щоб бути успішним, насправді стає стимулом для осмисленого індивідуалізованого переживання.

Приклади: 1) “Ви в змозі згадати деяке переживання свого дитинства, до якого ви так давно не зверталися?”; 2) “Чи пам’ятаєте ви той особливий момент, коли ви були задоволені собою?” Жодне із зазначених вище загальних навіювань спеціально не уточнює, який саме спогад мається на увазі.

Тому сугеренд сам змушений актуалізувати конкретні елементи індивідуального досвіду. Застосовуючи визначення “конкретний”, “певний”, “специфічний”, “особливий”, сугестор підштовхує сугеренда до концентрації на одному зі своїх реальних переживань, які мали місце в минулому. Здійснений сугерендом вибір конкретного суб’єктивного переживання є результатом актуальної взаємодії між свідомою й несвідомою сферами його психіки.

Непрямі навіювання *характеризуються або неясністю мети для сугеренда, або відсутністю прямої спрямованості на того, хто є дійсним об’єктом впливу.*

При цьому зміст непрямої сугестії включається сугестором у повідомлену інформацію в схованому, замаскованому вигляді й характеризується неусвідомленістю, непомітністю, мимовільністю її засвоєння сугерендом.

Непряме навіювання дуже часто *може бути ненавмисним*, будучи звичайним компонентом міжособистісного спілкування.

Різновидом непрямого навіювання є "**черезпредметне" (опосередковане)** навіювання. У цьому випадку використовується додатковий подразник, що набуває нового інформаційного значення через зроблене пряме навіювання.

Одним із часто використовуваних шляхів непрямого навіювання є призначення **плацебо.** Плацебо-ефект досягається призначенням індиферентної речовини з інформацією про очікуваний ефект у разі її вживання. Плацебо-ефект при цьому забезпечується кольором, формою, розміром, дозою препарату, режимом його прийому тощо.

Мовні форми непрямого навіювання.

1. "*Складне складене навіювання"*. Воно являє собою складносурядне або складнопідрядне речення. Найчастіше перша частина речення є "приєднанням", тобто описує психічний стан або ситуацію сугеренда в цей момент часу, а друга частина – "веденням", тобто описує ефект, який сугестор хоче викликати в сугеренда.

2. "*Послідовність прийняття*". Даний вид навіювання схожий з попереднім, але складається з більшої кількості фраз "приєднання" і дозволяє досягти таким чином більшої згоди сугеренда. Мова йде про послідовне прийняття якихось ідей. Людина, слідкуючи за логікою мовлення сугеренда, подумки погоджується з кожним наступним постулатом, оскільки перед цим уже погодилася з попереднім.

3. "*Пресуппозиція*". Під пресуппозицією або припущенням розуміється явище, що обов'язково трапиться. Речення зазвичай будується як складне й конструюється так, щоб наголос падав на одну частину, а ненаголошена частина, яка і є пресуппозицією, сприймається як така, що обов'язково трапиться

4. "*Трюїзм*". Це мовна констатація певних фактів, подій, явищ, які не можна заперечувати. Це можуть бути як факти, що випливають із життєвих спостережень, так і факти, які відомі всім.

5. "*Негативні парадоксальні навіювання*". Звичайно такі навіювання мають негативні частки й можуть діяти потрійно. По-перше, сугестор може прагнути привернути увагу сугеренда до предмета або явища. По-друге, оскільки деякі сугеренди звикли не погоджуватися з думкою оточуючих людей, то сугестор може використовувати їх "стратегію негативізму" за аналогією з математичним принципом: "мінус на мінус дає плюс".

6. "*Подвійна зв'язка, або вибір без вибору*". За логікою дії цей вид навіювання близький до пресуппозиції й дає ілюзорну можливість вибору там, де його немає. Таке навіювання приймається легко, оскільки існує видимість вільного ухвалення рішення.

7. "*Навіювання, які пов'язані з часом".* Такі сугестії мають на увазі, що трансформація відбудеться тоді, коли для сугеренда наступить суб'єктивно доречний час. Йому пропонується вибрати доречний часовий інтервал, коли він може виконати запропоновану дію.

8. "*Мобілізуючі навіювання*". Для мобілізуючих навіювань використовується особливий порядок побудови фрази, яка вимовляється за один видих.

9. "*Контекстуальне навіювання* (аналогове позначення)". Контекстуальне навіювання присутнє тоді, коли на тлі розміряного мовлення слово або фраза виділяється тоном голосу, паузами, гучністю або будь-якими іншими мовними характеристиками та інші.

Завдання на самостійну роботу

1. Сугестивні технології маніпулятивного впливу.
2. Соціотехнічне тестування та створення профілів персоналу.

Питання до самоконтролю

1. Сутність сугестивних технологій маніпулятивного впливу.
2. Наукові особливості сугестивних технологій.
3. Напрями реалізації сугестивних технологій.

Семінар 12. Заняття. 6.5. Інформаційно-комунікативне суспільство, як новий об'єкт сугестивного впливу.

Навчальні питання.

1. Наукові концепції інформаційного суспільства.

2. Україна в умовах формування інформаційно-комунікативного суспільства.

3. Сутність сугестивних технологій маніпулятивного впливу.

4. Наукові особливості сугестивних технологій.

5. Напрями реалізації сугестивних технологій.

Семінар 13. Заняття. 6.6. Чорний піар як сугестивна технологія.

Навчальні питання.

1. Чорний піар: підходи, зміст, принципи.

2. Сугестія як психолінгвістична основа чорного піару.

3. Піар: техніки реалізації сугестії.

4. Чорна риторика як маніпулятивна технологія чорного піару.

5. Принципи й правила чорної риторики: сугестивний підхід.

6. Сугестія в жанрах Інтернету (медіавіруси, блоги, комп'ютерні ігри тощо).

7. Принципи сугестивної лінгвістики в інтернетній комунікації.

Рекомендована до теми література

1. Інформаційна безпека: підручник. / В. В. Остроухов, М. М. Присяжнюк, О.І. Фармагей та ін.; під. ред. В. В. Остроухова. Київ: Видавництво Ліра, 2021. 412с.

2. Богданов О. М., Петрик В. М. Соціальна інженерія (сучасні технології та шляхи захисту): навч. посіб. Київ: ІСЗЗІ КПІ імені Ігоря Сікорського, 2018. 80 с.

3. Кулеба Д. Війна за реальність: як перемагати у світі фейків, правд і спільнот. Київ : Книголав, 2022. 384 с.

4. Теорія та практика сучасного інформаційно-психологічного протиборства: навчальний посібник. /В. В. Петрик, С. О. Гнатюк, М. М. Присяжнюк та ін. Полтава, 2022. 328 с.

5. Інформаційно-психологічне протиборство: підручник. Видання друге перекладене, доповнене та перероблене /В. М. Петрик, М. М. Присяжнюк, Я. М. Жарков та ін.]; за заг. ред. В. М. Петрика. Київ: Вид-во ІСЗЗІ КПІ імені Ігоря Сікорського, 2018. 388 с.

Лекція 8. Заняття 6.7. Маніпулятивні технології в засобах масової інформації.

Навчальні питання.

1. Сутність та походження феномену “маніпуляція”.

2. Види маніпулювання суспільною свідомістю.

1. Питання. Сутність та походження феномену “маніпуляція”

Маніпуляція – це природна частина спілкування. Вона використовується в усіх сферах соціального життя.

Маніпуля́ція (фр. manipulation) – складний прийом впливу, операція, витівка.

Маніпуля́ція – використовується у різних науках та сферах людської діяльності (соціології, психології, політиці, медицині, фізиці та ін.).

Феномен маніпуляції людської поведінки вивчається переважно у рамках психологічної науки. Маніпуляцію часто характеризують як форму впливу, яка не є ні примусом, ні раціональним переконанням.

Маніпуляція є дією з двома цілями: явною і прихованою.

Явна мета – на користь адресата, *прихована* – на користь того, хто говорить. Адресат не повинен здогадуватися про приховану мету того, хто говорить.

Маніпуляція – *це різновид прихованого мовного впливу, спрямованого на досягнення власних цілей суб’єкта впливу, які не збігаються з намірами або суперечать бажанням та інтересам об’єкта впливу.*

Термін “маніпуляція” зазвичай відноситься до “радикального програмування” або “обмеженого перепрограмування” всіх або більшості переконань, бажань та інших психічних станів агента. Таку глобальну маніпуляцію, як ми можемо її назвати, також зазвичай уявляють як процес, що відбувається за допомогою однозначно надзвичайних (специфічних) методів. Таких, наприклад, як надприродне втручання, пряма неврологічна інженерія або радикальні програми індоктринації (первісних інструкцій) та психологічного “кондиціонування”.

Основні складові маніпуляції

❖ **Об’єкт маніпулювання –** це свідомість людини та масова свідомість, на яку здійснюється певний вплив із метою досягнення бажаного результату.

❖ **Жертва маніпулювання** – це людина, група людей, суспільство, які були використані для досягнення встановленої мети маніпулятора.

❖ **Суб'єкт маніпулювання** – це людина (група людей), яка ініціювала проведення маніпулювання свідомістю для досягнення певної мети.

❖ **Інструменти маніпулювання** – це ідеї, прийоми, форми, способи, методи, використання яких дає змогу впливати на свідомість людини для досягнення цілі.

❖ **Мішені маніпулювання** – це окремі люди, соціальні групи, населення країни – об'єкти спеціальних інформаційних операцій.

Мішені маніпулятивного впливу

➢ *Збуджувачі активності людини*: потреби, інтереси, схильності.

➢ *Регулятори активності людини*: світогляд, вірування, групові норми, самооцінка, переконання, цільові установки та ін.

➢ *Когнітивні структури*: знання про навколишній світ, людей та інші відомості, які є інформаційним забезпеченням активності людини.

➢ *Операційний склад діяльності*: спосіб мислення, стиль поведінки, звички.

➢ *Психічні стани*: емоційні, функціональні, фонові.

Особливості маніпулятивного впливу

1. Об'єкт маніпуляції не усвідомлює вплив, що здійснюється над ним.

2. Маніпулятор здійснює вплив як на сферу свідомого (розум), так і на сферу несвідомого (інстинкти, емоції, потреби).

3. Маніпулятор встановлює контроль над думками, почуттями, поведінкою, відносинами та життєвими установками об'єкта маніпуляції.

4. Маніпулятор управляє ставленням об'єкта маніпуляції до предмету та явищ навколишнього світу.

5. Маніпулятор оперує подачею інформації, яка навмисно спотворює дійсність.

Науці відома низка версій маніпуляцій. Їх можна умовно згрупувати в *три основні категорії:*

❖ маніпуляція, як вплив, що оминає розум;

❖ маніпуляція, як форма такого собі обману;

❖ маніпуляція, як форма тиску.

1. Маніпуляція як "обхід розуму".

Маніпулювання – це прихований вплив. Прихований вплив на когось – нав'язування прихованого впливу – означає вплив на агентів способом, про який вони не знають і, таким чином, про який вони не можуть легко дізнатися.

2. Маніпуляція як обман.

Даний підхід до маніпуляції розглядає її як форму обману та концептуально пов'язує її з обманом. Маніпуляція – навмисна спроба обманом змусити когось прийняти будь-який хибний психічний стан – переконання, бажання, емоції тощо.

3. Маніпуляція як тиск.

Можна маніпуляцію також розглядати як різновид тиску, щоб діяти так, як того хоче особа впливу. З цього приводу такі тактики, як емоційний шантаж і тиск є парадигмальними випадками маніпуляції, оскільки вони чинять тиск на ціль, накладаючи плату за невиконання того, що хоче маніпулятор.

Подібні технології застосовуються в таких **видах впливу**, як:

- **маніпуляція образами** – оскільки образи володіють сильною психологічною дією, їх широко застосовують в комунікативній практиці, особливо в рекламі;
- **конвенціональна маніпуляція** – опирається не на особисті психологічні установки, а на соціальні схеми: правила, норми, традиції, стереотипи певної суспільної групи, сім'ї;
- **операційно-наочна маніпуляція** – заснована на таких психічних особливостях особи, як сила звички, інерція, логіка виконання дії;
- **маніпуляція особою адресата** – прагнення перекласти відповідальність за яку-небудь дію на адресата, тоді як у виграші залишається маніпулятор;
- **маніпуляція духовністю** – маніпуляція вищими рівнями психіки: значенням життя, духовними цінностями, почуттям обов'язку, тобто особистими смисловими установками індивіда.

Рівні маніпулювання:

1) посилення існуючих у свідомості людей потрібних маніпулятору ідей, установок, мотивів, цінностей, норм;

2) часткові, малі зміни поглядів на ті чи інші події, процеси, факти, що також впливають на емоційне і практичне ставлення електорату до конкретного явища;

3) кардинальна зміна життєвих установок шляхом поширення серед виборців сенсаційних, драматичних, надзвичайно важливих для них повідомлень.

Маніпуляції можуть застосовуватись до текстів, виступів, аудіо-, відео-, фотоматеріалів.

Медіаманіпуляція — *вид психологічного впливу, що здійснюється через пресу (газети, журнали, книги), радіо, телебачення, інтернет, кінематограф, звукозаписи та відеозаписи, відеотексти, телетексти, рекламні щити та панелі,*

домашні відеоцентри, що поєднують телевізійні, телефонні, комп'ютерні та інші лінії зв'язку, соціальні мережі, що призводить до пробудження у об'єкта впливу намірів, які змінюють його бажання, настрої, поведінку, погляди тощо.

Психологічні маніпуляції в медіа

Маніпулятивний вплив, який використовується у сучасних медіатекстах, розділяють на три групи:

- лінгвістичний;
- квазілінгвістичний;
- нелінгвістичний.

До вербальних засобів (лінгвістичний) маніпулятивного впливу належать стилістичні прийоми та виразні засоби мови, які сприяють створенню комічного ефекту, нагнітанню страху, відображенню чуток. Крім того, маніпулятивний вплив нерідко здійснюється за рахунок використання великої кількості чисел.

Щодо квазілінгвістичних засобів впливу, то до них можна віднести розмір та колористику шрифту, а також особливості розташування тексту у друкованому виданні. Квазілінгвістичні засоби маніпулятивного впливу сприймаються читачем за рахунок зорового каналу сприйняття і допомагають авторові газетного повідомлення імпліцитно виразити свою оцінку теми повідомлення та його об'єкту.

Нелінгвістичні засоби маніпуляції включають невербальні елементи смислового простору медіатексту: фотографії, графіки, схеми, таблиці, колажі, малюнки, тощо.

Рівні сприйняття:

1) індивідуальний;
2) груповий;
3) організаційний;
4) суспільний.

Індивідуальний рівень. Метою впливу ЗМІ на індивідуальний рівень може бути вироблення в індивіда:

- *усвідомлення*. ЗМІ доносить інформацію про певний об'єкт і висвітлює його значимість;
- *знання*. Важливою функцією мас-медіа є передача інформації великій кількості людей. Оволодіння знаннями є вагомим результатом, оскільки це веде до створення бажаного ставлення до певного об'єкта і стає необхідною умовою для подальшого формування у людини певної поведінки;

- *ставлення.* ЗМІ можуть корегувати ставлення аудиторій до певних об'єктів. Більш того, ставлення передбачає наявність цінностей і переконань, що можуть стати підставою до активних дій;
- *самодієвість*. Віра людини у здатність змінювати свою поведінку є важливим чинником у виборі й підтримці здорової поведінки. У даному випадку ЗМІ можуть використовуватися, щоб стимулювати розвиток самодієвості кількома шляхами, що зокрема містять: моделювання інтересу до поведінки, навчання вмінням, необхідним для прийняття певної моделі поведінки, заохочення простої тимчасової поведінки, такої, як пробна поведінка тощо;
- *вміння*. ЗМІ транслюють певні навички та вміння і заохочують аудиторію їх прийняти. У кінцевому результаті поведінка індивіда може змінитися повністю.

Рівень групи. ЗМІ можуть сприяти змінам у поведінці спілкування в межах соціальних груп. Кількість і види цих взаємодій можуть бути важливими цілями на рівні групи. ЗМІ намагаються залучати членів сім'ї, друзів, співробітників та інших до загальних дискусій.

Рівень організації. Об'єктами впливу ЗМІ тут зазвичай є робочі місця, школи, супермаркети та інші торгові точки роздрібної торгівлі тощо. Зазвичай використовуються друковані видання, наприклад, пам'ятні записки, інформаційні бюлетені і брошури. Вони розраховані на певні групи і пристосовані до певного контексту.

Рівень суспільства. Існує чотири русла впливу медіа на рівні суспільства:

1. Середовище суспільної інформації.

Кампанії мас-медіа є сильним засобом впливу на цю ланку, бо їм важливо створити таке середовище, яке сприятиме поширенню, впровадженню і засвоєнню необхідної інформації.

2. Громадська думка.

Громадська думка відіграє важливу роль у реалізації й підтримці державної політики, у розподілі суспільних ресурсів. Є твердження, що той, хто володіє засобами масової інформації, володіє громадською думкою.

3. Державна політика.

Мас-медіа можуть підтримувати урядові позиції і культивувати політику прийняття їхніх регулювань громадськістю.

4. Соціальні норми.

2. Питання. Види маніпулювання суспільною свідомістю

Маніпулятор може переслідувати різні цілі. Це впливає на те, які прийоми він використовуватиме для їхнього досягнення.

Види маніпуляції:

- вплив силою;
- вплив аргументацією;
- вплив авторитетом.

Маніпулювання масовою свідомістю — програмування думок і прагнень людей, їхніх настроїв і психічного стану з метою забезпечення такої поведінки, яка необхідна групі небагатьох власників засобів маніпуляції, що здійснюють такий вплив, переслідуючи свої особисті корисливі цілі.

Маніпулювання натовпом — це навмисне використання способів, заснованих на принципах психології натовпу для залучення, контролю або впливу на бажання юрби, задля спрямування її поведінки на певну дію. Ця практика є спільною для релігії, політики та бізнесу і може сприяти схваленню, засудженню або байдужості до особи, політики чи продукту.

Вікно Овертона

Теорію названо на честь віце-президента Макінакського центру громадської політики електроінженера, юриста ***Джозефа Овертона*** (1960 - 2003), який у 1990-х роках описав технологію того, як можна змінити ставлення суспільства до речей, які раніше вважалися абсолютно неприйнятними. Згідно з "Вікном Овертона", для кожної ідеї або проблеми в суспільстві існує т. зв. "вікно можливостей". У межах цього вікна ідеї можуть або не можуть широко обговорювати, відкрито підтримувати, пропагувати, намагатися закріпити законодавчо.

Дж. Овертон описав технологію, яка дозволяє легалізувати абсолютно будь-яку ідею. Це не концепція, а працююча технологія, тобто послідовність дій, виконання якої незмінно призводить до бажаного результату. Відповідно до теорії Овертона, ідея проходить кілька стадій, перш ніж стати соціально схваленою.

Вікно Овертона – це один із способів пояснити, як неприйнятні табуйовані ідеї стають мейнстримом і навпаки. Вікно Можливостей Овертона відіграє ключову роль у розумінні політичних динамік. Воно дозволяє нам вивчити, як суспільство взаємодіє з ідеями, перетворюючи їх з немислимих в політичну реальність. Вивчаючи різні етапи цього процесу – від мобільності та

гнучкості до стратегічних маніпуляцій – ми можемо отримати детальніше уявлення про рух політичних течій.

Оціночна шкала "Вікна Овертона" (*Джошуа Тревіньйо*)

- ❖ Неприйнятне;
- ❖ Радикальне;
- ❖ Прийнятне;
- ❖ Розумне;
- ❖ Популярне;
- ❖ Чинна норма.

Простота та наглядність ідеї створили цьому терміну помітну популярність, при цьому до початкової концепції деякі автори додали ідею про можливість свідомих маніпуляцій рамками вікна дискурсу.

Сам *Дж. Овертон* і популяризатори терміну хоча й допускали можливість маніпуляцій рамками дискурсу, але вважали поширення неправдивої інформації поганою політикою. Концепція залучалася для пояснення несподіваних явищ у суспільному і політичному житті різних країн світу. Концепція "вікна Овертона" ніколи не була перевірена та критикується дослідниками в галузі соціальних наук.

Завдання на самостійну роботу

1. Дезінформація як засіб впливу на людину.
2. "Вікна Овертона" у маніпулятивних технологіях.
3. Сугестивні технології маніпулятивного впливу.

Питання до самоконтролю

1. Основні складові маніпуляції.
2. Рівні маніпулювання.
3. Фактори впливу на діяльність ЗМІ.
4. Оціночна шкала "Вікна Овертона".

Семінар 14. Заняття 6/8. Технології маніпулювання свідомістю людини.

Навчальні питання.

1. Методи маніпулювання свідомістю людини.
2. Дезінформація як засіб впливу на людину.
3. Пропаганда.

4. Сугестивні технології маніпулятивного впливу.

Семінар 15. Заняття 6/9. Маніпулятивні технології в засобах масової інформації (ЗМІ).

Навчальні питання.

1. Фактори впливу на діяльність ЗМІ.
2. Базові захисні установки захисту від маніпулювання.
3. Характеристика впливу радіо та інформаційних агентств.
4. "Вікна Овертона" у маніпулятивних технологіях.
5. Засоби розпізнавання загрози маніпулятивного впливу.

Рекомендована до теми література

1. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект : підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. В. Толубка. Київ : ДУТ, 2015. 288 с. URL: https://law.sspu.edu.ua/files/documents/books/library/3/buryachok.pdf (дата звернення: 04.01.2024).

2. Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. Київ : Видавничий дім "Кондор", 2019. 272 с. URL: http://dcmaup.com.ua/assets/files/kiberbezpeka.pdf (дата звернення: 04.01.2024).

3. Богданов О. М., Петрик В. М. Соціальна інженерія (сучасні технології та шляхи захисту): навч. посіб. Київ: ІСЗЗІ КПІ імені Ігоря Сікорського, 2018. 80 с.

4. Кулеба Д. Війна за реальність: як перемагати у світі фейків, правд і спільнот. Київ : Книголав, 2022. 384 с.

5. Теорія та практика сучасного інформаційно-психологічного протиборства: навчальний посібник. /В. В. Петрик, С. О. Гнатюк, М. М. Присяжнюк та ін. Полтава, 2022. 328 с.

6. Інформаційно-психологічне протиборство: підручник. Видання друге перекладене, доповнене та перероблене /В. М. Петрик, М. М. Присяжнюк, Я. М. Жарков та ін.]; за заг. ред. В. М. Петрика. Київ: Вид-во ІСЗЗІ КПІ імені Ігоря Сікорського, 2018. 388 с.

7. Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року "Про створення Центру протидії дезінформації": Указ Президента України від 19 березня 2021 року № 106/2021. URL: https://zakon.rada.gov.ua/laws/show/n0015525-21#Text . (дата звернення: 29.06.2024).

Лекція 9. Заняття 6.10. Загрози інформаційній безпеці інформаційно-комунікаційних мережах.

Навчальні питання.

1. Інтернет як арена сугестивного маніпулятивного впливу.

2. Соціальна інженерія в аспекті маніпулятивного впливу.

1. Питання. Інтернет як арена сугестивного маніпулятивного впливу

Комунікативні й технічні особливості організації мережі створюють сприятливі умови для сугестивного впливу на індивіда, мережеві співтовариства та більш глобально – на світове співтовариство в цілому.

Інтернет в аспекті соціальних комунікацій став ареною сугестивних маніпулятивних впливів у формі міжособистісного й міжгрупового спілкування.

Функції інтернету які використовуються для маніпулятивного впливу:

- глобальний комунікаційний канал;
- глобальний архів;
- допоміжний засіб соціалізації, самопрезентації, особистості та соціальної групи;
- нова сфера комунікативної діяльності.

Сугестія відрізняється від переконання зниженим рівнем критичності й потреби у верифікації інформації.

Причини ефективності сугестивних технологій в Інтернеті

- ✓ висока довіра до неофіційних ресурсів мережі;
- ✓ аудиторія може бути залучена до інформації з надією розв’язати будь-які проблеми;
- ✓ формування мережевих співтовариств на основі співчуття.

Щоб результативно впливати на людину, сугестивні технології в інтернеті повинні ґрунтуватися на значущих мотивах і потребах людини. За *А. Маслоу,* це початкові потреби у захищеності, визнанні, задоволенні фізичних потреб.

Сугестивному впливу найбільш піддана аудиторія, що прагне розв'язати певні проблеми:

1. Люди активно шукають інформацію про проблему, що стосується їх, і фіксують інформацію, яка надходить до них зненацька та пропонує порятунок від проблеми.

2. Сила сугестивного впливу визначається ступенем віри людей у те, що існують перешкоди, які обмежують їхню спроможність реалізовувати плани.

3. Можливість сугестивного впливу зумовлюється рівнем причетності – ступенем, до якого людина відчуває себе залученою до певної ситуації й вирішує, чи діяти їй і яким чином.

Сугестивні технології в інтернеті націлені на масовий результат. Їхнім об'єктом найчастіше виступає певне мережеве співтовариство, або *соціальна мережа.*

У соціальному контексті дослідники порівнюють соціальні мережі (СМ) із неформальними об'єднаннями громадян.

Соціальна мережа в інтернеті – *співтовариство постійних користувачів певного мережевого ресурсу, "коло своїх", об'єднаних єдиними нормами й спільністю цілей комунікації.*

Термін "соціальна мережа" був введений у 1954 році соціологом *Джеймсом Барнсом*, котрий розвинув ідею взаємозв'язку між людьми за допомогою соціограм, тобто візуальних діаграм, у яких люди подавались у вигляді точок, а зв'язки між ними – у вигляді ліній.

В інтернеті діяльність СМ не має явно вираженого альтернативного характеру, але її становлення торкається всіх традиційно сформованих просторів – моральних, економічних, політичних, правових – на кожен із яких може бути спрямований сугестивний вплив.

СМ називається в інтернеті по-різному – кіберсоціумами, віртуальними співтовариствами, онлайновими співтовариствами, кібертовариствами, що свідчить про процес формування цього явища в мережі.

Переваги соціальних мереж Інтернету перед традиційними ЗМІ:

- оперативний обмін інформацією;
- встановлення нових зв'язків;
- неформальне спілкування;
- полегшений пошук потрібної людини.

Умови виникнення й існування СМ одночасно визначають параметри сугестивного впливу на їхніх членів:

- *можливість ідентифікації* індивіда або групи (псевдонім, домашня адреса та ін.);
- *механізм контролю*;
- *наявність історії* (чинники ідентифікації індивіда в межах спільної діяльності);
- *можливість впливати на членів* співтовариства й формувати правила комунікації;
- *єдність цілепокладання й довіри*.

Мережева організація інтернету виключає цільову аудиторію в традиційному її розумінні. Передбачається, що відправлена інформація стане загальнодоступною. Відпадає необхідність націлювання сугестивного впливу на певне вузьке коло людей, поширення інформаційних потоків координується самою мережею.

Аспекти сугестії в Інтернеті

1. Сугестивний вплив на мережеве співтовариство викликає "масову", "позаколективну" поведінку, його примітна ознака – стихійне передання інформації, суб'єкт діє практично без відчуття особистого контролю над ситуацією.

2. Зростає роль інтелектуальної рецепції – здатність духу переймати готові думки й судження інших мислячих істот і давати можливість цим судженням впливати на них своєю інтелектуальною дією.

3. Формування символічних систем як установлення влади. Хто формує символічні системи, той встановлює владу.

4. Психічне зараження, психологи визначають як несвідому, мимовільну схильність індивіда до певних психічних впливів. Індивід у цьому випадку несвідомо підпорядковується зразкам поведінки інших людей.

5. Метод переконання без критичного аналізу інформації. Широко використовується в сучасних сугестивних маніпулятивних технологіях. Він ґрунтується на збільшенні обсягу інформації про потрібний продукт.

6. Формування іміджу. Так, в основі завоювання аудиторії інтернетними ЗМІ лежить віра відвідувачів мережі у достовірність інтернетінформації й незаангажованість мережевої журналістики.

Сугестивний вплив можна виявити в інтернетних дискурсах різних жанрів. До сугестивних технологій Інтернету відносять: *медіавіруси, комп'ютерні ігри, блоги, фейки, тролі, флейми, спами, флуди, симулякри* тощо.

Розглянемо деякі з них.

Медіавіруси – це медіаподії, що зумовлюють значні соціальні зміни. Вони поширюються в інформаційній сфері та вводять в її середину приховані концепції у вигляді ідеологічних кодів. Медіавірус може бути розроблений із метою боротьби проти окремої людини, партії, економіки, релігії тощо. Медіавірусне зараження може підтримуватися насадженням в інформаційних потоках мережі ірраціоналізму, як компонента міфологізації суспільної свідомості.

Комп'ютерні ігри. Їх вплив є дуже результативним, оскільки у свідомості гравців відбувається когнітивна підміна цінностей віртуального та реального світу. Комунікативні й психологічні особливості комп'ютерних ігор відкривають широкі можливості для сугестивних технологій.

Блог – це мережевий щоденник, який побудований в хронологічному порядку та відкритий для коментарів. Серйозний сугестивний потенціал блогів усвідомлюють і дослідники, і автори, і відвідувачі. Сугестивні можливості блогів - розкручування будь-якого бренда, завоювання ринку впливу, закріплення нового тренду передбачають таку послідовність: *увага – довіра – репутація – вплив.*

Властивість блогів щодо сугестивного впливу.

- Легкість публікацій.
- Доступність.
- Соціальний характер.
- Вірулентність (швидкість).
- Безкоштовність.
- Відкритість.
- Взаємозв'язок.
- Авторитетна роль автора, з яким можна безпосередньо спілкуватися.

2. Питання. Соціальна інженерія в аспекті маніпулятивного впливу

Соціальна інженерія - *галузь знань, яка вивчає особливості використання психологічних методик та шахрайських прийомів з несанкціонованого доступу до захищених інформаційних ресурсів*.

Сучасні технології соціальної інженерії різноманітні та ефективні у своїх проявах.

Головні вектори нападу, які використовуються під час проведення атак за допомогою соціальної інженерії:

- ✓ он-лайн (інтерактивно);
- ✓ телефон;
- ✓ аналіз сміття;
- ✓ фізичні підходи;
- ✓ особисті підходи;
- ✓ реверсивна соціальна інженерія.

Комп'ютерна злочинність - *узагальнюючий термін, що означає злочини, вчинені з використанням комп'ютерної техніки, тобто характеризує специфіку способу здійснення і (або) укриття злочину.*

Характерні властивості кіберзлочинності:

1) інтелектуальний характер – здійснення кіберзлочину вимагає наявності спеціальних знань;

2) анонімність і неперсоніфікованість кіберзлочинів – механізми ідентифікації глобальної мережі дозволяють особі здійснювати операції анонімно або видавати себе за іншу особу, змінювати біографічні дані або соціальний статус;

3) віддаленість кіберзлочинів;

4) висока латентність;

5) транснаціональність – більше половини злочинів вчиняється у складі організованих груп, що знаходяться на території декількох країн;

6) швидке зростання кіберзлочинності, що пов'язане із дедалі більшим розповсюдженням та здешевленням Інтернет-послуг.

Способи протидії кіберзлочинності:

- ❖ побудова урядової моделі, спрямованої на забезпечення кібербезпеки;
- ❖ створення адекватного механізму протидії кіберзлочинності, заснованого на взаємодії приватного та державного секторів;
- ❖ чітке визначення прав та відповідальності приватного та державного сектора у сфері протидії кіберзлочинності;
- ❖ створення необхідної законодавчої бази;
- ❖ визначення ключових інформаційних інфраструктур;
- ❖ основних активів, сервісів та взаємозалежностей;

❖ підвищення готовності, зменшення часу реакції на інциденти, розробка плану відновлення після збоїв та розробка механізмів захисту ключових інформаційних інфраструктур;

❖ розробка системного та інтегрованого підходу до державного управління ризиками;

❖ підготовка вітчизняних фахівців у сфері кібербезпеки;

❖ посилення міжнародної співпраці.

Під комп'ютерним тероризмом (кібертероризмом) слід розуміти умисну, політично вмотивовану атаку на інформацію, яка обробляється комп'ютером, комп'ютерну систему і мережі, що створює небезпеку для життя і здоров'я людей або настання інших тяжких наслідків, якщо такі дії були скоєні з метою порушення суспільної безпеки, залякування населення, провокації військового конфлікту.

Комп'ютерний тероризм (кібертероризм) передбачає інформаційні атаки на обчислювальні центри, центри управління воєнними мережами й медичними закладами, банківські та інші фінансові мережі, засоби передачі даних за допомогою комп'ютерних мереж.

Основні напрями кібертероризму:

➢ здійснення несанкціонованого доступу до інформаційних ресурсів (шляхом використання програмно-апаратних засобів подолання систем захисту інформаційних і телекомунікаційних систем супротивника);

➢ створення та використання шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;

➢ здобуття необхідної інформації шляхом несанкціонованого втручання в інформаційні потоки, що передаються каналами зв'язку, чи бази даних, що перебувають в електронно-обчислювальних машинах (комп'ютерах);

➢ пригнічення елементів інформаційної інфраструктури державного або приватного сектору економіки.

Особливості кібертероризму:

- інформаційна зброя;
- міжнародний характер;
- різноманітні цілі;

- високий рівень латентності;
- невисокий рівень фінансових затрат.

Напрями боротьби з кібертероризмом:

✓ уніфікація та гармонізація національного законодавства та міжнародних актів;

✓ розробка єдиного понятійного апарату;

✓ удосконалення критеріальної основи безпеки інформаційних систем;

✓ проведення наукових досліджень у сфері створення сучасних технологій

✓ виявлення та запобігання кримінальним і терористичним впливам на інформаційні ресурси;

✓ створення спеціалізованих підрозділів у сфері боротьби з комп'ютерними злочинами та комп'ютерним тероризмом із ефективною системою координації їхніх взаємодії;

✓ удосконалення міжнародної організаційно-правової взаємодії з питань протидії комп'ютерній злочинності та комп'ютерному тероризму;

✓ удосконалення багаторівневої системи підготовки кадрів у сфері інформаційної безпеки.

Завдання на самостійну роботу.

1. "Вікна Овертона" у маніпулятивних технологіях.
2. Біометрія як механізм захисту від соціальної інженерії.

Питання до самоконтролю.

1. Кібертероризм як загроза інформаційній безпеці.
2. Комп'ютерна злочинність як загроза інформаційній безпеці.
3. Методика протидії соціальної інженерії.
4. Основні теорії створення методики протидії.

Семінар 16. Заняття 6.11. Захист від загроз маніпулятивного впливу.

Навчальні питання.

1. Соціальна інженерія: сутність та сучасне застосування.
2. Основні методи соціальної інженерії.
3. Види атак із використанням соціальної інженерії.
4. Кібертероризм як загроза інформаційній безпеці.
5. Комп'ютерна злочинність як загроза інформаційній безпеці.

Семінар 17. Заняття 6.12. Проблеми захисту інформації від соціальної інженерії.

Навчальні питання.

1. Методика протидії соціальній інженерії.
2. Основні теорії створення методики протидії.
3. Соціотехнічне тестування та створення профілів персоналу.
4. Підвищення захищеності системи.
5. Біометрія як механізм захисту від соціальної інженерії.
6. Модель захисту від соціальної інженерії.

Семінар 18. Заняття 6.13. МКР з тем 1 – 6.

Рекомендована до теми література

1. Інформаційна безпека: підручник. /В.В. Остроухов, М.М. Присяжнюк, О.І. Фармагей та ін.; під. ред. В.В. Остроухова. Київ: Видавництво Ліра, 2021. 412с.

2. Інформаційна безпека (соціально-правові аспекти): підручник. / Остроухов В.В., Петрик В.М. Присяжнюк М.М. та ін.; за заг. ред. Є. Д. Скулиша. Київ: КИТ, 2010. 776 с.

3. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа]; за заг. ред. В.Б. Толубка. Київ: ДУТ, 2015. 288 с.

4. Левченко О.В. Класифікація інформаційної зброї за засобами ведення інформаційної боротьби // Сучасні інформаційні технології у сфері безпеки та оборони. 2014. № 2. С. 142–146.

5. Сугестивні технології маніпулятивного впливу: навч. посіб. / В.П. Петрик, М.М. Присяжнюк, В.В. Остроухов та ін.; за ред. Є.Д. Скулиша. Київ: Наук. вид. відділ НА СБ України. 2010. 2458с.

6. Когут Ю. “Кібервійна та безпека об’єктів критичної інфраструктури”. 2-ге видання, Дакор. 2024. 368 с. ISBN : 9786179510038. [Електронний ресурс]. Доступно: https://pravo-izdat.com.ua

6. Білюга А.Д. Кіберзброя: сучасні загрози національній безпеці та шляхи протидії // Наука і оборона № 2, 2021. С.42-49. URL: http://nio.nuou.org.ua/article/view/239047

РОЗДІЛ IV. МЕНЕДЖМЕНТ ІЗ ЗАХИСТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Тема 7. Сутність та завдання менеджменту інформаційної безпеки.

Лекція 10. Заняття 7.1. Менеджмент в інформаційній безпеці.

Навчальні питання.

1. Базове поняття менеджменту.
2. Спеціалізовані міжнародні організації у сфері інформаційної безпеці.

1. Питання. Базове поняття менеджменту

Для визначення діяльності з координації роботи людей на практиці використовують різні поняття:

- ‟управління”;
- ‟менеджмент”;
- ‟адміністрування”;
- ‟керування” тощо.

Етимологічно менеджмент походить від латинського слова ‟manus” – рука. Початково це слово означало вміння дбайливо вести домашнє господарство, майстерно володіти засобами праці, вправно працювати.

Сучасний Оксфордський словник англійської мови тлумачить поняття ‟менеджмент” не однозначно, а саме:

- менеджмент – це спосіб, манера спілкування з людьми;
- менеджмент – це вміння та адміністративні навички організовувати ефективну роботу апарату організації;
- менеджмент – це влада та мистецтво керування;
- менеджмент – це органи управління, адміністративні одиниці, підрозділи.

Види менеджменту

- Адміністративний.
- Виробничий.
- Екологічний.
- Інвестиційний.
- Інформаційний.
- Менеджмент ризиків.
- Стратегічний.
- Фінансовий.

В останні роки спостерігається певна конвергенція поглядів на те, що ж таке *менеджмент*.

❖ *У широкому розумінні менеджмент – це одночасно система наукових знань, мистецтва та досвіду, втілених у діяльності професійних управлінців для досягнення цілей організації шляхом використання праці, інтелекту та мотивів поведінки інших людей.*

❖ *У вузькому розумінні менеджмент – це процес планування, організації, керування та контролю організаційних ресурсів для результативного та ефективного досягнення цілей організації.*

Основні функції менеджменту:

- планування;
- організація;
- керування;
- контроль.

Отже, аби усвідомити сутність категорії "менеджмент", перш за все слід з'ясувати, що таке організація, які цілі її діяльності і чому будь-якою організацією потрібно управляти.

Організація *– це група людей, діяльність яких свідомо координується для досягнення загальної мети або спільних цілей.*

Основні види ресурсів організації:

- людські ресурси;
- фінансові ресурси;
- фізичні ресурси (сировина, устаткування тощо);
- інформаційні ресурси.

Задачі менеджменту інформаційної безпеки в галузі зв'язку.

Забезпечення інформаційної безпеки держави та організацій зв'язку є допоміжною діяльністю в соціальних інститутах і включає у себе реалізацію та підтримку двох процесів: процесу створення, функціонування та удосконалення системи інформаційної безпеки і процесу менеджменту інформаційної безпеки.

Система менеджменту інформаційної безпеки держави включає:

1. Планування заходів та розробку комплексної системи захисту інформації (КСЗІ).

2. Організацію забезпечення інформаційної безпеки (організація відповідних підрозділів, які забезпечують захист інформації, розробка відповідних задач, політики та стратегії щодо захисту інформації).

3. Мотивацію персоналу, який забезпечує інформаційну безпеку (впровадження організаційно-психологічних засобів). Співробітники органів безпеки можуть виступати як об'єктом, так і суб'єктом загроз, спрямованих на порушення політичної, економічної стабільності держави тощо.

4. Контроль діяльності щодо забезпечення інформаційної безпеки. Проведення діючого контролю і перевірки ефективності планування й реалізації правових форм, методів захисту інформації відповідно до обраної стратегії та концепції безпеки.

Управління інформаційною безпекою є частиною функцій інформаційної безпеки, які забезпечуються ієрархією послуг безпеки і механізмів безпеки.

Управління безпекою включає в себе такі групи функцій:

- ❖ попередження проникненню;
- ❖ виявлення вторгнень;
- ❖ стримування та відновлення;
- ❖ адміністрування безпеки.

Набір функцій попередження, необхідний для перешкоджання проникненню:

– забезпечення законного доступу до інформаційних ресурсів;

– забезпечення безпечного доступу фізичними засобами (біометричні, електронні системи доступу тощо);

– охорона об'єктів доступу;

– аналіз персонального ризику для перевірки надійності працівників;

– екранування безпеки користувачів для підтримки запитів на підтвердження надійності замовника послуги, наприклад, платоспроможності.

Набір функцій виявлення вторгнень включає в себе:

– дослідження суттєвих змін у доходах, що можуть вказати на аферу або крадіжку;

– захист елементів підтримки типу моніторингу та аналізу аварійної сигналізації: пожежної, повені, відкривання дверей, вікон тощо;

– доступ замовників до інформації порушення безпеки в їхніх частинах мережі;

– аналіз та ідентифікація аномалій і нерегулярності в даних користувача, які можуть вказувати на злом у захисті або крадіжки послуг;

– аналіз даних користувача, які характеризують його характерну поведінку;

– дослідження крадіжки службових послуг за даними його характерної поведінки;

– дослідження внутрішнього трафіка, даних характерної поведінки та інформації контрольного журналу для виявлення злому в захисті або крадіжки послуг через дії персоналу;

– сигналізація безпеки мережі;

– аудит вторгнень програм, наприклад вірусів;

– підтримки звітів порушень елементів безпеки.

Набір функцій стримування та відновлення:

– захищене зберігання ділових даних, даних замовника послуг, даних конфігурації мережі та кінцевих елементів мережі;

– підтримка запитів на звіти порушень безпеки і запитів на дії з обмеження або ізоляції обладнання або даних, виключення прав доступу, а також запитів на відновлення спотворених даних або обладнання;

– підтримка судових справ проти порушників та їхньої затримки;

– підтримка запитів до резервних файлів для відновлення послуг, конфігурації мережі, кінцевого елемента після виявлення порушення безпеки;

– адміністрування списків відміни для доступу до списків усіх ключів та сертифікатів замовника послуг, конфігурації мережі, контролю доступу, які підозрюються у непрацездатності внаслідок порушення безпеки;

– підтримка запитів на роз’єднання зовнішніх або внутрішніх зв’язків для спроби збереження даних або системи за виявлення порушення безпеки;

Набір функцій адміністрування безпеки необхідний для планування та адміністрування політики безпеки та безпеки відносно ділової інформації.

До цього набору входять функції захисту:

– політики безпеки, який забезпечують доступ до директив компанії для установлення і підтримки безпечного середовища для персоналу, технічних засобів та програмного забезпечення;

– підтримка доступу до засобів і процедур, які використовуються для відновлення мережі та спотворених даних під час порушення безпеки;

– аналіз інформації контрольного журналу для ідентифікації можливих або потенційних порушень безпеки індивідуумами або групами користувачів;

– аналіз та оцінка порушень безпеки за допомогою директив моніторингу;

– оцінка цілісності корпоративних наборів даних для захисту від несанкціонованого доступу;

– адміністрування внутрішніх та зовнішніх запитів і відповідей ідентифікації, контроль доступу, видача сертифікатів, кодування і ключі;

– управління порушенням безпеки замовника послуги для виявлення атаки на безпеку в його частині мережі;

– тестування механізмів контрольного журналу;

– управління журналом аудиту мережі, порушення безпеки мережі та кінцевих пунктів;

– адміністрування ключів та підтримка запитів на генерацію ключів, які використовуються у комунікаціях між кінцевими пунктами та іншими елементами мережі.

2. Питання. Спеціалізовані міжнародні організації у сфері інформаційної безпеки

Характер розповсюдження ІКТ, розвитку світового інформаційного простору та нових викликів, які виникають при цьому, вимагає впровадження інтернаціональних підходів до підтримки безпеки, як суто інформаційної, так і в інших її вимірах. З огляду на це, виникає потреба у формуванні міжнародної системи інформаційної безпеки (МСІБ), яка б дозволяла здійснювати ефективні заходи реагування на існуючі та потенціальні виклики, підтримувати нормальне функціонування загальносвітового інформаційного простору.

Глобалізація підходів до досягнення та підтримки інформаційної безпеки зумовлена декількома причинами.

По-перше, зміною інформаційних потреб, які вийшли на загальносвітовий рівень. Це пов’язано зі зростанням рівня інтернаціоналізації економіки і, зокрема, транснаціоналізації виробництва і капіталу.

По-друге, індустрія, що забезпечує процеси інформатизації (включно зі стандартами, технічною інфраструктурою, протоколами передачі даних тощо) набуває загальносвітового значення, насамперед у плані уніфікації. Глобальність стосується і світового рівня інформаційних послуг.

По-третє, інформаційні загрози розглядаються відносно всього світового співтовариства та організації сучасної світогосподарської системи.

По-четверте, рівень інформатизації зріс наскільки, що стало можливим говорити про виникнення глобального інформаційного суспільства з багатьма концепціями його проєктування на майбутнє.

По-п’яте, комп’ютерна або кіберзлочинність та загрози, що створюються нею, все більше набувають транснаціонального характеру.

Все це виводить завдання досягнення і підтримки інформаційної безпеки у розряд міжнародних і світових, від вирішення яких залежить прогрес людства.

Міжнародна система інформаційної безпеки (МСІБ) охоплює:

- правові інститути;
- різноманітні стандарти і методи досягнення безпеки;
- технологічні компоненти;
- структури, що забезпечують практичну реалізацію відповідних заходів.

Головними трендами, які з’явилися у сфері міжнародної інформаційної безпеки в останні роки, є:

- **б**езпека стає пріоритетом (перевагою) найвищого рівня для держав і бізнесу;
- підвищується значущість інформаційних ризиків;
- відбувається розвиток і розширення сфер кіберзлочинності;
- з’являються нові виміри інформаційної безпеки (наприклад, Інтернет речей, операції з великими даними і знаннями, прийняття рішень, що базуються на обробці даних, та ін.);
- посилюється асиметричність заходів щодо підтримки інформаційної безпеки у різних країнах і регіонах світу;
- відбувається розвиток спеціальних технологій у сфері безпеки (включно з інформаційними);
- загострюються проблеми захисту інформації та інтелектуальної власності (особливо в Інтернеті).

Розуміння цих трендів та загроз, що виникають, дозволяє розділити рівні регулювання інформаційної безпеки (національний, міжнародний і глобальний), враховуючи різні ніші, критерії та цілі.

Основні елементи МСІБ:

1) міжнародні доктринальні документи універсального характеру, присвячені інформатизації, інформаційному суспільству та інформаційній безпеці;

2) міжнародні стандарти у галузі інформаційної безпеки;

3) міжнародні професійні (спеціалізовані) установи, які займаються питанням інформаційної безпеки у різних галузях;

4) міжнародно-регіональні інститути та структури, які створюються інтеграційними об’єднаннями (на прикладі, ЄС);

5) інститути, що створюються військово-політичними організаціями (на прикладі НАТО);

6) національні доктрини, концепції та стратегії.

Головними міжнародними доктринальними документами є:

1. Окінавська Хартія глобального інформаційного суспільства (розвиток та ефективне функціонування електронної ідентифікації, електронного підпису, криптографії та інших засобів забезпечення безпеки та достовірності операцій);

2. Резолюції Генеральної Асамблеї:

- "Досягнення у сфері інформатизації і комунікацій у контексті міжнародної безпеки";
- "Створення глобальної культури кібербезпеки та оцінка національних зусиль щодо захисту найважливіших інформаційних інфраструктур";
- "Стратегія у галузі ІКТ";
- "Боротьба зі злочинним використанням інформаційних технологій".

Головними і найбільш авторитетними міжнародними професійними установами, які займаються питанням інформаційної безпеки є:

- International Telecommunication Union;
- Institute of Electrical and Electronics Engineers;
- Association for Computing Machinery;
- W3 Consortium;
- Information Systems Security Association;
- Center for Internet Security;
- International Organization for Standardization;
- Internet Engineering Task Force;
- International Computer Security Association та ін.

Ці установи реалізують практичні заходи у таких напрямах, як:

- протоколи інформаційних мереж;
- засоби шифрування даних (архітектури, алгоритми, протоколи);
- розробка правил щодо побудови інформаційних мереж обміну даними та інших елементів інфраструктури інформаційної безпеки тощо.

Також важливими елементам роботи цих структур є: обмін досвідом і знаннями, освітня діяльність, організація та підтримка різноманітних баз даних і баз знань.

Завдання на самостійну роботу

1. Системи менеджменту інформаційної безпеки.
2. Спеціалізовані міжнародні організації у сфері інформаційної безпеки.

Питання до самоконтролю

1. Поняття менеджменту.
2. Системи менеджменту інформаційної безпеки.

Семінар 19. Заняття 7.2. Менеджмент в інформаційної безпеці: поняття та його роль.

Навчальні питання.

1. Базове поняття менеджменту.
2. Системи менеджменту інформаційної безпеки.
3. Спеціалізовані міжнародні організації у сфері інформаційної безпеки.
4. Основні елементи МСІБ.
5. Характеристика МСІБ.
6. Групи функцій управління безпекою.

Рекомендована до теми література

1. Якименко І. З. Менеджмент інформаційної безпеки: конспект лекції з дисципліни. Тернопіль: 2019. 218с.

2. Інформаційна безпека: підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей та ін.; під. ред. В. В. Остроухова. Київ: Видавництво Ліра, 2021. 412с.

3. Менеджмент інформаційної безпеки: навчальний посібник для студентів спеціальності 125 "Кібербезпека" /О. Г. Корченко, М. Є. Шелест, С. В. Казмірчук, Ю. М. Ткач, Є. В. Іванченко. Ніжин: ФОП Лук'яненко В. В. ТПК "Орхідея", 2019. 408 с.

4. Менеджмент інформаційної безпеки: конспект лекцій / Бакалинський О. О., Кожедуб Ю. В., Цуркан В. В. Київ: Україна: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2017. 90 с.

5. Методи захисту системи управління інформаційною безпекою : вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT), ДСТУ ISO/IEC 27001:2015, Національний стандарт України, ДП "УкрНДНЦ", 2016, с. 28.

6. Information technology. Security techniques. Code of practice for information security controls : ISO/IEC **27002:2013**, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2013, p. 80.

Тема 8 Актуальні питання підготовка фахівців у сфері інформаційної безпеки та кібербезпеки.

Лекція 11. Заняття 8.3. Складові системи менеджменту інформаційної безпеки (СМІБ).

1. Переваги впровадження та сфери дії СМІБ.
2. Стандарти ISD /IEC 27000.

1. Питання. Переваги впровадження та сфери дії СМІБ

Підхід до управління ризиками інформаційної безпеки на базі міжнародних стандартів серії ISO є проактивним та здатним допомогти інформаційним системам організацій різних рівнів та будь-якого розміру у вирішенні проблем, що виникають в процесі забезпечення відповідності інформаційної безпеки регулятивним нормам. Основними вимогами національного нормативного забезпечення в галузі безпеки інформації та кібербезпеки, що потребують врахування є впровадження гармонізованих стандартів з проєктування та оцінки безпеки систем інформаційних технологій серії ISO/IEC 15408 та стандартів системи управління інформаційною безпекою серії ISO/IEC 27к, що забезпечують надійність і стійкість захисту інформації. Поряд із зазначеними вимогами національного нормативного забезпечення в галузі кібербезпеки з гармонізації стандартів, важливим є ознайомлення із моделлю забезпечення безпеки інформації на основі серії стандартів NIST SP 800 Національного інституту стандартів та технологій США.

Найбільш значними стандартами інформаційної безпеки у сфері управляння інформаційної безпеки є:

- критерії безпеки комп’ютерних систем;
- європейські критерії безпеки інформаційних технологій;
- федеральні критерії безпеки інформаційних технологій;
- канадські критерії безпеки комп’ютерних систем;
- загальні критерії безпеки інформаційних технологій;
- сім’я стандартів ISO.

Усі вони визнають значення процесу управління ризиками, базові методи та затверджують концепцію процесу створення, впровадження, використання, моніторингу, перевірки, підтримання та вдосконалення системи захисту організації.

Для ефективного функціонування організації доводиться ідентифікувати та управляти багатьма процесами, один з них процес управління ризиками інформаційного об’єкту. Процес управління ризиками безпеки дозволяє організаціям досягти поєднання максимальної економічної ефективності з відомим та прийнятним рівнем ризику та надає керівникам різних рівнів зрозумілий метод організації та пріоритизації ресурсів з обмеженим доступом для реалізації управління ризиками.

Реалізація управління ризиками безпеки дозволяє організаціям з розподіленими корпоративними мережами використовувати економічно ефективний контроль, що знижує ризик до прийнятного рівня. Визначення допустимого ризику та підхід до управління ризиками залежать від структури конкретної інформаційної системи, її розподіленості, оскільки не існує універсального рішення, а різні організації використовують різні моделі управління ризиками. Кожна модель пропонує власне поєднання точності, ресурсів, часу, складності та суб’єктивності.

Крім того, ефективна програма управління ризиками допоможе розподіленим корпоративним мережам забезпечити дотримання чинних законодавчих вимог із забезпечення гідного рівня інформаційної безпеки. Оцінювання ризиків організації є первинним етапом під час розробки та експлуатації захищених інформаційних систем. Через оцінки ризиків ідентифікуються загрози активам, оцінюються їхні уразливість і ймовірність виникнення загроз, а також можливий руйнівний вплив під час реалізації несанкціонованих дій.

Запропонований сценарій розрахунку ризиків складається з наступних базових складових, а саме:

– визначення методології оцінювання ризику для інформаційної системи;

– розроблення критеріїв ухвалення ризиків та визначення прийнятого рівня ризику;

– визначення активів;

– виявлення небезпеки для активів;

– виявлення вразливих місць в системі захисту;

– виявлення дій, які порушують конфіденційність, цілісність та доступність активів та інформаційної системи;

– визначення ймовірності провалу системи безпеки за наявності переважних небезпек та вразливостей;

– оцінювання рівнів ризику;

– визначення прийнятності ризику або проведення процедури скорочення, використовуючи встановлені критерії допустимості та прийнятності ризику;

– вибір завдань та засобів управління для скорочення ризиків з умов забезпечення ефективності захисту.

Етапи розробки і впровадження системи менеджменту ІБ

- інвентаризація активів;
- категорювання активів;
- оцінка захищеності інформаційної системи;
- оцінка інформаційних ризиків;
- обробка інформаційних ризиків (у тому числі визначення конкретних заходів для захисту цінних активів);
- впровадження вибраних заходів обробки ризиків;
- контроль виконання та ефективність вибраних заходів;
- роль керівництва соціального інституту в системі управління ІБ.

Одним з основних умов ефективного функціонування системи управління ІБ є залучення керівництва організації в процес управління ІБ.

Всі співробітники повинні розуміти, що,

по-перше, вся діяльність по забезпеченню ІБ ініційована керівництвом і обов'язкова для виконання,

по-друге, керівництво організації особисто контролює функціонування системи управління ІБ,

по-третє, саме керівництво виконує ті ж правила із забезпечення ІБ, що і всі співробітники компанії.

Для ефективного впровадження системи управління інформаційної безпеки в організацію, необхідно не тільки виконати всі розробки і впровадження, а також провести навчання співробітників. Навчання співробітників можна виконувати у формі очних та заочних курсів з подальшим тестуванням, доцільно організовувати навчання співробітникам за допомогою системи дистанційного навчання, в рамках якого можуть бути представлені різні курси (як для користувачів, так і для фахівців), ігрові методики навчання.

Основна складність може полягати у перевірці ефективності процедур системи управління ІБ. Тобто, для кожної процедури необхідно розробити критерії, за якими буде перевірятися її ефективність, і, крім цього, такі критерії потрібно розробити для всієї системи управління в цілому.

2. Питання. Стандарти ISD /IEC 27000

Впровадження системи менеджменту інформаційної безпеки допомагає запобігти можливим втратам, а також зберегти ресурси та збільшити довіру зацікавлених осіб. Стандарти надають модель того, як організація може розробити та впровадити *систему управління інформаційної безпеки* (СУІБ). Це допомагає забезпечити організаціям та особам конфіденційність, цілісність і доступність їхньої інформації, а також відповідає законодавству і вимогам часу. Вона робить це через систематичний та структурований підхід до управління ризиками та заходами інформаційної безпеки.

Перший стандарт з інформаційної безпеки був прийнятий на державному рівні в 1995 році і розроблений Британським інститутом стандартів BS 7799 – Part 1.

Міжнародні стандарти серії ISO (ISO/IEC 17799, ISO 27001, ISO 27002) є основоположними в сфері управління інформаційною безпекою. Вони являють собою модель системи менеджменту, яка визначає загальну організацію процесів, класифікацію даних, системи доступу, напрямки планування та удосконалення системи безпеки, відповідальність співробітників і оцінку ризику. Основна ідея стандартів серії ISO – забезпечення надійного захисту інформаційних ресурсів ІКСМ та організація ефективного доступу до даних й процесу їхньої обробки згідно з визначеними послугами. На даний момент стандартом, який визначає вимоги до побудови СУІБ, є **ISO / IEC 27001-2013.**

Стандарт ISO 27001 носить не технічний, а управлінський характер і спрямований на впровадження процесів, що дозволяють забезпечити належний рівень інформаційної безпеки організації. СУІБ базується на процедурі оцінки та аналізу ризиків, інтегральних показників захищеності ключових інформаційних активів і виборі заходів щодо мінімізації ризиків до прийнятного залишкового рівня.

ISO/IEC 27001 – міжнародний стандарт з інформаційної безпеки, розроблений спільно Міжнародною організацією зі стандартизації та Міжнародною електротехнічною комісією. Згідно з міжнародним стандартом

ISO 27001, система управління інформаційною безпекою – *це "частина загальної системи управління організації, яка заснована на оцінці ризиків, створює, реалізує, експлуатує, здійснює моніторинг, перегляд, супровід і вдосконалення загальної інформаційної безпеки".*

Стандарт ISO 27001 визначає інформаційну безпеку як: "збереження конфіденційності, цілісності та доступності інформації". ISO 27001:2005 являє собою перелік вимог до системи менеджменту інформаційної безпеки, обов'язкових для сертифікації, а стандарт ISO 27002:2005 виступає в якості керівництва із впровадження, яке може використовуватися під час проектування механізмів контролю, вибраних організацією для зменшення ризиків інформаційної безпеки.

Стандарт ISO 27001 визначає процеси, що представляють можливість:

- встановлювати, застосовувати, переглядати, контролювати і підтримувати ефективну систему менеджменту інформаційної безпеки;
- встановлює вимоги до розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та вдосконалення документованої системи менеджменту інформаційної безпеки в контексті існуючих ризиків організації.

Поряд з елементами управління для комп'ютерів і комп'ютерних мереж, стандарт приділяє велику увагу питанням розробки політики безпеки, роботі з персоналом (прийом на роботу, навчання, звільнення з роботи), забезпечення безперервності виробничого процесу, юридичним вимогам.

Вимоги цього стандарту мають загальний характер і можуть бути використані широким колом організацій:

- малими, середніми і великими;
- органами влади;
- комерційними і промисловими секторами ринку;
- фінансовими та страховими;
- сферами телекомунікацій, комунальними послугами;
- секторами роздрібної торгівлі і виробництва;
- різними галузями сервісу;
- транспортними сферами тощо.

Стандарт ISO 27001 гармонізований зі стандартами систем менеджменту якості ISO 9001:2000 та ISO 14001:2004 і базується на основних принципах. Більш

того, обов'язкові процедури стандарту ISO 9001 потрібні і за стандартом ISO 27001. Структура документації за вимогами ISO 27001 аналогічна структурі вимогам ISO 9001. Велика частина документації, потрібна за ISO 27001, вже могла бути розроблена, і могла використовуватися в рамках ISO 9001.

Таким чином, якщо організація вже має систему менеджменту відповідно, наприклад, з ISO 9001 та ISO 14001), то краще забезпечувати виконання вимоги стандарту ISO 27001 в рамках вже існуючих систем, що передбачає значне зниження внутрішніх витрат підприємства та вартості робіт щодо впровадження та сертифікації. За стандартом ISO 27001:2005 проводиться міжнародна сертифікація системи управління інформаційною безпекою.

У стандарті ISO/IEC 27001 (ISO 27001) зібрані описи найкращих світових практик у галузі управління інформаційною безпекою. ISO 27001 встановлює вимоги до системи управління інформаційної безпеки для демонстрації можливості організації захищати свої інформаційні ресурси. Цей стандарт підготовлений як модель для розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та покращення Системи Управління (менеджменту) Інформаційної Безпеки (СУІБ).

Відповідно до вимог ISO/IEC 27001 система управління інформаційною безпекою має містити такі етапи:

1 етап – планування (фаза створення переліку інформації, оцінки ризиків і вибору заходів та механізмів захисту);

2 етап – дія (етап реалізації та впровадження відповідних заходів);

3 етап – перевірка (фаза оцінки ефективності та надійності функціонування створеної системи, проведення внутрішнього аудиту системи, виявлення недоліків);

4 етап – удосконалення (виконання коригувальних дій з покращення функціонування системи).

Згідно стандарту, СМІБ складається з політик, процедур, інструкцій, практик та технологій, які допомагають захищати конфіденційну інформацію від загроз та ризиків. Іншими словами, СМІБ – це системний підхід до управління і забезпечення інформаційної безпеки в організації.

ISO 27001 описує структуру системи менеджменту інформаційною безпекою (скорочено СМІБ) для компаній незалежно від організаційної структури, розміру або орієнтації. Стрижнем тут є управління ризиками.

Основа стандарту ISO 27001 – система управління ризиками, пов'язаними з інформацією.

Система управління ризиками дозволяє отримувати відповіді на такі питання:

- ❖ на якому напрямку інформаційної безпеки потрібно зосередити увагу;
- ❖ скільки часу та коштів можна витратити на це технічне рішення для захисту інформації.

Система управління інформаційною безпекою на основі стандарту ISO 27001 дозволяє:

- зробити більшість інформаційних активів найбільш зрозумілими для менеджменту компанії;
- виявляти основні загрози безпеки для існуючих бізнес-процесів;
- розраховувати ризики і приймати рішення на основі бізнес-цілей компанії;
- забезпечити ефективне управління системою в критичних ситуаціях;
- проводити процес виконання політики безпеки (знаходити і виправляти слабкі місця в системі інформаційної безпеки);
- чітко визначити особисту відповідальність;
- досягти зниження і оптимізації вартості підтримки системи безпеки;
- полегшити інтеграцію підсистеми безпеки в бізнес-процеси і інтеграцію з ISO 9001:2000;
- продемонструвати клієнтам, партнерам, власникам бізнесу свою прихильність до інформаційної безпеки;
- отримати міжнародне визнання і підвищення авторитету компанії, як на внутрішньому ринку, так і на зовнішніх ринках;
- підкреслити прозорість і чистоту бізнесу перед законом завдяки відповідності стандарту.

Переваги застосування системи управління інформаційною безпекою на базі міжнародних стандартів серії ISO:

- *Забезпечення неперервності*. Від якості застосовуваних новітніх технологій захисту інформації залежить не тільки збереження конфіденційності та цілісності інформації, а й взагалі існування конкретних інформаційних і телекомунікаційних сервісів, послуг та програм.
- *Мінімізація ризиків*. Впровадження системи управління інформаційною безпекою дозволяє зменшити інформаційні ризики, розкрадання і неправильне

використання обладнання, пошкодження та порушення роботи інформаційної системи організації за рахунок розмежування фізичного доступу та впровадження механізму моніторингу (аудиту) стану інформаційної безпеки. Оцінка та мінімізація ризиків дозволяє ідентифікувати загрози інформаційним ресурсам та послугам, оцінити їхню уразливість і ймовірність виникнення загроз, а також можливий руйнівний вплив при реалізації несанкціонованого доступу.

- *Зниження витрат на інформаційну безпеку*. Застосування передових технологій зі створення, моніторингу та поліпшення інформаційної безпеки дозволяє знизити витратну частину бюджету, що спрямована на забезпечення інформаційної безпеки.

- *Забезпечення цілісності*, конфіденційності та доступності критичних інформаційних ресурсів ІКСМ.

- *Забезпечення комплексного та централізованого контролю рівня захисту інформації.*

Проведення комплексу заходів із побудови системи управління інформаційною безпекою відповідно до вимог стандарту ISO 27001 дозволить вирішити такі завдання.

- **Підвищення рівня безпеки.** Стандарт розроблений з урахуванням кращих світових практик забезпечення інформаційної безпеки.

- **Управління.** Стандарт передбачає побудову циклічного і керованого процесу забезпечення інформаційної безпеки.

- **Оптимізація витрат**. СУІБ дозволяє оптимізувати і обґрунтувати витрати на інформаційну безпеку.

- **Ризики.** Зниження рівня фінансових ризиків, пов'язаних з інформаційною безпекою, шляхом їхньої ідентифікації, оцінки та прийняття адекватних захисних заходів.

- **Привабливість.** Підвищення ступеня привабливості компанії на внутрішньому і зовнішньому ринках (конкурентні переваги).

- **Довіра.** Підвищення довіри з боку акціонерів, клієнтів, партнерів і контрагентів.

- **Репутація.** Підвищення рівня ділової репутації шляхом сертифікації СУІБ, яка демонструє високий рівень зрілості компанії.

Комплекс робіт з побудови СУІБ включає наступні роботи

1. Визначення області дії СУІБ.

2. Попередній аудит на відповідність вимогам ISO 27001:

- збір вихідних даних про бізнес-процеси, структурні підрозділи, інформаційно-телекомунікаційну інфраструктуру, методи і засоби забезпечення інформаційної безпеки;
- аналіз діючої організаційно-розпорядчої документації, що регламентує питання забезпечення інформаційної безпеки;
- оцінка поточного рівня відповідності вимогам стандарту ISO 27001.

3. Проведення оцінки ризиків:

- Розробка методики оцінки ризиків;
- Інвентаризація та класифікація активів;
- Формування карти загроз;
- Аналіз і оцінка ризиків;
- Розробка плану обробки ризиків.

4. Розробка процедур і документації СУІБ:

- Розробка процесів управління інформаційною безпекою;
- Розробка процесів забезпечення інформаційної безпеки;
- Розробка комплекту організаційно-розпорядчої документації, що регламентує питання забезпечення інформаційної безпеки;
- Розробка програм підвищення обізнаності з питань управління та забезпечення інформаційної безпеки;

5. Впровадження процедур і документації СУІБ:

- Впровадження процесів управління інформаційною безпекою;
- Впровадження процесів забезпечення інформаційної безпеки;
- Навчання та підвищення обізнаності співробітників в області забезпечення інформаційної безпеки.

6. Дослідна експлуатація СУІБ.

7. Сертифікаційний аудит і видача міжнародного сертифікату:

- Взаємодія з органом сертифікації;
- Консультаційна підтримка під час проходження сертифікаційного аудиту.

Результатом робіт є СУІБ організації, що відповідає вимогам стандарту ISO 27001. Вимоги стандарту є загальними, тобто документ може використовувати будь-яка організація, незалежно від типу, розміру чи сектора.

Тому він слугує спільною мовою для управління інформаційною безпекою або інструментом для всіх.

Переваги сертифікації системи менеджменту за ISO/IEC 27001

- Виявлення основних загроз безпеці для існуючих бізнес-процесів.
- Зниження вартості системи безпеки.
- Ефективне керування системою в критичних ситуаціях.
- Інформаційні активи зрозумілі для менеджменту компанії.
- Демонстрація клієнтам та партнерам прихильності до інформаційної безпеки.
- Міжнародне визнання та підвищення авторитету компанії.
- Співпраця з правильними (безпечними) постачальниками, партнерами, субконтракторами та інші.

Завдання на самостійну роботу

1. Безпека персоналу.
2. Криптографічне забезпечення.
3. Аудит системи менеджменту інформаційної безпеки.

Питання до самоконтролю

1. Сфери дії СМІБ.
2. Цілі СМІБ.
3. Організаційне забезпечення інформаційної безпеки.
4. Переваги сертифікації системи менеджменту за ISO/IEC 27001.

Семінар 20. Заняття 7.4. Характеристика СМІБ.

Навчальні питання.

1. Сфери дії СМІБ.
2. Цілі СМІБ.
3. Забезпечення СМІБ.
4. Функціонування СМІБ.
5. Оцінка ефективності СМІБ.
6. Вдосконалення СМІБ.
7. Переваги сертифікації системи менеджменту за ISO/IEC 27001.
8. Завдання відповідно до вимог стандарту ISO 27001 із побудови системи управління інформаційною безпекою.

Семінар 21. Заняття 7.5. Засоби підтримки функціонування СМІБ.

Навчальні питання.

1. Організаційне забезпечення інформаційної безпеки.
2. Безпека персоналу.
3. Криптографічне забезпечення.
4. Управління доступом.
5. Безпека комунікацій.
6. Впровадження та експлуатація інформаційних систем.
7. Аудит системи менеджменту інформаційної безпеки.

Рекомендована до теми література

1. Якименко І. З. Менеджмент інформаційної безпеки: конспект лекції з дисципліни. Тернопіль: 2019. 218с.

2. Інформаційна безпека: підручник. /В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей та ін.; під. ред. В. В. Остроухова. Київ: Видавництво Ліра, 2021. 412с.

3. Менеджмент інформаційної безпеки: навчальний посібник для студентів спеціальності 125 "Кібербезпека" /О. Г. Корченко, М. Є. Шелест, С. В. Казмірчук, Ю. М. Ткач, Є. В. Іванченко. Ніжин: ФОП Лук'яненко В. В. ТПК "Орхідея", 2019. 408 с.

4.Методи захисту системи управління інформаційною безпекою : вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT), ДСТУ ISO/IEC 27001:2015, Національний стандарт України, ДП "УкрНДНЦ", 2016, с. 28.

5. Захист інформації за стандартами NATO: Держспецзв'язку посилює співпрацю з міжнародними партнерами. 05.09.2024. URL: https://cip.gov.ua/ua/news/zakhist-informaciyi-za-standartami-nato-derzhspeczv-yazku-posilyuye-spivpracyu-z-mizhnarodnimi-partnerami (cip.gov.ua)

6. Information technology. Security techniques. Code of practice for information security controls : ISO/IEC **27002:2013**, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2013, p. 80.

7. Information technology. Security techniques. Information security management systems implementation guidance : ISO/IEC **27003:2017**, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2017, p. 45.

Лекція 12. Заняття 8.1. Напрями підготовки та удосконалення професіоналізму фахівців інформаційної безпеки та кібербезпеки України.

Навчальні питання.

1. Підготовка фахівців у сфері інформаційної безпеки у сучасному суспільстві.

2. Міжнародний досвід підготовки фахівців інформаційної безпеки та кібербезпеки.

3. Підготовка фахівців інформаційної безпеки та кібербезпеки в Україні.

1. Питання. Підготовка фахівців у сфері інформаційної безпеки у сучасному суспільстві

Інформаційна безпека й кібербезпека є невід'ємними складовими кожної зі сфер національної безпеки і, водночас, інформаційна безпека та кібербезпека є важливими самостійними складовими процесу забезпечення національної безпеки.

Фактори, які впливають на підготовку і підвищення кваліфікації фахівців з ІБ:

- розширення інформаційної сфери;
- розширення обсягу інформації, що підлягає захисту;
- ускладнення умов збереження та захисту інформації.

Сьогодні людина є основним носієм і користувачем інформації, вона є основним суб'єктом і об'єктом інформаційної боротьби, а також основним творцем та користувачем комп'ютерних систем і мереж та/або телекомунікаційних мереж і, саме тому, вона є основним суб'єктом і об'єктом кіберборотьби. Кіберпростір, кібернетичні ресурси, комп'ютерно-системна й мережева інфраструктура та інформаційні технології значною мірою впливають на рівень і темпи соціально-економічного, науково-технічного і культурного розвитку. Інформаційна безпека й кібербезпека є невід'ємними складовими кожної зі сфер національної безпеки і, водночас, інформаційна безпека та кібербезпека є важливими самостійними складовими процесу забезпечення національної безпеки

Захист інформації – складна, наукомістка і багатогранна проблема в умовах упровадження сучасних інформаційних технологій, створення

розподілених обчислювальних систем і мереж зв'язку, що набуває особливої гостроти.

Забезпечення режиму інформаційної безпеки в обстановці, що постійно змінюється і ускладнюється, вимагає:

- постійного проведення фундаментальних та прикладних досліджень явищ і процесів у цій предметній області;
- необхідну кількість підготованих і компетентних фахівців.

Державну політику в інформаційної безпеці та кібербезпеці *варто розуміти як діяльність держави в інформаційній та кібернетичній сфері, спрямовану на задоволення інформаційних потреб людини і громадянина через формування відкритого інформаційного суспільства (кібернетичного суспільства) на основі розвитку єдиного кібернетичного простору цілісної, інформаційно розвиненої держави та її інтеграції у світовий кібернетичний простір з урахуванням збереження національної ідентичності, реалізації національних інтересів за гарантування кібернетичної безпеки на внутрішньодержавному та міжнародному рівнях.*

Проблеми підготовки фахівців для структур забезпечення інформаційної безпеки (ІБ) актуальні вже для багатьох країн світу. Першочерговий інтерес викликає досвід підготовки фахівців у США, КНР, деяких країнах ЄС та в Україні.

Зміст та обсяги підготовки фахівців у цих країнах визначаються:

- ступенем їхньої вразливості в інформаційному просторі й, у першу чергу, в кіберпросторі;
- ступенем розуміння загроз інформаційній безпеці з відповідною адекватною реакцією органів державного (корпоративного) управління;
- визначеними завданнями кадрового забезпечення наявних і перспективних структур, які відповідають за інформаційну безпеку особистості, суспільства і держави.

Аналіз систем підготовки фахівців ІБ у провідних країнах світу і в Україні свідчить про достатньо спільні підходи до їх формування та розвитку, як у техносфері, так і в гуманітарній сфері.

1. Провідні країни перейшли до масової підготовки фахівців з ІБ.
2. Підготовка фахівців ІБ, як правило, проводиться за трьома групами галузей знань:

- фахівці у галузях безпеки і військових наук (інформаційна безпека, переважно технічні фахівці);

- фахівці у галузях інженерії (технічні фахівці);

- фахівці у галузях соціальних наук, бізнесу і права (гуманітарні фахівці).

Основною за чисельністю в усіх зазначених країнах є підготовка технічних фахівців ІБ. Визначені спільні проблемні питання підготовки фахівців права зі спеціалізаціями в напрямі інформаційного права, розслідування комп'ютерної злочинності тощо. Отримують розвиток тенденції комплексування навчальних планів і змісту підготовки фахівців певного напряму елементами підготовки суміжних напрямів. Базова підготовка фахівців ІБ з вищою освітою у ЗВО суттєво доповнюється розвиненою курсовою підготовкою.

Обов'язкові умови до організації підготовки фахівців ІБ:

➢ забезпечення обміну слухачами і досвідом між ЗВО, відомствами, змагальність наукових і практичних шкіл різних ЗВО;

➢ залучення до навчального процесу і діагностування фахівців відповідних структур;

➢ практична направленість навчання.

Спільні проблеми підготовки фахівців ІБ:

✓ недостатня адаптація змісту підготовки фахівців у ЗВО до сучасних потреб інформаційної безпеки;

✓ поєднання в змісті підготовки фахівців ІБ елементів освіти інших напрямів;

✓ недостатньо узгоджений зміст навчання в системі безперервної підготовки фахівців ІБ у ЗВО та курсах;

✓ необхідність узгодження змісту підготовки фахівців гуманітарного та технічного профілю;

✓ нормативно-правове забезпечення професійної підготовки фахівців ІБ та ін.

Спільні вимоги до підготовки фахівців ІБ:

❖ інформаційна безпека потребує комплексного підходу до процесу підготовки фахівців (фундаментальні та прикладні знання гуманітарних та інженерних дисциплін);

❖ загальну підготовку з питань ІБ повинні мати всі суб'єкти інформаційної діяльності;

❖ підготовка фахівців ІБ повинна будуватися на єдиній методичній і правовій основі;

❖ система підготовки фахівців в галузі ІБ має відповідати рівню наукових знань і темпам розвитку інформаційних технологій;

❖ система підготовки фахівців ІБ потребує постійного моніторингу з боку держави.

2. Питання. Міжнародний досвід підготовки фахівців інформаційної безпеки та кібербезпеки

Найбільших успіхів у підготовці фахівців інформаційної безпеки та кіберосвіти у світі досягли США, КНР, Ізраїль, Японія, країни ЕС.

У США та КНР реалізовуються масштабні проєкти перепідготовки персоналу органів державного, корпоративного і військового управління з питань ІБ. У КНР реалізовуються масштабні заходи з адаптації населення до інформаційного суспільства.

Достатньо актуальними є проблеми професійного відбору та супроводження фахівців, зокрема в процесі їхньої професійної діяльності, виховної роботи, профілактики комп'ютерної злочинності серед фахівців ІБ.

Загалом можливо стверджувати, що нарощення кількісних показників розвитку систем підготовки фахівців ІБ забезпечує певні якісні перетворення, зокрема на рівні прийняття рішень органів державного та міжнародного управління з питань розвитку ІС та забезпечення ІБ.

Важливою особливістю розвитку системи підготовки фахівців ІВ у США є гармонійне поєднання зусиль федеральних органів, відомчих та громадських структур.

Для цього, починаючи з 1991 року, створені:

❖ агентство з захисту інформаційних систем (Defense Information Systems Agency - DISA);

❖ національний центр захисту інфраструктури, який об'єднує представників влади, військових і приватного сектору;

❖ міжнародна асоціація фахівців комп'ютерних досліджень (IACIS);

❖ національний союз кібербезпеки, створений спільно урядом і промисловцями США.

Підготовка фахівців ІБ (як переважно технічного, так і гуманітарного напряму) проводиться в розвиненій мережі закладів вищої освіти (більше 150 ЗВО).

Система стандартів вищої освіти та сертифікації якості підготовки фахівців з більшості галузей знань у США є децентралізованою і забезпечується комісіями штатів (регіональними комісіями з акредитації). Водночас стандартизацією і сертифікацією підготовки фахівців ІБ у США займається федеральний орган – Рада з акредитації програм у галузі техніки і технологій (Accreditation Board for Engineering and Technology – ABET). Це, в першу чергу, напрями: комп'ютерні науки, комп'ютерна і системна інженерія (Computer Science. Computer Engineering, Systems Engineering).

Крім цього, одним з напрямів удосконалення системи підготовки фахівців ІБ є створення за ініціативою США міжнародних консорціумів. Світовим лідером з сертифікації фахівців ІБ є міжнародний консорціум з сертифікації в галузі безпеки інформаційних систем: International Information Systems Security Certification Consortium.

Для забезпечення національних потреб у фахівцях ІБ, США активно використовують імміграційні механізми, за якими періодично отримують запрошення десятки тисяч фахівців, у тому числі з країв СНД.

Основним координатором з питань інформаційної безпеки, зокрема з підготовки фахівців ІБ, є Агентство національної безпеки (NSA), яке тісно співпрацює з Міністерством оборони, його структурним підрозділом DISA, а також ЦРУ, ФБР, НАСА, Міністерством фінансів, Мінюстом, Міненерго.

Високому рівню організації взаємодії між різними федеральними відомствами, особливо між АНБ, ФБР та Міністерством оборони, сприяє спільна підготовка фахівців ІБ, обмін кадрами, в тому числі одночасне призначення високопосадовців, наприклад АНБ чи ФБР на посади заступників відповідних структур з ІБ в Міністерстві оборони тощо.

Підготовка військових фахівців ІБ (зокрема для відповідних федеральних відомств) проводиться у більшості базових ЗВО Міністерства оборони США, провідними серед них є:

- університет інформаційних технологій (Форт Гордон);
- технологічний університет Військово-Повітряних сил (ВПС, Райт-Патерсон);

- військова академія Армії США (Вест-Пойнт);
- коледж інформаційного менеджменту університету національної оборони (Форт Макнейр), який ще називають школою інформаційної війни і стратегії;
- центр і школа спеціальних методів війни імені Дж. Ф. Кеннеді (Форт-Брег) та ін.

Навчальні підрозділи цих ЗВО інтегровані з науково-дослідними, що забезпечує достатній науковий рівень і сучасну практичну підготовку фахівців. Наприклад, у військовій академії Вест-Пойнт це Факультет електронної інженерії і комп'ютерних наук та академічний навчальний і науково-дослідний центр інформаційних технологій і операцій, у складі якого є "Лабораторія досліджень і аналізу інформаційної війни".

Необхідно зазначити, що за останні роки саме кадети Вест-Пойнту стають переможцями навчань – змагань з кібернетичного захисту "Cyber Defense Exercise" між шістьма провідними академіями США за участю Агентства національної безпеки.

Спеціальні навчальні курси з інформаційної безпеки передбачені і в інших ЗВО, які надають військову освіту на різних рівнях. Також практична підготовка (спеціалізація) фахівців проводиться в інших військових навчальних підрозділах, центрах ІБ, навчання в яких є складовою основної освітньо-професійної програми чи післявузівської підготовки. До таких центрів можна віднести центри інформаційної боротьби всіх видів збройних сил, навчальні курси (Net Warfare Training) кібернетичного Командування на базі ВПС у Барксдейлі та ін.

Американський досвід у сфері кібербезпеки зазначає, що розповсюдження інформаційних засобів відкриває можливість для розвитку особистості, актуалізує вивчення змін у свідомості людини в постіндустріальному суспільстві США, у якому формується потреба якісного кадрового забезпечення галузей.

Аналіз Національної стратегії досягнення безпеки в кіберпросторі (National Strategy to Secure Cyberspace) у США, дозволяє виокремити п'ять пріоритетів діяльності США в ІТ-галузі та кібербезпеки країни:

- становлення і розвиток національної системи реагування на події в сфері інформаційної безпеки;

- реалізація комплексної системи заходів щодо зменшення загроз інформаційній безпеці;
- забезпечення підготовки фахівців у сфері комп'ютерної безпеки й забезпечення відповідального ставлення всього населення країни до питань захисту ІТ-систем;
- забезпечення захисту інформаційних систем, що мають відношення до державних органів;
- розвиток різних форм кооперації (у тому числі й міжнародної) у сфері забезпечення інформаційної безпеки.

Для забезпечення кіберзахисту США "Національна стратегія досягнення безпеки в кіберпросторі" передбачає реалізацію таких основних заходів:

- ✓ просування багатосторонньої загальнонаціональної програми з інформування та розвитку відповідального ставлення громадян країни до забезпечення безпеки тих інформаційних систем, до яких вони мають будь-який доступ;
- ✓ заохочення створення програм підготовки фахівців, які забезпечили б задоволення потреби в професіоналах;
- ✓ підвищення ефективності існуючих програм підготовки фахівців із кібербезпеки;
- ✓ підтримку зусиль приватних компаній щодо створення, поширення й забезпечення загального визнання сертифікаційних програм у сфері інформаційної безпеки.

Підготовка фахівців з кібербезпеки у США ґрунтується на оволодінні сучасними інформаційними технологіями, фундаментальними та прикладними науковими дисциплінами, що дозволяє одержувати високий рівень теоретичного та практичного навчання. Проведений аналіз дозволяє стверджувати, що США приділяють велику увагу посиленню національної безпеки, захисту цивільних прав та інтересів бізнесу тому, що науковий, технічний, військовий, фінансовий потенціал та потенціал високих технологій США є національним надбанням американського народу, що потребує захисту на державному рівні. Концентрація найбільших фінансових компаній, науково-дослідницьких установ та корпорацій, які суттєво впливають на фінансову стабільність і економічний розвиток країни, на створення та розвиток важливих

технологічних процесів підсилюють значимість управління кібербезпекою в США.

Показовим є те, що до сукупності кращих світових навчальних закладів у галузі кібербезпеки належать, саме американські заклади вищої освіти:

- Каліфорнійський державний університет Сан-Бернардіно, штат Каліфорнія, (США);
- Університет Карнегі-Меллона, Піттсбург, штат Пенсильванія (США);
- Університет Джорджа Вашингтона, округ Колумбія (США);
- Університет Індіани Блумінгтон, штат Індіана, (США);
- Канзаський державний університет Манхеттен, штат Канзас (США);
- Університет штату Пенсильванія, штат Пенсильванія (США);
- Глобальний кампус Університету Меріленда, Адельфі, штат Меріленд (США);
- Техаський університет в Сан-Антоніо, штат Техас (США).

Підготовка фахівців з управління інформаційною та кібернетичною безпекою базується на урахуванні різних категорій кібербезпеки:

❖ мережева кібербезпека (захист комп'ютерів від зловмисників, шкідливих програм);

❖ безпека додатків (захист програмного забезпечення і пристроїв від кіберзагроз);

❖ інформаційна безпека (захист цілісності і конфіденційності даних під час їхнього зберігання чи передачі);

❖ аварійна безпека і безперервність бізнесу (реагування на аварійні ситуації в сфері кібербезпеки, які призводять до втрати операцій або даних);

❖ операційна безпека (забезпечення обробки і захист даних).

Велику увагу підготовці фахівців ІБ приділяють в КНР політичне керівництво якої визначило впровадження ІКТ в усі сфери життєдіяльності першочерговими пріоритетами модернізації країни.

За більшістю абсолютних показників Китай виходить на 1-2 місце у світовому рейтингу. Саме масштабне розгортання підготовки ІТ-фахівців забезпечило спроможність країни до самостійного і масового виробництва майже усієї номенклатури засобів інформатизації.

Підготовка фахівців ІБ у ЗВО Китаю визначена пріоритетною, це при тому, що витрати на освіту в країні перевищили 3,5 відсотків ВВП.

Провідну роль у питаннях підготовки фахівців ІБ традиційно відіграють Міністерство державної безпеки і Народно-визвольна армія Китаю (НВАК), на які покладено функцію охорони інформаційних систем країни. Тим більше, що третя воєнна доктрина КНР передбачає пріоритетний розвиток спроможності держави і її збройних сил до ведення інформаційних воєн як асиметричної відповіді на перевагу США у воєнному потенціалі.

Це визначає наявність певних навчальних курсів з ІБ в багатьох ЗВО НВАК, що свідчить про намагання військово-політичного керівництва Китаю надати спроможність до застосування технологій ІБ значній частині офіцерського складу.

Провідними вищими військовими навчальними закладами НВАК з питань інформаційної безпеки за поглядами американських фахівців з управління іноземної військової освіти (Foreign МіШоїу Studies Office, Fort Leavenworth, KS) можливо вважати:

- інститут психологічної війни НВАК (м. Сіань пров. Шаньсі);
- командна академія зв'язку (м. Ухань, пров. Хубей);
- інформаційно-технічний університет (г. Шеньджоу, пров. Хенань);
- університет оборонної науки і техніки (м. Харбін);
- інженерний коледж Інженерного університету ВМС (м. Ухань, пров. Хубей);
- національний оборонний університет науки і техніки (м. Чанша, пров. Хунань) та ін.

У КНР в інтересах ІБ для вирішення проблеми перепідготовки фахівців середнього і старшого віку створюється система багаторівневої підготовки та перепідготовки фахівців залежно від їхнього віку.

КНР дуже активно вивчає досвід підготовки фахівців ІКТ у провідних країнах світу, направляє велику кількість студентів, аспірантів та молодих вчених вчитись за кордон. Це є також дуже ефективним засобом моніторингу наукових шкіл провідних університетів світу з питань ІБ.

3. Питання. Підготовка фахівців інформаційної безпеки та кібербезпеки в Україні

Сутність концепції підготовки фахівців ґрунтується на тому, що поведінка людини в життєвих ситуаціях позбавлена дискретності, побудованої на конкретних знаннях. Вона являє собою цілісне поле, яке містить у собі весь попередній досвід, що охоплює як суб'єкт (людину), так і об'єкт діяльності.

Завдяки цьому поведінка логічна, адекватна, людська. Аналогічна форма професійної поведінки спостерігається у серйозних фахівців, конкретні знання яких давно перетворилися на власне надбання, власне бачення професійних проблем, коли немає потреби щось конкретне пригадувати для того, щоб розібратися у ситуації.

Здатність людини в умовах обмеженого часу адекватно реагувати на зміни обстановки, швидко і безпомилково робити висновки та приймати логічно беззаперечні рішення слід розуміти як інтелект.

Стратегічні пріоритети підготовки професійних кадрів у сфері кібербезпеки для України.

Перший – це утвердження в суспільстві культури кібербезпеки. Для нас важливо мати поінформоване та обізнане населення, що володіє базовими навичками безпечної поведінки у кіберпросторі.

Другий – це розбудова сталої системи підготовки кадрів у сфері формальної освіти: з навчальних закладів мають виходити кваліфіковані фахівці.

Третій – розбудова системи професійної підготовки, розвиток трудового ресурсу.

Четвертий – це посилення кадрового потенціалу і формування кадрового резерву основних суб'єктів Національної системи кібербезпеки.

Рекомендації Постанови Кабінету Міністрів України з проблем підготовки кадрів з ІБ:

- ❖ збільшення чисельності фахівців, оскільки їх кількість не задовольняє існуючим потребам;
- ❖ гармонізація вітчизняної системи освіти до європейських критеріїв і стандартів, практичного приєднання до Болонського процесу;
- ❖ вдосконалення навчального процесу з метою підготовки висококваліфікованих фахівців;
- ❖ розширення номенклатури спеціальностей з ІБ.

Фундаментальні компетенції (які мають базуватися на відповідних академічних компетенціях, знаннях технологій та навичках користувача) фахівця кібербезпеки:

- ➢ демонстрація вільного використання принципів функціонування інформаційних технологій та кібербезпеки;

- реалізація практичних навиків користувачів комп'ютерною технікою і програмного забезпечення;
- репродукування і маніпулювання інформаційним текстом та зображеннями, володіння практикою візуалізації;
- демонстрація здатності конструювати знання нелінійною навігацією через області академічного знання (наприклад: аналіз контексту або графіки через Інтернет чи через інші медіа (комунікаційні) середовища;
- демонстрація здатності критично оцінити текстові або графічні характеристики цифрових ЗМІ, їхні соціальні контексти і тенденції, спрямованість, а також економічне й культурне значення;
- демонстрація вільного використання методів візуалізації або графічного подання загальних даних;
- вміння оцінити якість, доречність, повноцінність, ефективність, і адекватність інформації і безпосередньо джерела інформації для певної мети або політики організації (у тому числі повноваження і своєчасність інформації);
- демонстрація здатності аналізувати (порівняння, контраст, підсумок), інтерпретувати і висвітлювати інформацію від багатьох джерел, яка зібрана з використанням інструментів якісного менеджменту за умов подальшого розвитку організації:
- вміння забезпечувати захист інформаційних ресурсів і баз даних;
- вміння забезпечувати висвітлення інформаційних потоків даних тощо.

Для забезпечення необхідної адекватності, гнучкості й безперервності підготовки фахівців ІБ функціонує розгалужена *система курсів перепідготовки, підвищення кваліфікації та навчальних центрів у складі*:

- навчальних підрозділів післядипломної освіти ЗВО і науково-дослідних установ;
- навчальних центрів відповідних відомств;
- навчальних підрозділів великих корпорацій, компаній, підприємств:
- навчальних центрів фірм-виробників ІТ-продукції;
- філій великих міжнародних спеціалізованих ІТ-академій;
- окремих комерційних навчальних структур.

Завдання на самостійну роботу

1. Проблеми підготовки фахівців у сфері інформаційної безпеки.

2. Міжнародний досвід підготовки фахівців інформаційної безпеки та кібербезпеки.

3. Організація підготовки фахівців інформаційної безпеки та кібербезпеки в Україні.

4. Напрями удосконалення системи підготовки фахівців Україні у сфері інформаційної безпеки та кібербезпеки.

Питання до самоконтролю

1. Актуальність проблеми підготовки фахівців у сфері інформаційної безпеки.

2. Організація підготовки фахівців інформаційної безпеки та кібербезпеки в Україні.

3. Інформаційна культура фахівця Держспецзв'язку.

Семінар 22. Заняття 8.2 Підготовка фахівців у сфері інформаційної безпеки.

Навчальні питання.

1. Актуальність проблеми підготовки фахівців у сфері інформаційної безпеки.

2. Міжнародний досвід підготовки фахівців інформаційної безпеки та кібербезпеки (США, КНР, ФРН та ін.).

3. Організація підготовки фахівців інформаційної безпеки та кібербезпеки в Україні.

4. Напрями удосконалення системи підготовки фахівців у сфері інформаційної безпеки та кібербезпеки в Україні.

5. Інформаційна культура фахівця Держспецзв'язку.

6. Інформаційна культура населення України та роль фахівців в її формування.

Семінар 23. Заняття 8/3. Захист рефератів.

Рекомендована до теми література.

1. Арсенович, Л. Сучасний стан організації кіберосвіти в умовах особливого періоду. /Електронний журнал "Державне управління: удосконалення та розвиток". 2022. № 9.

2. Арсенович, Л. "Формування системи підготовки фахівців у сфері кібербезпеки органів публічної влади в умовах глобалізації", Публічне управління в умовах глобалізації [Public administration in the context of globalization], Міжнародна студентська наукова конференція [International student scientific conference], ВАПН-NSG Київ, Україна, 07.12.2018 p, available at:https://internconferences.io.ua/s2640916/arsenovich_leonid.07.12.2018r._za_red._v.bebika.k._vapn-nsg (Accessed 30 Jan 2024).

3. Бистрова Б. "Основні поняття досягнення та концептуальні засади професійної підготовки фахівців із кібербезпеки", Педагогічні науки: теорія, історія, інноваційні технології, 2017. Вип. 8. С. 58–70.

4. Горлинський В.В., Горлинський Б.В. Освітні пріоритети підготовки фахівців з кібербезпеки в умовах воєнного стану в державі. Збірник «Інформаційні технології та безпека» July-December, 2024, Vol. 12. Iss. 2(23). С. 268-282. DOI: https://doi.org/10.20535/2411-1031.2024.12.2.315746.

5. Горлинський В.В., Горлинський Б.В. Аналіз ключових чинників формування системи компетентностей фахівців у галузі кібербезпеки // Information Technology and Security. July-December 2021. Vol. 9. Iss. 2. P. 219–231. Доступно: https://doi.org/10.20535/2411-1031.2021.9.2.249976

ПЕРЕЛІК ПИТАНЬ, ЯКІ ВИНОСЯТЬСЯ НА СЕМЕСТРОВИЙ КОНТРОЛЬ

1. Сутність, задачі національної безпеки.
2. Об’єкти національної безпеки.
3. Види національної безпеки.
4. Значення знання концептуальних засад національної безпеки для фахівців Держспецзв’язку.
5. Інформаційна безпека держави: сутність, структура.
6. Об’єкти інформаційної безпеки держави.
7. Структура інформаційного впливу.
8. Об’єкти інформаційного впливу.
9. Загальні інтереси держави у сфері інформаційної безпеки.
10. Інформаційна політика держави.
11. Геополітичні особливості сучасного інформаційного простору.
12. Стратегія формування єдиного інформаційного простору держави.
13. Стратегія розвитку єдиного інформаційного простору України.
14. Гендерні стереотипи та комунікативні моделі.
15. Гендерні особливості інформаційного впливу.
16. Роль інтернет-ресурсів у популяризації гендерної проблематики.
17. Загальна характеристика зовнішніх загроз держави у сфері інформаційної безпеки.
18. Загальна характеристика внутрішніх загроз держави у сфері інформаційної безпеки.
19. Інформаційна зброя: особливості та класифікація.
20. Інформаційна війна.
21. Спеціальні інформаційні операції в інформаційній політиці.
22. Зробіть порівняльний аналіз визначень щодо інформації.
23. Принципи, суб’єкти та об’єкти інформаційних відносин.
24. Визначення понять “інформаційна сфера”, “безпека інформаційної сфери”, “інформаційна діяльність”, “інформаційні ресурси”, “інформаційна структура”, “інформаційний суверенітет”.
25. Співвідношення понять “безпека інформації”, “безпека інформаційної сфери” та “інформаційна безпека”.
26. Визначіть поняття “інформаційна безпека”, “інформаційна безпека”,

“інформаційна безпека особи”, “інформаційна безпека суспільства”, “інформаційна безпека держави”.

27. Реальні та потенційні загрози інформаційній безпеці України.

28. Форми та види інформаційного протиборства.

29. Розкрийте співвідношення понять “інформаційне протиборство”, “інформаційна війна”, “спеціальна інформаційна операція”, “акція інформаційного впливу”.

30. Форми та види інформаційного протиборства. Розкрийте співвідношення понять “інформаційне протиборство”, “інформаційна війна”, “спеціальна інформаційна операція”, “акція інформаційного впливу”.

31. Дайте визначення та розкрийте завдання інформаційної війни (ІВ).

32. Назвіть об’єкти посягань, об’єкти деструктивного інформаційного впливу та форми ІВ.

33. Назвіть сім складових ІВ та основні компоненти ІВ у військовій сфері.

34. Охарактеризуйте етапи, ознаки та суб’єктів проведення спеціальних інформаційних операцій (СІО).

35. Методи СІО, дайте визначення та розкрийте форми дезінформування і пропаганди.

36. Форми диверсифікації громадської думки, психологічного тиску й поширення чуток.

37. Джерела загроз інформаційній безпеці особи та суспільства.

38. Рівень ефективності проведення інформаційно-психологічного впливу (ІПсВ).

39. Зміни в індивідуальній свідомості, до яких можуть призвести небезпечні ІПсВ.

40. Види ІПсВ.

41. Дайте визначення таким поняттям як “маніпулювання”, “об’єкт маніпулювання”, “суб’єкт маніпулювання”, “жертва маніпулювання”, “інструмент маніпулювання”, “мішені маніпулювання”.

42. Визначення і базові методи ІПсВ. Розкрийте алгоритми здійснення переконання та навіювання.

43. Розкрийте п’ять груп “мішеней маніпулювання”.

44. Опишіть вектори нападу методами соціальної інженерії під час використанні мережі Інтернет.

45. Розкрийте засоби і методи соціального інженера спрямовані на якості людської природи.

46. Охарактеризуйте базові методи захисту від атак за допомогою соціальної інженерії.

47. Розкрийте основні фази активного захисту від соціальної інженерії.

48. Базове поняття менеджменту.

49. Системи менеджменту інформаційної безпеки.

50. Спеціалізовані міжнародні організації у сфері інформаційної безпеки.

51. Сфери дії СМІБ.

52. Цілі СМІБ.

53. Забезпечення СМІБ.

54. Функціонування СМІБ.

55. Оцінка ефективності СМІБ.

56. Вдосконалення СМІБ

57. Організація підготовки фахівців інформаційної безпеки та кібербезпеки в Україні.

58. Напрями удосконалення системи підготовки фахівців у сфері інформаційної безпеки та кібербезпеки в Україні.

59. Розкрийте природу й основні види ризику у сфері кібербезпеки.

60. Визначити основні терміни стосовно менеджменту ризиків.

61. Охарактеризувати призначення, мету, принципи менеджменту ризиків.

62. Проаналізуйте чинники прояву ризиків.

63. Охарактеризувати впровадження стилю менеджменту ризиків.

64. Охарактеризувати впровадження процесу менеджменту ризиків.

65. Охарактеризувати контролювання стилю менеджменту ризиків.

66. Охарактеризувати процесну модель менеджменту ризиків.

67. Розкрийте етапи (стадії) менеджменту ризиків.

68. Охарактеризувати встановлення контексту менеджменту ризиків.

69. Охарактеризувати оцінювання ризиків.

70. Охарактеризувати ідентифікування ризиків.

71. Охарактеризувати аналізування ризиків.

72. Охарактеризувати атестування ризиків.

73. Охарактеризувати обробляння ризиків.

74. Охарактеризувати шляхи зменшення ризиків.

75. Визначити основні терміни за стандартом ISO/IEC 27000.

76. Охарактеризувати вимоги стандарту ISO/IEC 27001 до побудови СМІБ.

77. Розкрийте загальну характеристику кіберзлочинності.

78. Зробіть системний аналіз соціальної інженерії.

79. Проаналізуйте заходи з протидії атакам за допомогою соціальної інженерії.

80. Розкрийте принципи дії та особливості застосування інформаційної та сейсмічної зброї.

81. Організаційне забезпечення інформаційної безпеки.

82. Безпека персоналу.

83. Криптографічне забезпечення.

84. Управління доступом.

85. Безпека комунікацій.

86. Впровадження та експлуатація інформаційних систем.

87. Аудит системи менеджменту інформаційної безпеки: сутність та цілі.

88. Внутрішній аудит системи менеджменту інформаційної безпеки.

89. Зовнішній аудит системи менеджменту інформаційної безпеки.

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ДО ВИКОНАННЯ ІСЗ (РЕФЕРАТУ)

Реферат – один із важливих видів самостійної роботи курсантів, який допомагає більш глибоко вивчати одну з проблем курсу, опрацювавши відповідну наукову, та методичну літературу. Підготовка рефератів сприяє виробленню навичок самостійного аналізу матеріалу, систематизації та його вільного викладу. ***Реферат*** *(referre – з лат. повідомляти, доповідати)* – це дослідження, огляд наукових і правових джерел, спрямований на вивчення, аналіз і узагальнення ідеї, викладених у наукових працях з визначеної проблеми. Загальний обсяг реферату має становити 25 – 30 рукописних (надрукованих) аркушів, оформлених як наукова робота. Структурно реферат складається з титульного аркушу, змісту, вступу, двох, трьох питань, висновків та списку використаної літератури. Автор реферату має підготуватися до виступу на семінарі, щоб на вимогу викладача протягом 5–10 хвилин викласти суть проблеми, що розглядається в рефераті. Оформлений згідно з вимогами до наукових робіт, реферат оцінюється викладачем.

Загальними вимогами до реферату є:

- чіткість та логічна послідовність викладення матеріалу;
- переконливість аргументації;
- стислість і точність формулювань, які виключають можливість неоднозначного тлумачення;
- конкретність викладення результатів дослідження;
- наукова обґрунтованість висновків;
- зв’язок з майбутньою професійною діяльністю.

Підготовка до написання рефератів починається зі складання бібліографії – списку використаної літератури (не менш десяти назв першоджерел, монографій, наукових статей) та її опрацювання. У ***вступі*** розкривається важливість та актуальність проблеми, стан її висвітлення у літературі, обов’язково визначаються мета та завдання реферату.

В основній частині, що складається з 2–3 питань, потрібно зробити *огляд літератури* за темою, у логічній послідовності, аргументовано, з посиланнями на джерела, розкрити зміст кожного питання з відповідними *висновками*, що узагальнюють результати аналізу його опрацювання в наукових і правових джерелах. ***У загальних висновках*** наводять узагальнюючу оцінку отриманих результатів дослідження стосовно суті питань, що розглядались у роботі,

визначається наукова та практична цінність виконаної роботи. Наприкінці, потрібно підкреслити *значущість набутих знань для розв'язування комплексних проблем наукового напрямку та у професійній діяльності фахівця Держспецзв'язку.* Викладати матеріал слід сучасною українською мовою, короткими чіткими фразами, правильно оформлюючи науковий апарат. Наприкінці реферату подається ***список використаної літератури*** (джерел). Список використаних джерел – елемент бібліографічного апарату, котрий містить бібліографічні описи використаних джерел згідно з державним стандартом: вказується прізвище автора, його ініціали, повна назва книги, місце видання та рік видання, загальна кількість сторінок; для наукових статей додається номер журналу та номери сторінок публікації.

Загальні правила цитування. Цитування повинно бути повним, допускається пропуск слів, речень, абзаців без перекручення авторського тексту. Випущений текст замінюється трьома крапками. При непрямому цитуванні (переказі) слід бути гранично точним у викладанні думок автора і давати відповідні посилання на джерело. Посилання у тексті реферату на джерело слід зазначати порядковим номером за переліком джерел, виділеним двома квадратними дужками, наприклад: "... у працях [1-3]...". Якщо використовують відомості, матеріали з джерел із великою кількістю сторінок, то у посиланні необхідно точно вказати номери сторінок, наприклад: [1, с.3].

До технічного оформлення реферату висуваються наступні вимоги – робота має бути надрукована з одного боку паперу формату А4. Робота набираються 14 шрифтом із полуторним інтервалом. Аркуш реферату повинен мати наступні рамки поля: ліве – 25 мм., праве – 15 мм., верхнє – 20 мм. та нижнє – 20 мм. Нумеруються всі сторінки реферату, починаючи з титулу, але на ньому номер сторінки не проставляють. Абзацний відступ повинен бути однаковим упродовж усього тексту роботи і дорівнювати п'яти знакам (1,25 см.).

На титульному аркуші реферату зазначаються: назва інституту, кафедра, назва дисципліни, тема, прізвище, ім'я по батькові виконавця, курс, група, науковий ступінь, вчене звання прізвище, ім'я, по батькові особи, що має провірити реферат, місто та рік. Друга сторінка має містити план реферату, що складається із вступу, двох або трьох питань та висновки. Остання сторінка містить перелік використаної літератури.

КРИТЕРІЇ ОЦІНЮВАННЯ ВИКОНАННЯ КУРСАНТОМ ІСЗ

Якість виконання курсантом ІСЗ (реферату) оцінюється за такими загальними показниками:

- опанування змістом теми і літературою, що була використана;

- якість виконання текстової частини реферату, відповідність змісту теми реферату вимогам до наукових праць;

- якість оформлення реферату згідно з формальними вимогами;

- актуальність і зв'язок теми з майбутньою професійною і службовою діяльністю.

Максимальний бал за ІСЗ (реферат) оцінюється в 25 балів за такими критеріями:

– "відмінно" – творчий підхід, всебічне, глибоке, логічне, аргументоване розкриття проблеми з посиланням на наукові джерела, обґрунтуванням її значущості для майбутньої соціальної і професійної діяльності та розвитку світогляду – 23-25 балів;

– "добре" – повне, науково обґрунтоване, логічне розкриття проблеми з відображенням власної позиції – 19-22 балів;

– "задовільно" – неповне і недостатньо аргументоване розкриття проблеми з певними недоліками – 15-18 балів;

– "незадовільно" – ІСЗ не виконане, тобто ІСЗ не зараховано – 0 балів.

Наявність позитивної оцінки за ІСЗ є умовою допуску до залікової контрольної роботи.

РЕКОМЕНДОВАНА ТЕМАТИКА РЕФЕРАТІВ.

1. Теоретичні погляди на безпеку, її сутність, зміст і класифікацію.
2. Державна безпека України: місце в системі національної безпеки.
3. Інформаційна безпека України, її сутність і характеристика.
4. Загальна характеристика видів національної безпеки.
5. Основи, цілі та принципи національної безпеки і оборони України.
6. Пріоритети і правові засади забезпечення кібербезпеки і безпеки інформаційних ресурсів.
7. Інформаційна безпека: сутність, структура, загальна характеристика.
8. Воєнна безпека: сутність, зміст і призначення.
9. Сектор безпеки і оборони, національна політика держави.

10. Місце і завдання Держспецзв’язку в секторі безпеки і оборони України.

11. Воєнна безпека держави як складова національної безпеки.

12. Стратегія сталого розвитку і національна безпека України.

13. Кіберпростір і кібербезпека у міжнародних відносинах.

14. Міжнародні стандарти прав і свобод людини у світовому і національному кіберпросторі.

15. Інформаційне суспільство, інформаційний простір та інформаційна безпека.

16. Інформаційна безпека, як чинник і передумова сталого розвитку суспільства.

17. Міжнародні документи про права людини та їх захист у кіберпросторі.

18. Гендерні аспекти організації інформаційної та інформаційно-психологічної безпеки.

19. Сутність, мета, форми і технології інформаційно-психологічного протиборства.

20. Спеціальні інформаційні операції: цілі, ознаки, суб’єкти та етапи.

21. Сутність, цілі, засоби і компоненти ведення інформаційних і кібервійн.

22. Теорія вікон Овертона в аспекті маніпулювання свідомістю.

23. Сугестивні технології маніпулятивного впливу в Інтернеті.

24. Проксі- та нелінійні війни сучасності.

25. Роль інформаційної складової у сучасних гібридних війнах.

26. Інформаційний тероризм та інформаційна безпека в сучасних умовах.

27. Засоби масової комунікації як інструмент інформаційних війн.

28. Маніпулятивні технології сучасних соціальних мереж.

29. Соціальна інженерія в аспекті інформаційної безпеки людини.

30. Методи профілактики наслідків негативного інформаційно-психологічного впливу на військовослужбовців.

31. Методики протидії негативному інформаційно-психологічному впливу на військовослужбовців під час виконання службово-бойових завдань.

32. Основні методи, що застосовуються у технологіях соціальної інженерії та способи захисту.

33. Психологічні війни та операції як складові морально-психологічного впливу в сучасному світі.

34. Теорія нейролінгвістичного програмування як модель програмування людської поведінки та комунікацій.

35. Цілі, форми, методи та особливості здійснення сугестивного впливу через Інтернет і засобами комунікації та способи захисту.

36. Засоби масової інформації як інструмент впливу на інформаційний простір в умовах гібридної війни.

37. Інформаційна безпека держави в умовах глобалізації.

38. Система забезпечення інформаційної безпеки України.

39. Перспективи та проблеми інтеграції України у світовий інформаційний процес.

40. Нейролінгвістичне програмування як інструмент сугестивного маніпулятивного впливу.

41. Сучасні маніпулятивні технології в засобах масової інформації.

42. Комп'ютерна злочинність та кібертероризм як загрози інформаційній безпеці.

43. Причини, умови виникнення та наслідки злочинів у сфері використання ПЕОМ.

44. Державна політика у сфері інформаційної безпеки України.

45. Формування позитивного іміджу України у світовому інформаційному просторі.

46. Фундаментальні національні інтереси держави згідно із Законом "Про національну безпеку України".

СПИСОК ВИКОРИСТАНИХ ТА РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. Національна безпека держави в сучасних умовах: монографія. /Ананьїн В. О., Ананьїн О. В., Горлинський В. В., Пучков О. О., Терещенко О. М., Уваркіна О. В. За ред. В. О. Ананьїна. Київ : ІСЗЗІ КПІ імені Ігоря Сікорського. Вид-во "Політехніка", 2021. 346 с.

2. Теорія та практика сучасного інформаційно-психологічного протиборства: навчальний посібник. /В. В. Петрик, С. О. Гнатюк, М. М. Присяжнюк та ін. Полтава, 2022. 328 с.

3. Інформаційно-психологічне протиборство: підручник. Видання друге перекладене, доповнене та перероблене /В. М. Петрик, М. М. Присяжнюк, Я. М. Жарков та ін.]; за заг. ред. В. М. Петрика. Київ: Вид-во ІСЗЗІ КПІ імені Ігоря Сікорського, 2018. 388 с.

4. Богданов О. М., Петрик В. М. Соціальна інженерія (сучасні технології та шляхи захисту): навч. посіб. Київ: ІСЗЗІ КПІ імені Ігоря Сікорського, 2018. 80 с.

5. Ананьїн В. О., Горлинський В. В., Пучков О. О. Міжнародна безпека та євроатлантична інтеграція України: навч. посіб. Київ : ІСЗЗІ КПІ ім. Ігоря Сікорського, 2020. 231 с.

6. Інформаційна безпека: підручник /В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін; під. ред. В. В. Остроухова. Київ : Вид-во Лира-К, 2021. 412 с. URL: https://lira-k.com.ua/preview/12867.pdf (дата звернення: 14.02.2024).

7. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 "Управління інформаційною безпекою", 125 "Кібербезпека"/ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. Ніжин : ФОП Лук'яненко В.В. ТПК "Орхідея", 2018. 166 с.

8. Безпека України: актуальні проблеми та критерії оцінки. Монографія / В. О. Ананьїн, В. В. Горлинський, Л. О. Євдоченко, О. О. Пучков. За заг. ред. В. О. Ананьїна. Київ : ІСЗЗІ КПІ ім. Ігоря Сікорського, 2018. 240 с.

9. Менеджмент інформаційної безпеки: конспект лекцій / Бакалинський О. О., Кожедуб Ю. В., Цуркан В. В. Київ: Україна: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2017. 90 с.

10. Менеджмент інформаційної безпеки: навчальний посібник для студентів спеціальності 125 "Кібербезпека" /О. Г. Корченко, М. Є. Шелест, С. В. Казмірчук,

Ю. М. Ткач, Є. В. Іванченко. Ніжин: ФОП Лук'яненко В. В. ТПК "Орхідея", 2019. 408 с. URL: https://ir.stu.cn.ua/handle/123456789/19244

11. Золотар О. О. Інформаційна безпека людини: теорія і практика: монографія. Київ : ТОВ Видавничий дім "АртЕк", 2018. 446 с. URL: Інформаційна безпека людини:теорія і практика | Інститут інформації, безпеки і права Національної академії правових наук України (дата звернення: 29.06.2024).

12. Інформаційний вимір гібридної війни: досвід України: матеріали міжнародної наук. практ. конференції. Київ : НУОУ, 2017. 104 с. URL: https://nuou.org.ua/assets/documents/zbirn-gibr-mizhn-konf.pdf (дата звернення: 29.06.2024).

13. Мужанова Т. М. Інформаційна безпека держави: навч. посіб. Київ: ДУТ, 2019. 131 с. URL: https://duikt.edu.ua/ua/lib/1/category/742/view/1856?lang=ua&act=view&page=1&category=742&id=1856 . (дата звернення: 04.01.2024).

14. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект : підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. В. Толубка. Київ : ДУТ, 2015. 288 с. URL: https://law.sspu.edu.ua/files/documents/books/library/3/buryachok.pdf (дата звернення: 04.01.2024).

15. Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. Київ : Видавничий дім "Кондор", 2019. 272 с. URL: http://dcmaup.com.ua/assets/files/kiberbezpeka.pdf (дата звернення: 04.01.2024).

16. Алещенко В. І Інформаційно-психологічна складова безпеки особистості в умовах війни. Вісник Національного університету оборони України, № 2 (66). 2022. С. 5- 17. URL: http://visnyk.nuou.org.ua/article/view/255150 (дата звернення: 04.01.2024).

17. Загородня Ю. В. Кібербезпека як інноваційний захист у політичному просторі України. Вісник Національного технічного університету України "Київський політехнічний інститут". Політологія. Соціологія. Право. 2021. №. 4 (52). С. 33–38. URL:https://visnyk-psp.kpi.ua/article/view/248130/ . (дата звернення: 04.01.2024).

18. Кулеба Д. Війна за реальність: як перемагати у світі фейків, правд і спільнот. Київ : Книголав, 2022. 384 с.

19. Світова гібридна війна: український фронт /За заг. ред. В. П. Горбуліна. Київ: НІСД, 2017. 496 с. URL: http://resource.history.org.ua/item/0013707 .(дата звернення: 04.01.2024).

20. Когут Ю. “Кібервійна та безпека об’єктів критичної інфраструктури”. 2-ге видання, Дакор. 2024. 368 с. ISBN : 9786179510038. [Електронний ресурс]. Доступно: https://pravo-izdat.com.ua .(дата звернення: 10.07.2024).

21. Управління інноваціями (Програма, курс лекцій, практичні заняття, самостійна робота, індивідуальні завдання, тести). Навч.-метод. посібник. / І. І. Стойко /Тернопіль, ТНТУ імені Івана Пулюя, 2018. 200 с.

22. Методичні рекомендації з інтеграції ґендерних підходів у систему підготовки фахівців для сектору безпеки і оборони України. URL: https://ukraine.unwomen.org/uk/digital-library/publications/2021/11/guidelines-on-integrating-gender-approaches-in-training-specialists (дата звернення 26.05.2024).

23. Білюга А. Д. ,Кіберзброя: сучасні загрози національній безпеці та шляхи протидії // Наука і оборона № 2, 2021. С.42-49. URL: http://nio.nuou.org.ua/article/view/239047

24. Горлинський В.В., Горлинський Б.В. Освітні пріоритети підготовки фахівців з кібербезпеки в умовах воєнного стану в державі. Збірник «Інформаційні технології та безпека» July-December, 2024, Vol. 12. Iss. 2(23). С. 268-282. DOI: https://doi.org/10.20535/2411-1031.2024.12.2.315746.

25. Горлинський В.В., Горлинський Б.В. Аналіз ключових чинників формування системи компетентностей фахівців у галузі кібербезпеки // Information Technology and Security. July-December 2021. Vol. 9. Iss. 2. P. 219–231. DOI: https://doi.org/10.20535/2411-1031.2021.9.2.249976

26. Конституція України [Електронний ресурс]: Закон України від 28.06.1996 р. № 254к/96-ВР // Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 14.02.2024).

27. Про інформацію: Закон України № 2658-XII від 02.10.1992 р. Верховна Рада України. Відомості Верховної Ради України. 1992. № 48. URL: https://zakon.rada.gov.ua/laws/show/2657-12Text (дата звернення 13.05.2024).

28. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.94 р. № 81/94-ВР. Редакція від 28.06.2024. // Верховна Рада України. URL https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

29. Про основні засади забезпечення кібербезпеки України . Закон України від 05.10.2017 р. № 2163-VII. URL: https:// https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 14.02.2024).

30. Про електронні комунікації. Закон України, від 16.12.2020 р., № 1089-IX, URL: https://zakon.rada.gov.ua/laws/show/1089-20#n2246 (дата звернення 13.05.2024).

31. Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки. Закон України від 09.01.2007. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text (дата звернення 13.05.2024).

32. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки". URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 29.06.2024).

33. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про стратегію кібербезпеки України": Указ Президента України. URL: http://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення: 04.01.2024).

34. Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року "Про створення Центру протидії дезінформації": Указ Президента України від 19 березня 2021 року № 106/2021. URL: https://zakon.rada.gov.ua/laws/show/n0015525-21#Text (дата звернення: 29.06.2024).

35. Рішення Ради національної безпеки і оборони України "Про План реалізації Стратегії кібербезпеки" від 30 грудня 2021 року. Указ Президента України від 1 лютого 2022 року № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text (дата звернення: 14.02.2024).

36. Рішення Ради національної безпеки і оборони України "Про Стратегію національної безпеки України" від 14 вересня 2020 року. Указ Президента України від 14 вересня 2020 року № 37/2022. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 14.02.2024).

37. Адміністрація державної служби спеціального зв'язку та захисту інформації України, Наказ № 773 від 30.08.2023 Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту систем електронного документообігу URL: https://zakon.rada.gov.ua/rada/show/v0773519-23#Text (дата звернення: 14.02.2024)

38. Методи захисту системи управління інформаційною безпекою : вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT), ДСТУ ISO/IEC 27001:2015, Національний стандарт України, ДП "УкрНДНЦ", 2016, с. 28.

39. Information technology. Security techniques. Code of practice for information security controls : ISO/IEC **27002:2013**, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2013, p. 80.

40. Information technology. Security techniques. Information security management systems implementation guidance : ISO/IEC **27003:2017**, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2017, p. 45.

41. Захист інформації за стандартами NATO: Держспецзв'язку посилює співпрацю з міжнародними партнерами. 05.09.2024. URL: https://www.kmu.gov.ua/news/zakhyst-informatsii-za-standartamy-nato-derzhspetszviazku-posyliuie-spivpratsiu-z-mizhnarodnymy-partneramy (дата звернення: 08.09.2024)

Інформаційні ресурси:

1. Центр протидії дезінформації при Раді національної безпеки та оборони України – Режим доступу: https://cpd.gov.ua/category/leadership/#

2. Портал безпека [Електронний ресурс]. – Режим доступу: https://www.bezpeka.com/uk/golovna/

3. Верховна Рада України. Законодавство України: [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/

4. Державна служба спеціального зв'язку та захисту інформації: [Електронний ресурс]. – Режим доступу: https://cip.gov.ua/ua

5. Команда реагування на комп'ютерні надзвичайні події України: [Електронний ресурс]. – Режим доступу: https://cert.gov.ua/

6. SAE Standards [Electronic Resource], Mode of access: World Wide Web., URL: http://standards.sae.org.

7. Інститут перспективного вивчення інформаційних війн (IASIW) URL: https://web.archive.org/web/20070709005214/http://www.psycom.net/iwar.1.html

ГЛОСАРІЙ

А

Аватар – графічне персоніфіковане зображення, що асоціюється з конкретним користувачем.

Анонімус – більшість відвідувачів фоловерів, які вільно висловлюють свої найсміливіші думки.

Акаунт – персональна або корпоративна сторінка у соціальній мережі.

Атака (attack) – спроба знищити, розкрити, змінити, зробити недоступним, вкрасти або отримати несанкціонований доступ або несанкціоновано використовувати інформаційні ресурси.

Б

Бан (від англійського ban – забороняти) – Жаргонний вираз:

1) спосіб покарання адміністрацією сайту за некоректну поведінку користувача або використання спамерських прийомів, який полягає у видаленні облікового запису з бази. Відновлення не гарантоване, звичайно вимагає особистого листування з адміністрацією і в будь-якому випадку займає тривалий час;

2) видалення учасника з групи за некоректну поведінку через занесення його в чорний список. Учасник групи, занесений в такий, не має можливості потрапити в групу. Після виведення з чорного списку, учасник у групі автоматично не відновлюється. Бан-лист – список користувачів, які за некоректну поведінку та з інших причин, заблоковані. Користувачі, занесені в Бан-лист, не можуть відправляти повідомлення та переглядати інформацію.

Безпека, у загальному розумінні, означає надійне існування будь-якого об’єкта за наявності всіляких йому загроз.

Безпека (національна безпека) – визначений ступінь захищеності особистості, суспільства, держави від внутрішніх і зовнішніх загроз, що дозволяє їм існувати і постійно стало розвиватися.

Безпека політична – це стан захищеності політичних інтересів особи, соціальних груп, держав від внутрішніх та зовнішніх загроз, а також система заходів щодо забезпечення цієї захищеності.

Безпека економічна – визначений рівень розвитку і стану економічної і фінансової системи, при якому гарантовані стабільний соціально-економічний розвиток та стійкість до несприятливих внутрішніх і зовнішніх впливів.

Безпека інформаційна – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Безпека науково-технологічна – це стан захищеності наукового потенціалу держави, наявних в країні конкурентоспроможних технологій, а також недопущення та усунення наслідків технологічної недосконалості господарської діяльності.

Безпека мереж і послуг – здатність електронних комунікаційних мереж і послуг протистояти діям, що становлять загрозу доступності, цілісності чи конфіденційності таких мереж і послуг, а також даних, що зберігаються, передаються чи обробляються, та пов'язаних із ними послуг, що надаються або доступ до яких здійснюється через електронні комунікаційні мережі чи послуги.

Безпека воєнна – це стан захищеності прав і свобод громадян, базових інтересів та цінностей суспільства та суверенної держави від можливих зазіхань із застосуванням воєнної сили.

Безпека екологічна – це допустимий рівень негативного впливу природних і антропогенних факторів екологічної небезпеки на навколишнє середовище та людину.

Безпека демографічна – захищеність генофонду народу від різних негативних впливів і створення сприятливих умов для його існування, розвитку і самореалізації.

Безперервність інформаційної безпеки (information security continuity) – процеси і процедури, що гарантують постійне забезпечення інформаційної безпеки.

Блог – це мережевий щоденник якій побудований в хронологічному порядку та відкритий для коментарів.

Блогер – автор мережевого блогу.

Блогосфера – мережевий простір, у рамках якого функціонують блоги.

Блогінг – процес створення й просування блогів.

Блокування інформації – дії, наслідком яких є припинення доступу до інформації.

Бот (англійське bot скорочення від robot) – віртуал, створений спеціальною програмою для виконання певної дії в соціальній мережі, як правило, розсилки спаму. На питання і повідомлення інших користувачів бот не відповідає. Звернення до боту може спровокувати візит до користувача великої кількості його "братів".

В

Веб-браузер – програмне забезпечення для перегляду веб-сайтів. Призначений для запиту веб-сторінок, їхньої обробки, виведення і переходу від однієї сторінки до іншої. Популярні веб-браузери: Mozilla Firefox, Opera, Internet Explorer, Safari, Chrome.

Вебінар – різновид веб-конференції, проведення онлайн-зустрічей або презентацій через Інтернет у режимі реального часу.

Віджет – змістовний модуль з контентом, який монтується на веб-сторінці або браузері.

Віки-проєкт – веб-сайт, структуру та зміст якого користувачі можуть самостійно створювати й змінювати за допомогою інструментів, що надаються адміністрацією ресурсу.

Вірусна реклама – активне розповсюдження (як правило, у геометричній прогресії) рекламного матеріалу, в якому беруть участь представники цільових груп.

Витік інформації – результат дій порушника, унаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї.

Втрата інформації – дія, внаслідок якої інформація перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі.

Г

Гео-сервіси – географічні інформаційні системи, картографічний сервіс.

Гендер – це сукупність соціальних та культурних норм, які суспільство наказує виконувати людям залежно від їхньої біологічної статі.

Гендерна соціалізація – це процес засвоєння людиною соціальної ролі, визначеної для неї суспільством від народження, залежно від того, чоловіком або жінкою вона народилась.

Гендерні ролі – норми та правила поведінки жінок і чоловіків в суспільстві.

Гендерна культура – це система уявлень, які формують соціокультурні аспекти статі, визначають їхні ролі й моделі поведінки у різних сферах життя

Гібридна (асиметрична) війна – засіб протистояння, який поєднує в собі комплекс різноманітних інструментів політичного, економічного, військового та ідеологічного характеру.

Д

Диверсифікація громадської думки **–** розпорошення уваги на штучно акцентовані проблеми для відволікання свідомості спільноти від вирішення нагальних першочергових проблем, необхідних для безпечної життєдіяльності особи, функціонування суспільства та держави.

Дезінформування **–** метод спеціальних інформаційних операцій (СІО), який передбачає введення об'єкта СІО в оману щодо справжності намірів для спонукання до запрограмованих, суб'єктом СІО, дій.

Державна політика в інформаційної безпеці та кібербезпеці – діяльність держави в інформаційної та кібернетичній сфері, спрямована на задоволення інформаційних потреб людини і громадянина через формування відкритого інформаційного суспільства.

Діалогові комунікаційні канали **–** канали взаємодії із цільовими групами (безкоштовні гарячі телефонні лінії, форуми та ін.)

Домен – певна зона в мережі Інтернет, виділена для забезпечення доступу до наданої на веб-сайті інформації, що належить власникові домена.

Достовірність (authenticity) – властивість інформації, яка вказує, що об'єкт являє собою те, що він заявляє про себе.

Доступність (availability) – властивість інформації бути доступною і придатною до використання на вимогу уповноваженої особи.

Е

Емограма – графічний символ, що використовується для вираження емоцій.

З

Захист інформації **–** сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують конфіденційність, цілісність та належний порядок доступу до неї.

Захист інформації в системі **–** діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі.

Захист від негативного інформаційно-психологічного впливу противника – це напрям забезпечення інформаційно-психологічної безпеки, що містить комплекс узгоджених і взаємопов'язаних заходів, які проводяться командирами, штабами і органами МПЗ та виховної роботи з прогнозування, попередження (відвертання), запобігання, нейтралізації і усунення наслідків деструктивної інформаційно-психологічної дії на військовослужбовців.

Знищення інформації в системі – дії, внаслідок яких інформація в системі зникає.

І

Інсайдер – особа, що має доступ до конфіденційної інформації в організації.

Інтегровані дослідження комунікаційних процесів – комплексні процеси дослідження та аналізу інформаційних процесів, для здійснення яких залучаються традиційні інструменти та інноваційні методики.

Інтернет-мем (англ. Internet meme) – назва явища спонтанного поширення якоїсь інформації чи фрази, часто безглуздої, що випадково набула популярності в інтернет-середовищі завдяки поширенню усіма можливими способами (електронною поштою, на форумах, у блогах тощо).

Інформація – відомості або дані про явища та предмети навколишнього середовища, яке оточує людину. Інформація – відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

Інформація з обмеженим доступом – це конфіденційна, таємна та службова інформація.

Інформація конфіденційна – це інформація про фізичну особу, інформація, доступ до якої обмежено фізичною або юридичною особою, а також інформація, визнана такою на підставі закону *(наприклад, комерційна таємниця)*.

Інформація таємна – це інформація, що містить відомості, які становлять державну чи іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі *(наприклад, державна таємниця)*.

Інформаційна атака – здійснення тимчасового або остаточного виведення з ладу систем та підрозділів противника, що відповідають за процеси управління та інформування.

Інформаційна безпека України – складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об’єктивної інформації.

Інформаційна зброя – сукупність технік і технологій інформаційного впливу на інформаційну інфраструктуру та інформаційне поле певної території чи держави, на психіку, свідомість її населення задля дестабілізації інформаційного простору з подальшим завданням шкоди суспільно-політичній системі та збройним силам.

Інформаційний процес **–** діяльність зі створення, накопичення, зберігання, пошуку та розповсюдження відомостей або даних певного тематичного характеру.

Інформаційний вибух **–** суттєве прискорення процесів створення, накопичення, пошуку та поширення інформації.

Інформаційна війна **–** циклічний або лінійний обмін інформацією, яка може/має спричинити шкоду отримувачу, надаючи певну перевагу автору.

Інформаційне поле **–** соціальний або географічний простір, у межах якого відбуваються типові комунікаційні процеси, що охоплюють їх учасників (суб'єкти) на основі обміну інформацією (об'єкт).

Інформаційний ресурс – сукупність документів в інформаційних системах (бібліотеках, архівах, банках даних тощо).

Інформаційна система – система оброблення даних засобами накопичення, зберігання, обновлення та їхнього пошуку і відображення.

Інформаційно-психологічні акції – обмежені за масштабом і часом заходи інформаційно-психологічного впливу на конкретний об'єкт (групу об'єктів);

Інформаційно-психологічна війна – характеризуються застосуванням кібервійськ і кіберзброї в інтересах конкретної держави; великими масштабами в часі й просторі із застосуванням інформаційного і військово-економічного потенціалу держави, системністю організації; спрямовані проти конкретної держави чи групи держав, змістовно охоплюють всі форми інформаційно-психологічного та інформаційно-технічного впливу, є елементом стратегії держави чи групи держав. До цієї групи належать *кібервійни*.

Інформаційно-психологічні дії – сукупність узгоджених за метою, завданнями, простором і часом заходів інформаційно-психологічного впливу, які слугують компонентами інформаційно-психологічних операцій;

Інформаційно-психологічний вплив (ІПсВ) – вплив на свідомість особи і населення з метою внесення змін у їхню поведінку та (або) світогляд.

Інформаційно-психологічні операції *(спеціальні інформаційні операції)* – сукупність узгоджених і взаємопов'язаних за метою, завданнями, місцем і часом інформаційно-психологічних акцій та дій щодо впливу на морально-психологічний стан воєнно-політичного керівництва, особового складу військ, населення противника, щодо знищення об'єктів інформаційної інфраструктури, радіоелектронного придушення його телекомунікаційних систем, а також протидії

інформаційно-психологічному впливу на власні сили та засоби. До цієї форми належать *спеціальні інформаційні операції СІО*;

Інформаційна революція – докорінна зміна методів створення, накопичення, зберігання, пошуку та поширення інформації.

Інцидент в системі захисту інформації (information security incident) – одна або серія небажаних або несподіваних подій в системі захисту інформації, які мають шанс поставити під загрозу захист інформації.

Інцидент інформаційної безпеки (information security incident) – одне або кілька небажаних або несподіваних подій ІБ, які зі значним ступенем вірогідності загрожують інформаційній безпеці.

К

Карта інформаційного поля – схематичне зображення інформаційно-комунікаційних каналів компанії, за допомогою яких остання взаємодіє із зовнішніми та внутрішніми цільовими групами.

Кібербулінг *(кіберзалякування, англ. Cyberbullying)* – умисне анонімне залякування особи-жертви у кіберпросторі впродовж тривалого часу.

Кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів**.**

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

Кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечується сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання та нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Кібервійна – протистояння сторін на рівні програмного забезпечення шляхом видобування закритої інформації та виведення з ладу програмно-апаратних засобів противника з метою отримання суттєвих переваг в економічних, політичних та військових протистояннях. Кібервійну визначають як конфлікт у кіберпросторі,

який розпочинають зі стратегічної політичної мети та організовують системою кібератак на комп'ютерні та інформаційні системи противника.

Кіберрозвідка – діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням.

Кібертероризм – терористична діяльність, що здійснюється у кіберпросторі або з його використанням.

Кібершпигунство – шпигунство, що здійснюється у кіберпросторі або з його використанням.

Критична інформаційна інфраструктура – сукупність об'єктів критичної інформаційної інфраструктури.

Кракер *(крекер)* – особа, яка цілеспрямовано займається комерційним зломом комп'ютерних систем і мереж із корисною метою.

Комунікація – процес передання або обміну інформацією.

Контент – (англ. content – вміст) будь-яке інформаційно значиме наповнення інформаційного ресурсу (наприклад, веб-сайту) – тексти, графіка, мультимедіа; вся інформація, яку користувач може завантажити на диск комп'ютера з дотриманням відповідних норм.

Кроспостінг – цілеспрямоване автоматичне, напівавтоматичне або ручне розміщення однієї статті, посилання або теми, у форуми, блоги, будь-які інші форми веб-ресурсів або публічне листування, в тому числі й у режимі онлайн спілкування.

Комп'ютерна злочинність (кіберзлочин) – узагальнюючий термін, що означає злочини, вчинені з використанням комп'ютерної техніки, тобто характеризує специфіку способу здійснення і (або) укриття злочину.

Л

Лайк – позначка на уподобаному контенті.

Лінійна модель комунікації – цілеспрямований процес передання інформації від автора повідомлення до отримувача.

Лінкбайтінг – засіб отримання зворотних посилань на свій сайт природнім шляхом за власною ініціативою відвідувачів.

Лічка – персональне листування власника акаунту.

М

Маніпуляція **–** це різновид прихованого мовного впливу, спрямованого на досягнення власних цілей суб'єкта впливу, які не збігаються з намірами або суперечать бажанням та інтересам об'єкта впливу.

Маніпулюва́ння ма́совою свідо́містю – програмування думок і прагнень людей, їхніх настроїв і психічного стану з метою забезпечення такої поведінки, яка необхідна групі небагатьох власників засобів маніпуляції, що здійснюють такий вплив, переслідуючи свої особисті корисливі цілі.

Маніпулювання натовпом – це навмисне використання способів, заснованих на принципах психології натовпу для залучення, контролю або впливу на бажання юрби, задля спрямування її поведінки на певну дію. Ця практика є спільною для релігії, політики та бізнесу і може сприяти схваленню або засудженню чи байдужості до особи, політики або продукту.

Мас-медіа **–** технології та засоби трансляції інформації від конкретного джерела на широку аудиторію, що обмежується рамками певного інформаційного поля, в якому ці мас-медіа діють.

Медіа **–** канали та засоби зберігання, передачі й подання інформації або даних.

Медіавірус (англ. media virus) – медіаподія, що прямо чи опосередковано викликає зміни в житті суспільства.

Медіаманіпуляція – вид психологічного впливу, що здійснюється через пресу (газети, журнали, книги), радіо, телебачення, інтернет, кінематограф, звукозаписи та відеозаписи, відеотексти, телетексти, рекламні ролики.

Медіатерроризм (media terrorism) – цілеспрямоване, планомірне, систематичне використання можливостей засобів масової інформації (мас-медіа) для створення і тиражування почуттів страху (жаху, неспокою, тривоги) і розповсюдження їх в інформаційному просторі з метою маніпулювання суспільною свідомістю.

Мережева інформаційна війна **–** інформаційно-комунікаційне протистояння у форматі офлайн та онлайн мережевих структур.

Мобільний маркетинг **–** комплекс маркетингових заходів, спрямованих на промоцію товарів або послуг із використанням засобів стільникового зв'язку.

Н

Національні інтереси України – це життєво важливі матеріально-інтелектуальні й духовні цінності українського народу, визначальні потреби суспільства і держави, реалізація яких гарантує державний суверенітет України та її розвиток.

Несанкціонований доступ – доступ до інформації, що здійснюється з порушенням встановлених, в автоматизованій системі, правил розмежування доступу.

Нік (від англ. nick, nickname – прізвисько) –вигадане ім'я, яким називає себе користувач соцмереж або на різноманітних чатах, форумах, месенджерах тощо.

О

Об'єкти інформаційних процесів – інформація або ті, хто отримує цю інформацію, в процесі спрямованої комунікації.

Організація – це група людей, діяльність яких свідомо координується для досягнення загальної мети або спільних цілей.

П

Підробка інформації – навмисні дії, що призводять до перекручування інформації, яка повинна оброблятися або зберігатися в автоматизованих системах (АС).

Прогнозування інформаційно-психологічного впливу передбачає розвідку та виявлення сил і засобів проведення психологічних операцій противника, визначення форм і методів впливу на наші війська та його спрямованості; визначення негативних чинників суспільно-політичної обстановки, які може використати противник для впливу; прогнозування наслідків впливу та реакції, змін поведінки особового складу.

Попередження (відвертання) інформаційно-психологічного впливу противника на свідомість військовослужбовців містить такі загальні соціально-психологічні напрямки: виховання в особового складу пильності, неприйнятності до ворожої ідеології, формування антивербувальної стійкості свідомості; протидія сприйняття особовим складом деструктивної інформації; захист систем зв'язку, комунікацій і управління; перекриття каналів проникнення противника в інформаційні ресурси; роз'яснення особовому складу прихованих цілей противника, прийомів ведення їм інформаційно-психологічної боротьби; припинення неправдивих чуток, панічних настроїв і профілактика різних фобій серед особового складу підрозділу.

Порушення цілісності інформації в системі – несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст.

Психографіка – характерні психологічні особливості представників певних цільових аудиторій.

Р

Рерайтинг – написання унікального тексту на основі вже існуючої новини, статті. Для рерайтинга типово використання синонімічних слів, переклад прямої мови в непряму, переміщення абзаців.

С

Система безпеки – є продукт конкретного суспільства, у якому відбиваються його специфічні риси.

Системи менеджменту інформаційної безпеки (СМІБ) – вимоги серії міжнародних стандартів інформаційної безпеки ISO/IEC 27000 до технології забезпечення інформаційної безпеки, управління ризиками, організації раціонального розподілу функцій і ефективної взаємодії з питань захисту інформації всіх підрозділів і співробітників.

Соціальна безпека – рівень регулювання соціальних процесів з метою реалізації соціальних пріоритетів, збалансування соціальних пропорцій і недопущення соціальних деформацій, що призводять до соціально-політичної нестабільності та ускладнюють соціально-економічний розвиток держави.

Соціально-політичній чинник в безпеці країни виражає механізм і гостроту протікання політичних процесів у суспільстві, рівень його стабільності.

Соціальна інженерія – галузь знань, яка вивчає особливості використання психологічних методик та шахрайських прийомів з несанкціонованого доступу до захищених інформаційних ресурсів.

Соціальна мережа – це соціальна структура, створена об’єднаними за однією або декількома ознаками взаємозалежності вузлами, які здебільшого представлені індивідуальними членами або організаціями. Соціальні мережі можуть бути створеними на тлі спільності цінностей, дружби, родинності, неприязні, конфлікту, торгівлі, зв’язків у мережі Інтернет, сексуальних зв’язків, релігійних поглядів тощо.

Соціальна мережа в інтернеті – співтовариство постійних користувачів певного мережевого ресурсу, “коло своїх”, об’єднаних єдиними нормами й спільністю цілей комунікації.

Спеціальні інформаційні операції (СІО) – сплановані дії, спрямовані на ворожу, дружню або нейтральну аудиторію, які передбачають вплив на її свідомість і поведінку за допомогою використання організованої інформації та інформаційних технологій для досягнення певної мети. СІО є основною формою реалізації компонентів

інформаційного протиборства, що належать до виключної компетенції сил безпеки й оборони. До СІО належать психологічні дії зі стратегічними цілями, психологічні консолідуючі дії та психологічні дії з безпосередньої підтримки бойових дій.

Співтовариство віртуальне **–** група людей зі схожими інтересами, які спілкуються один з одним в основному через Інтернет.

Споук-персона **–** офіційна особа, що презентує позицію компанії, є транслятором інформаційних меседжів.

Стіна **–** спосіб публікації відкритих записів особистого і загального характеру тимчасової значущості, відсортованих у зворотному хронологічному порядку, тобто останній запис знаходиться зверху.

Суб'єкти інформаційних процесів – учасник комунікацій, індивідуум, соціальні групи, організації (ЗМІ, громадські, державні, комерційні структури).

Сугестія – це сукупність різних засобів вербального і невербального емоційно забарвленого впливу на людину з метою створення у неї певного стану або спонукання її до певних дій.

Сугестор – людина, яка маніпулює (навіює); сугеренд – об'єкт навіювання.

Сугестивний вплив – це вплив, що обходить свідомий контроль, що йде в обхід розуму через прямі або непрямі навіювання.

Т

Таргетування **–** вибір цільової групи або цільового сегменту інтернет-простору.

Технічний захист інформації *(ТЗІ)* – вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації. ТЗІ містить такі основні напрямки: захист інформації від несанкціонованого доступу та захист інформації від витоку технічними каналами.

ТИЦ (тематичний індекс цитування**) –** технологія оцінки авторитетності інтернет-ресурсів з урахуванням якісної характеристики – посилань на інших сайтах. Цей показник розраховується як сумарна вага посилань через систему апдейтів (рахівників показників) з оновленням два рази на місяць.

Тред – група повідомлень, об'єднаних єдиною тематикою.

Тренд – популярна тема обговорення в соцмережах.

Тролінг (від англ. trolling) – розміщення в Інтернеті (на форумах, в групах новин Usenet, у вікі-проектах та ін.) провокаційних повідомлень з метою викликати

конфлікти між учасниками, образи, війну правок, марнослів'я тощо. Тролінг є грубим порушенням мережевого етикету (нетикету). Особу, яка займається тролінгом, називають тролем.

У

Уразливість (vulnerability) – слабке місце системи інформаційної безпеки або засобів управління, яке може бути використано однією або більше загрозами.

Ф

Флог/Фейк – фальшивий блог, акаунт, на якому міститься неправдива інформація.

Фолловер – підпис на новини й оновлення.

Флуд – повідомлення у форумах і чатах, що займають великі об'єми і не несуть корисної інформації.

Фішинг – різновид шахрайства в інтернеті з метою отримання незаконного доступу до конфіденційних даних користувачів.

Фішингова атака – тип кібератаки, який розроблено, щоб обманом примусити людей розкрити свою приватну або конфіденційну інформацію.

Хакер (англ. hacker, від to hack – рубати) – особа, що намагається отримати несанкціонований доступ до комп'ютерних систем, з метою отримання секретної інформації або виявлення вразливості системи.

Х

Хай-х'юм технології (англ. high-hum – високі гуманітарні технології) – сукупність знань, духовних та культурних цінностей, а також методів транслювання інформації, що стимулює людей до певної колективної діяльності.

Ц

Цілісність інформації – властивість збереження точності і повноти інформації.

Ч

Чинник геополітичний є сукупність географічних параметрів, які визначають відповідну політику держави стосовно забезпечення її життєво важливих інтересів на певному етапі розвитку.

Чинник економічний – є найважливіший у формуванні системи безпеки. Мова йде про взаємозв'язок потенціалу країни з реалізацією своїх інтересів у

внутрішній і зовнішній сферах із забезпечення безпеки. Національна безпека й економічна могутність країни нероздільні.

Чинник етнонаціональний – зберігає в собі специфіку етнонаціональних протиріч і механізми їх розв'язання, які значною мірою виражені соціальною стабільністю та рівнем консолідації суспільства.

Ш

Шифрування – перетворення електронного документа із застосуванням криптографічних методів з метою захисту його змісту.

Ц

Цільова аудиторія – аудиторія, на яку спрямовані зусилля інформаційного процесу комунікацій. Визначається за певними соціально-демографічними характеристиками (стать, вік, освіта, прибуток, споживацькі уподобання, стиль життя)

Циклічна модель комунікації – взаємний обмін інформацією, в процесі якого учасники комунікації поступово змінюють ролі автора та отримувача повідомлення.

D

dDoS-атака (Distributed Denial Of Service Attack) – атака з використанням безлічі адрес нічого не підозрюючих користувачів для заблокування каналу, через відкриття максимально можливої кількості з'єднань із соціальною мережею. Послання великої кількості паразитного трафіку для перевантаження і виведення з ладу операційної системи, яка не встигає обробити всі з'єднання, в результаті чого, користувачі соціальної мережі не мають можливості з'єднання з сервером, на якому розміщений сайт.

I

ISO/IEC 27001 – міжнародний стандарт системи управління інформаційною безпекою, розроблений спільно Міжнародною організацією зі стандартизації та Міжнародною електротехнічною комісією.

ISO/IEC 15408 – міжнародний стандарт з проектування та оцінки безпеки систем інформаційних технологій.

ISO - International Organization for Standardization.

IEC - International Electrotechnical Commission;

ISO - International Organization for Standardization.

N

NIST SP 800 – стандарт з інформаційної безпеки Національного інституту стандартів та технологій США.

P

PageRanke **–** алгоритм виміру популярності інтернет-ресурсу за 10-ти бальною шкалою. Оцінює важливість та авторитетність інформації за кількістю посилань. Використовується системою Google для ранжування сайтів при видачі результатів пошуку за запитами користувачів.

S

SMM-аудит – методика оцінки впізнаваності та характеру іміджу досліджуваного об'єкта в соціальних мережах та в мережі Інтернет у цілому.

SEO (Search Engine Optimization) – комплекс заходів із пошукової оптимізації, орієнтований на підвищення позиції веб-сайту в пошукових системах.

SMO (Social Media Optimization) – комплекс заходів із просування веб-ресурсів у мережі Інтернет.

SMM (Social Media Marketing) – комплекс заходів із просування персонального акаунту або окремого контенту в соціальних мережах.