ТЕМА 8. ІНФОРМАЦІЙНА ГІГІЄНА ЛЮДИНИ

1. Основні поняття про інформацію, її властивості та види.
2. Дезінформація та протидія фейкам.
3. Основи інформаційної безпеки в інтернеті.
4. Кібербулінг та його особливості.

1. Основні поняття про інформацію, її властивості та види.

Поняття *"інформація"* походить з латини (informatio) і означає виклад, роз'яснення, тлумачення факту чи події.

Інформація — будь-які відомості, створенні людиною для передачі в часі та/чи просторі. Прийом, обмін та використання інформації становить інформаційний процес. Інформація, яку ми засвоїли й використовуємо, стає знаннями. Процес опрацювання інформації залежить від багатьох факторів.

Інформація з обмеженим доступом — та, що становить державну таємницю, оголошення якої наносить шкоду державі, суспільству або окремій особі. Інформація сприяє взаємодії різних груп людей, тому інформаційна взаємодія виступає найважливішою формою соціальної взаємодії. Можна сказати, що зараз увесь світ залучений в єдину інформаційну систему, яка фактично працює в режимі реального часу. Рівень задоволення потреби в інформації відіграє важливу роль у житті суспільства. Зокрема, дезінформація та інформаційний хаос викликають почуття невпевненості й безсилля.

Проблему споживання інформації можна розв’язати лише через упорядкування інформації, її сортування та спеціалізацію, самостійний добір людиною. Інформація, що виникла разом із суспільством, є соціальною інформацією. Основними характеристиками соціальної інформації є її кількість, цінність, зміст, об’єктивність, адекватність, вірогідність, точність, оперативність, надійність.

Соціальна інформація має важливу якість: вона ніколи не буває нейтральною. Соціальну інформацію, яка передається за допомогою мас-медіа, треба розглядати як процес масової комунікації. Масова комунікація включає в себе зміст, тобто соціальну інформацію, процеси інформаційного обміну, технічні засоби та багато іншого. Точного, загальноприйнятого означення термінів «комунікація» та «інформація» немає і в багатьох працях, зокрема в документах міжнародних організацій, часто ці терміни використовують як синоніми. Основне завдання масової інформації — відображати дійсність.

Коли характеризують інформацію (повідомлення), то звертають увагу на її *якісні ознаки* (властивості): адекватність, вірогідність, актуальність, повноту та об'єктивність.

Адекватність - відповідність створюваного (за допомогою отриманої інформації) образу реального об'єкта, явища або процесу.

Актуальність - важливість на даний момент часу.

Об'єктивність - неупередженість, незалежність інформації від думки, волі та бажань людини.

Повнота. Інформацію можна вважати повною, якщо її достатньо для розуміння та прийняття рішення.

Інформація має бути *цінною*, це вимірюється користю, яку здатна принести інформація для досягнення мети. І нарешті, інформація має бути *доступною.* Доступність визначається здатністю адресата до сприйняття інформації.

Єдиний *інформаційний простір,* як фундамент інформаційного суспільства, створюється людиною і для людини. Тому змістове навантаження інформації має відповідати інтересам людини, морально-етичним нормам, попереджати негативні морально-етичні наслідки. В цьому полягає принцип *гуманістичної орієнтації інформаційного суспільства*, який має бути одним із провідних.

Достовірність інформації — властивість бути правильно сприйнятою, безсумнівна вірність наведених відомостей, які сприймає людина. Достовірна інформація обов'язково має містити посилання на джерело, щоб можна було перевірити та підтвердити правдивість слів.

Про достовірність інформації свідчить підтримка експертів, однак експертна думка має бути висловлена фахівцем з питання, що висвітлюється, та з посиланням на нього, і за можливості — залучити кілька фахівців. Якщо в тексті вживаються узагальнені вислови: «на думку експертів», «як зазначили науковці», «говорять», «усім відомо», «ви, можливо, чули про» тощо, то це свідчить про те, що інформація може бути недостовірною.

При висвітленні певних питань краще звертатися до першоджерел, а не до інтерпретації цих питань. Також для більшої достовірності інформації можна порівняти її в різних джерелах, що забезпечує її повноту. Також важливо перевіряти репутацію джерела. Солідні медіа бережуть свою репутацію й ніколи не стануть ризикувати, подаючи неправдиву інформацію. Більшої довіри заслуговує джерело, коли відомо, хто його автор, і коли він має авторитет.

Щоб протидіяти маніпуляціям та отримувати якісну достовірну інформацію, потрібно навчитися її аналізувати, зокрема відрізняти факти від суджень, оціночних думок.

Факт — означає дійсність, подію, те, що реально відбулося. Фактами можуть бути цифри, дати, імена, події — все, що можна, виміряти, перерахувати, підтвердити. Факти надають різні джерела, це можуть бути науково-дослідні та соціологічні інститути, органи влади, органи місцевого самоврядування, установи статистики, архіви, пошукові інтернет-системи тощо.

Завдання мас-медіа та фахівців, які готують матеріали, — подавати правду, спираючись на факти. Факти треба повідомляти незалежно від того, кому вони вигідні або чиєму іміджеві можуть зашкодити. Приховувати факти чи

перекручувати їх — неприпустимо. Часто з метою маніпуляції факти подають разом з оціночними судженнями.

2. Дезінформація та протидія фейкам.

Дезінформація – спотворена, свідомо неправдива, провокаційно-тенденційна інформація, поширена як правдива з метою введення в оману громадськості, політичних опонентів, конкурентів тощо. Дезінформацією також називають сам процес поширення у ЗМІ чи у інший спосіб викривлених або свідомо неправдивих відомостей. У військовій справі – спосіб тактичного або стратегічного маскування, суть якого полягає у планомірному навмисному розповсюдженні неправдивих відомостей про власні збройні сили, їх склад, озброєння, боєздатність і плани військових дій.

Основні ознаки дезінформації:

1. Вплив на певну аудиторію через оприлюднення.
2. Цілеспрямованість (передбачає організатора та умисел).
3. Негативні (суспільно-небезпечні) наслідки.
4. Наявність в основі «неправдивості», що піддається перевірці.
5. Імітаційність, представленість як правдивого матеріалу.
6. «Вбудованість» у певні системи поглядів, відповідність певним переконанням. Дезінформація стосується певних переконань, відповідає певній системі поглядів, дезінформація на випадкові теми не досягає мети.
7. Прив’язка до соціально значущих подій, тобто суспільно-важливої інформації, що є чутливою або має символічну цінність.

Які види дезінформації існують:

- Фейки;
- Маніпулювання;
- Обман конкретної особи чи групи людей, а також навіть нації;
- Створення необхідної громадської думки.

Серед впливів, які домінують у сучасному світі найпоширенішим є вплив інформаційний як інструмент, який несе нові виклики та загрози, пов’язані з дезінформацією, фейковими новинами, фальшивою інформацією. Фейки - одна із найважливіших проблем сучасності. Вони є інструментами впливу.

Фейк — навмисно змаліпульована новина. Іноді фейки — це абсолютна вигадка, фікція. Якщо раніше треба було перевіряти об’єктивність факту, то зараз варто з’ясовувати, чи був він взагалі. Фейки створюються для того, щоб досягати бажаного ефекту, наприклад, формування відношення, реакції до певного явища, події, людини чи групи.

У нинішньому інформаційно-комунікаційному просторі дедалі частіше трапляється фейкова інформація, спрямована на дискредитацію як окремої особистості, так і цілого етносу, народу чи нації.

Що більше фейкових новин людина споживає, то більше вона стає дезорієнтованою. Тому кожну інформацію необхідно перевіряти на достовірність, знаходити першоджерела інформації, авторів і причини створення.

Маніпуляція в медіа — це техніка цілеспрямованого викривлення інформації заради формування певного погляду, ставлення до тієї або іншої проблеми / особи / явища. Маніпулювання здійснюється для того, щоб управляти масами, керувати поведінкою людини через вплив на свідомість, інстинкти та ідеологію людини. За допомогою маніпуляцій людині нав'язуються певні ідеологічні кліше, штампи сприйняття дійсності й реакції на події.

Новина — оперативне інформаційне повідомлення, яке містить суспільно важливу та актуальну інформацію, що стосується певної сфери життя суспільства чи окремих його груп.

Основні характеристики новини: оперативність, актуальність, суспільна значущість або інтерес, об'єктивність, достовірність, специфічність побудови інформаційного повідомлення.

Маніпуляції в новинах спостерігаються, коли для аудиторії подаються новини, які не відповідають дійсному стану речей, з використанням помилкових даних і повідомлень.

Одним з методів маніпуляцій суспільною свідомістю є пропаганда.

Пропаганда — форма комунікації, спрямована на поширення фактів, аргументів, чуток та інших відомостей для впливу на суспільну думку на користь певної спільної справи чи громадської позиції. Пропаганда є цілеспрямованою, її тактика має на меті зміну системи цінностей і поведінки.

Пропаганда впливає на ставлення до певних явищ або груп людей. Це ставлення емоційно підвищене й завжди контрастне, як, наприклад, ворожість, захоплення. Пропаганда є потужною зброєю інформаційної війни; використовується для дегуманізації та створення ненависті до відповідного ворога — як зовнішнього, так і внутрішнього. Пропаганда передбачає спотворення інформаційних потоків, створенням хибного образу у свідомості.

Мова ворожнечі — це будь-які вислови, контекст чи візуальне зображення, що призводить до створення або ж поглиблення вже існуючої ворожнечі між відмінними за певними ознаками групами суспільства. Найчастіше ці групи різняться за територіальним походженням, політичними чи соціальними поглядами.

Ознаками мови ворожнечі є: негативні вислови, починаючи від підбурювання й закінчуючи упередженням, ненавистю, зловживанням, дискредитацією, образливими словами та епітетами, спрямовані проти особи або групи осіб, що належать до інших національностей, етнічних груп, конфесій, партій, орієнтацій тощо.

Такі форми висловлювань провокують, стимулюють або виправдовують расову ненависть, ксенофобію, антисемітизм або інші форми ненависті, засновані на нетолерантності, у тому числі ворожості щодо меншин і мігрантів.

Мова ворожнечі поділяється на жорстку, середню та слабку.

Жорстка: прямі й завуальовані заклики до насилля, заклики до дискримінації, заклики не дати групі можливості закріпитися в регіоні.

Середня: виправдання випадків насилля та дискримінації, звинувачення певної групи в негативному впливі на суспільство чи державу, твердження про кримінальність певної територіальної чи етнічної групи, ствердження про її неповноцінність.

Слабка: створення негативного іміджу певної групи суспільства, ствердження про моральні недоліки такої групи, протиставлення однієї групи іншій, згадування групи чи окремих її представників у принизливому чи образливому контексті, пряме або завуальоване ствердження того, що одна група створює незручності в існуванні іншої.

Нині також постає проблема з перевірки інформації в мережі Інтернет, де часто автори залишаються анонімними, працюють боти, що поширюють неправдиву інформацію. Користувачі здебільшого самі мають звертати увагу, яку інформацію вони споживають, а особливо поширюють.

Питання достовірності інформації регулюється правовими нормами, що передбачають можливу відповідальність журналістів за поширення недостовірної інформації.

Джерела бувають таких типів:

Первинні — оригінальні джерела, що не містять інтерпретації. До них відносять фотографії, щоденники, листи, дослідницькі звіти, оригінальні твори мистецтва.

Вторинні — містять авторську інтерпретацію, аналіз і підсумки. Це наукові статті, книжки тощо.

Третинні — компіляції матеріалів з інших джерел: реферати, таблиці, енциклопедії.

Не всі джерела є надійними та об’єктивними. Найбільшу довіру викликають джерела, які є нейтральними, неупередженими, не відстоюють нічиїх інтересів.

2. Основи інформаційної безпеки в інтернеті.

Інтернет — це невід’ємна частина нашого життя. Він є глобальною системою взаємозалежних комп’ютерних мереж. Інтернет є мережею мереж, що дає можливість створення кіберпростору, де відбувається онлайнова комунікація. Інтернет має як переваги, так і недоліки.

Переваги:

- Інтернет є найбільше джерело інформації.
- Інтернет — це колосальний крок уперед у розвитку наукових досягнень, він є потужним засобом соціалізації людини, що перебуває в Мережі.
- Він дає можливість взаємодіяти з багатьма людьми з різних континентів, спілкуватися, об'єднуватися заради проведення спільних дій і суспільно-соціальних проектів, обмінюватися ідеями, ділитись інформацією, здійснювати соціальну підтримку, провадити бізнес, спрямовувати дії, створювати твори мистецтва, грати в ігри, залучатися до політичних дискусій тощо.
- Інтернет дає можливість сплачувати послуги, поширювати рекламу, робити покупки онлайн, що економить людині багато часу, який можна використати для саморозвитку чи своїх потреб.

Недоліки:

Віруси, інтернет-залежність, ігроманія, втрата реального спілкування та перенесення у віртуальний світ, шахрайство.

Соціальна мережа — це веб-сервіс, віртуальна спільнота, що складається з людей з однаковими інтересами, нахилами, діяльністю. Соціальні мережі спеціалізуються на різних потребах та інтересах людей, і в більшості користувачів є акаунти у двох-трьох соціальних мережах.

Інформаційна гігієна - область знань, що вивчає закономірності впливу на організм людини та суспільне здоров'я інформаційних потоків що надходить до людини.

Метою інформаційної гігієни є попередження негативного впливу інформації на психічне, фізичне та соціальне благополуччя окремої людини, соціальних груп, населення в цілому.

Інформаційна безпека — розділ інформатики, що вивчає закономірності забезпечення захисту інформаційних ресурсів фізичних осіб, підприємств, організацій, державних установ тощо від втрати, порушення функціонування, пошкодження, спотворення, несанкціонованого копіювання та використання.

Інформаційна безпека базується на таких принципах: *доступність, конфіденційність, цілісність.*

Основні загрози інформаційні безпеці:

- знищення та спотворення даних;
- отримання доступу до конфіденційних даних;
- пошкодження пристроїв ІС;
- отримання прав на виконання певних дій;
- отримання доступу до виконання фінансових операцій;
- отримання повного доступу до керування ІС.

Загрози безпеці інформаційної системи (ІС) класифікують за такими принципами:

- За обсягом завданих збітків (*нешкідливі, шкідливі, дуже шкідливі*);
- За метою (*зловмисні, випадкові*);
- За місцем виникнення (з*овнішні; внутрішні);*
- За походженням (п*ридодні; техногенні; антропогенні*).

Засоби і методи підтримки інформаційної безпеки мають різне призначення.

Програмні засоби — захист від вірусів, ідентифікація користувачів тощо.

Технічні засоби — захист від несанкціонованого доступу, від пошкодження ІС тощо.

Адміністративні методи — регламентація порядку взаємодії користувачів із ІС.

Морально-етичні засоби — норми поведінки осіб в інформаційному просторі.

Правові методи — правила користування інформацією та відповідальність за їхнє порушення.

Етичні норми передбачають, що користувачі комп'ютерів не використовують комп'ютерну техніку та програмне забезпечення для завдання шкоди іншим людям, не порушують авторських прав.

Правові основи захисту даних базуються на правових актах, що утверджують права і свободи людини та якими встановлено відповідальність за злочини в галузі інформаційної безпеки.

Правила безпечної поведінки в інтернеті:

1. Нікому не надавати особисту інформацію: домашню адресу, номери телефонів, робочу адресу батьків, адресу школи тощо.
2. Не погоджуватися на зустріч з людиною, з якою ви познайомилися в Інтернеті.
3. Не посилати свої фотографії чи іншу інформацію незнайомим людям.
4. Не відповідати на грубі листи.
5. Не давати нікому свої паролі.
6. Не робити протизаконних вчинків і речей в Інтернеті.
7. Не шкодити і не заважати іншим користувачам.

4. Кібербулінг та його особливості.

Кібербулінг — умисне цькування щодо визначеної особи у кіберпросторі, як правило, впродовж тривалого проміжку часу.

Кібербулінг – це булінг із застосуванням цифрових технологій. Він може відбуватися в соціальних мережах, платформах обміну повідомленнями (месенджерах), ігрових платформах та мобільних телефонах.

Це неодноразова поведінка, спрямована на залякування, провокування гніву чи приниження тих, проти кого він спрямований.

Приклади включають:

- поширення брехні про когось або розміщення фотографій, які компрометуюсь когось, у соціальних мережах;
- надсилання повідомлень або погроз, які ображають когось або можуть завдати комусь шкоди, через платформи обміну повідомленнями;
- видання себе за когось іншого/іншу і надсилання повідомлень іншим людям від його/її імені.

Типові ознаки кібербулінгу:

- систематичність (повторюваність) діяння;
- наявність сторін – кривдник (булер), потерпілий (жертва булінгу), спостерігачі (за наявності);
- дії або бездіяльність кривдника, наслідком яких є заподіяння психічної та/або фізичної шкоди, приниження, страх, тривога, підпорядкування потерпілого інтересам кривдника та/або спричинення соціальної ізоляції потерпілого.

До найпоширеніших видів кібербулінгу належать:

Під *використанням особистої інформації* слід розуміти «зламування» поштових скриньок, серверів, сторінок у соціальних мережах із метою отримання особистої інформації про людину та переслідування її.

Анонімні погрози полягають у надсиланні листів на електронну пошту своєї жертви з повідомленнями загрозливого змісту. Іноді ці погрози мають образливий характер із вульгарними висловами і ненормативною лексикою.

Кіберпереслідування відбуваються за допомогою мобільного зв'язку або електронною поштою. Хулігани можуть тривалий час переслідувати свою жертву, завдаючи брудних образ принизливого характеру або шантажуючи будь-якими таємними фактами. Відстежуючи через інтернет необережних користувачів, переслідувач отримує інформацію про час, місце і всі необхідні умови для вчинення злочину.

Тролінг здійснюється шляхом розміщення в інтернеті (на форумах, у блогах) провокаційних повідомлень із метою викликати флейм, тобто конфлікти між учасниками, взаємні образи.

Флеймінг – це улюблений метод «тролів» (провокаторів), що полягає в обміні короткими, гнівними і запальними репліками між двома чи більше учасниками, використовуючи комунікаційні технології. Частіше за все розгортається в «публічних» місцях інтернету: в чатах, форумах, у дискусійних групах, спільнотах. Інколи він перетворюється у затяжну війну.

Обмовляння або зведення наклепів – це поширення принизливої, неправдивої інформації з використанням комп'ютерних технологій. Це можуть бути і текстові повідомлення, і фото (використання фотошопу), і пісні, які змальовують жертву у шкідливій манері.

Хеппіслепінг – один із видів кібербулінгу. Його назва походить від випадку в англійському метро, де підлітки били перехожих, тоді як інші записували це на камеру мобільного телефона. Тепер ця назва закріпилася за будь-якими відеороликами з записами реальних сцен насильства.

Секстинг – це обмін власними фото/відео/текстовими матеріалами інтимного характеру, із застосуванням сучасних засобів зв'язку (мобільних телефонів, електронної пошти, соціальних мереж). Секстинг стає все більш популярним серед підлітків.

Онлайн-грумінг – це побудова в мережі інтернет дорослим або групою дорослих осіб довірливих стосунків із дитиною (підлітком) із метою отримання її інтимних фото/відео та подальшим її шантажуванням про розповсюдження цих фото. Це робиться з метою отримання грошей, більш інтимних зображень чи навіть примушування до особистих зустрічей.

За булінг (цькування) неповнолітньої чи малолітньої особи передбачений штраф від 850 до 1700 грн або громадські роботи від 20 до 40 годин. За такі дії, вчинені повторно протягом року після або групою осіб – штраф від 1700 до 3400 грн або громадські роботи на строк від 40 до 60 годин.

Якщо булінг (цькування) вчинить дитина у віці до 16 років – відповідатимуть її батьки або особи, що їх заміняють. До них будуть застосовані штраф від 850 до 1700 грн або громадські роботи на строк від 20 до 40 годин.