3-ій модуль
11-ий клас
Інформаційна війна

Заняття 1. Цілі та завдання інформаційної війни.
Заняття 2. Учасники інформаційної війни.
Заняття 3. Методи інформаційної війни (пропаганда, дезінформація, кібератаки, психологічні операції, інформаційні операції).
Заняття 4. Роль критичного мислення в інформаційній війні.
Заняття 5. Роль медіа в інформаційній війні.
Заняття 6. Роль штучного інтелекту в інформаційній війні.
Заняття 7. Кібербезпека в умовах інформаційної війни.
Заняття 8. Розвідка на основі відкритих джерел (OSINT).
Заняття 9. Цілі та завдання osint. інструменти та методи OSINT.
Заняття 10. Верифікація джерел. візуальний аналіз.
Заняття 11. Особливості професій, пов’язаних із сучасними цифровими технологіями. Військові професії та перспективи.

Заняття 1. Цілі та завдання інформаційної війни

Мета заняття:

- повідомити про інформаційну сферу, у якій ведеться своя війна;
- пояснити основні поняття інформаційного протистояння.

Навчальні та виховні цілі:

- засвоїти низку понять;
- дізнатися про різновиди інформаційних війн;
- сформувати розуміння важливості інформаційного впливу на населення.

Вступ

Людство живе в інформаційному суспільстві, де рушійною силою розвитку стає не володіння матеріальними благами, а створення, обробка та використання інформації. Інформація – це глобальний ресурс, використання якого дозволяє значно підвищити ефективність управління всіма сферами життя. Вона є основним інструментом боротьби за владу та впливу на свідомість людей.

Тематика інформаційної війни є надзвичайно важливою, оскільки базується на знаннях із багатьох наукових дисциплін, таких як історія, культура, соціологія, психологія, географія, кібербезпека тощо. Згідно з однією з теорій: якщо ви не є учасником війни, ви – територія, за свідомість якої ведеться боротьба (Рені ДіРеста).

1. Що таке інформаційна війна?

Війни в інформаційному полі ведуться тисячоліттями. Вони є невід'ємною частиною будь-яких воєнних кампаній. Інформаційний вплив на ворога можна побачити ще в давньому Римі в епоху феодалізму і в пізніші часи. Поради, як впливати інформацією на інших людей, описані в трактаті «Мистецтво війни» китайського полководця Сунь Цзи (V ст. до н. е.).

З появою друкованих та електронних засобів масової інформації інформація стала справді масовим явищем. Тому застосування інформаційного впливу перетворилося на самостійний вид війни.

За інтенсивністю, масштабами і засобами, які використовуються, виділяють такі ступені інформаційного протиборства:

- інформаційна експансія — діяльність із досягнення національних інтересів методом безконфліктного проникнення в інформаційну сферу;
- інформаційна агресія — незаконні дії однієї зі сторін в інформаційній сфері. Шляхом обмеженого і локального за своїми

масштабами застосування сил ставиться мета завдати конкретної, відчутної шкоди в окремих галузях діяльності іншої сторони;
- інформаційна війна.

Інформаційна війна (ІВ) – якісно новий вид бойових дій, що включає активну протидію в інформаційному просторі. Вона спрямована на атаку інформаційної функції держави незалежно від засобів, що застосовуються. Тому тепер інформацію можна розглядати і як самостійну зброю, і як вигідну ціль.

Ця зброя не завдає фізичної шкоди, але може призвести до справжньої війни. Канадський дослідник Маршалл Маклюен, який ввів термін «інформаційна війна», проголосив тезу: «Істинно тотальна війна – це війна за допомогою інформації».

Водночас інформаційна війна – складова частина ідеологічної боротьби. Такі війни не призводять безпосередньо до кровопролиття, руйнувань, при їх веденні немає жертв, ніхто не позбавлений їжі, не залишається без домівки. І це породжує небезпеку: люди не звертають увагу на них і піддаються впливу. З часом це може призвести до справжньої війни та до набагато серйозніших наслідків.

Інформаційні війни можуть проходити не тільки в міждержавних відносинах, але і в комерційній, суспільній та інших сферах. Ми розглядаємо ту частину, до якої більш правильно застосовувати поняття «стратегічні інформаційні війни» – протистояння з використанням державного глобального інформаційного простору й інфраструктури для проведення стратегічних військових операцій, а паралельно при цьому зміцнення впливу на власний інформаційний ресурс. Стратегічні інформаційні війни (СІВ) поділяють на перше і друге покоління.

СІВ першого покоління включає основні методи інформаційної війни, які США реалізують у наш час:
- вогневе придушення (у воєнний час) елементів інфраструктури державного та військового управління;
- ведення радіоелектронної боротьби;
- отримання розвідувальної інформації шляхом перехоплення та розшифрування інформаційних потоків;
- несанкціонований доступ до інформаційних ресурсів з подальшою їх фальсифікацією або викраденням;
- масове поширення дезінформації в інформаційних каналах противника або в глобальних мережах з метою впливу на осіб, які ухвалюють рішення;
- отримання інформації через перехоплення відкритих джерел.

СІВ другого покоління може призвести до відмови від використання військової сили через:
- створення атмосфери бездуховності та аморальності, негативне ставлення до культурної спадщини противника;
- маніпуляцію суспільною свідомістю населення з метою створення політичної напруженості та хаосу;

- дестабілізацію політичних відносин між партіями, об'єднаннями й рухами для провокації конфліктів, розпалювання недовіри, загострення політичної боротьби, провокування репресій проти опозиції та навіть громадянської війни;
- зниження рівня інформаційного забезпечення органів влади, інспірування помилкових управлінських рішень;
- дезінформацію населення про роботу державних органів, підрив їх авторитету, дискредитацію органів управління;
- підрив міжнародного авторитету держави та її співпраці з іншими країнами;
- завдання шкоди життєво важливим інтересам держави в політичній, економічній, оборонній та інших сферах.

Можна говорити про:

1. ведення ІВ під час воєнних дій як форму підтримки «гарячої» війни;
2. міждержавне протистояння в управлінні, економіці тощо;
3. підготовку до окупації.

До видів інформаційної війни можна віднести:

- психологічну війну;
- кібервійну;
- мережеву війну;
- ідеологічну диверсію;
- семантичну війну;
- радіоелектронну боротьбу, що може виявлятися через:
    - подавлення телебачення і радіомовлення;
    - захоплення або підкорення ресурсів телебачення та радіо для кампаній дезінформації;
    - блокування або недоступність мереж комунікацій;
    - саботаж операцій фондової біржі через електронне втручання, поширення дезінформації або витік чутливої інформації.

Прикладом прояву ІВ є випадок, коли в 1991 році під час війни в Перській затоці проти Іраку голландські хакери викрали інформацію про пересування американських військ у Міністерстві оборони США. Вони спробували продати її іракцям, проте ті відмовилися, вважаючи це містифікацією.

2. Мета інформаційної війни

Мета інформаційної війни — послабити моральні та матеріальні сили противника або конкурента і посилити власні. Вона включає пропагандистський вплив на свідомість людини в ідеологічних та емоційних сферах. Інформаційні війни можуть завдати руйнувань у суспільній психології та психології особистості, які за своїм масштабом та значенням можуть перевищувати наслідки збройних конфліктів.

Інформаційні війни складаються з актів, які називаються інформаційними операціями (в Україні більш поширений неточний термін ІПСО – інформаційно-психологічна операція). Інформаційна операція –

це інтегроване використання можливостей електронної зброї, комп'ютерних мережевих операцій, психологічних операцій, дезінформації та операцій із безпеки для впливу на свідомість людини з метою порушення або перехоплення контролю над процесом ухвалення рішень противника, що відбувається паралельно із захистом свого власного інформаційного поля. Мається на увазі, що вплив на іншу країну може спричинити непрогнозований вплив на своє ж суспільство, якщо вчасно не прийняті контрзаходи.

3. Інформаційна зброя – головний інструмент інформаційних війн

Інформаційна зброя – це донесення інформації в спосіб, який змінює сприйняття та думки щодо ситуації, спричиняє переосмислення мотивацій жертви, що може призвести до втрати бажання воювати або протистояти. Інформаційна зброя може впливати на те, що знає об'єкт впливу, і на те, у що він вірить, які цінності сповідує. Це призводить до розмивання розуміння істини.

Інформаційні війни є частиною гібридних війн, які поєднують використання зброї, тероризму, кібервійну, торгові війни, патентні війни, інформаційний тероризм, пропаганду, порушення прав людини, переселення та вплив на громадську думку. У таких випадках завдання – якомога довше зберегти двозначність і плутанину між урядом і суспільством. І одне з головних завдань агресорів у разі гібридної війни – заперечувати, прикривати, розмивати трактування своїх ворожих дій. Бачимо також приклад росії, яка поставила як завдання в інформаційній війні створення позитивного іміджу росії через популяризацію російської культури («великий балет», «великий спорт»), жертовного образу російської інтелігенції (росіяни – жертви політики путіна, «прості росіяни за мир»), розмивання кордонів між російським та українським народами (через спотворення історії, акцентування на «спільній» історії, мовний експансіонізм).

4. Завдання інформаційних війн

Інформаційна війна може мати конкретні завдання в різних напрямках, які випливають з мети та інструментів, якими вона оперує. Це зокрема:

- внесення в суспільну та індивідуальну свідомість ворожих, шкідливих ідей та поглядів;
- дезорієнтація та дезінформація мас;
- послаблення певних переконань та систем;
- залякування власного населення образом ворога;
- залякування супротивника своєю могутністю;
- забезпечення ринку збуту для своєї економіки (у цьому випадку інформаційна війна є складовою частиною конкурентної боротьби).

У країнах, супроти яких ведеться інформаційна операція, завданнями можуть бути провокування:

- соціальних, політичних, національно-етнічних або релігійних зіткнень;
- ініціювання страйків, масових заворушень та інших акцій протесту;
- дискредитування історичних фактів та національної самобутності народу;
- зміна системи цінностей, яка визначає спосіб життя і світогляд людей;
- применшення та нівелювання визнаних досягнень у науці, техніці та інших галузях з акцентом на помилках, недоліках та хибних діях влади;
- завдання шкоди інформаційно-технічній інфраструктурі (технічним засобам, програмному забезпеченню, засобам захисту від витоку інформації).

Ці дії формують передумови для економічної, духовної чи військової поразки, втрати волі до боротьби та перемоги. Водночас ворог намагається представити свій спосіб життя як модель для наслідування, а також захиститися від деструктивного інформаційно-психологічного впливу з боку інших.

Таким чином, завдання інформаційних війн полягають у впливі на свідомість і психіку як окремих людей, так і суспільства в цілому, маніпуляції їх поведінкою, дезінформації та руйнуванні їх моральних та ідеологічних засад. Інформаційні війни стають ефективним інструментом у гібридних конфліктах, де основною метою є вплив на свідомість і волю населення, а не лише на фізичні об’єкти чи ресурси.

Висновки

Війни в інформаційному полі ведуться тисячоліттями, вони є невід’ємною частиною будь-яких воєнних кампаній. Головна мета інформаційної війни — послабити моральні та матеріальні сили противника або конкурента і посилити власні. Зброєю цієї війни є донесення інформації таким чином, щоб змінити сприйняття та думки щодо ситуації, переосмислити мотивації жертви, втратити розуміння істини та неправди. Усе це веде до формування передумов для економічної, духовної чи військової поразки, втрати волі до боротьби та перемоги.

Заняття 2. Учасники інформаційної війни

Мета заняття:

- дізнатися про розподіл ролей в інформаційній війні;
- проаналізувати ефект застосування мережі штучних користувачів;
- проаналізувати прояви ІВ у сучасній російсько-українській війні.

Вступ

Інформаційна війна не відбувається сама по собі. Як і в інших військових підрозділах, її учасники мають чіткий розподіл обов'язків та свої завдання. Вміння їх виділити, зрозуміти їхні цілі та мотиви дає можливість протистояти ворожому впливу.

1. Рівні учасників інформаційної війни

Можна виділити кілька рівнів учасників інформаційної війни за рівнем суб'єктності. Зверніть увагу, ті, проти кого ведуться ІВ, не є їх учасниками, бо вони не самостійні в такому протистоянні. Їх вважають всього-на-всього «територією боїв».

Низовий рівень: тролі, боти, активісти з асоціальними настроями.

Тролі – термін походить або зі скандинавської міфології про злу і шкідливу істоту, або від слова «тролити», що з англійського рибацького сленгу перекладається як – вести, водити (рибалка водить вудкою, імітуючи активність приманки, аби привернути до неї увагу). Коментарі тролів дуже часто є емоційно зарядженими або просто образливими, такими, що провокують сварку. Основна мета «тролінгу» – спровокувати людей на активну дискусію щодо тієї чи іншої теми в потрібному ракурсі або «поховати тему» за сваркою. Може діяти за гроші або з ідеологічних мотивів.

Боти – це програми, які в автоматичному режимі реагують на ключові слова і відповідно реагують. Комерційних ботів застосовують у підтримках клієнтів (вони можуть автоматично відповідати на питання користувачів сайту, надаючи підтримку клієнтам 24/7), автопостять контент у соцмережах, моніторять згадки бренду, розсилають повідомлення тощо. Але боти інформаційної війни починають імітувати дискусію за ключовими словами. Також так називають людей, що займаються подібним – масовим поширенням коротких, схожих між собою, повідомлень. Вони навіть не беруться аргументувати свою позицію, тільки репостять картинки чи повідомлення. Також ботами називають найманих інтернет-користувачів, які штучно створюють ілюзію суспільного інтересу до потрібного їм медіа-ресурсу або тематики. Під час повномасштабної фази війни СБУ викривала цілі мережі російських ботів, які налічували тисячі і навіть десятки тисяч акаунтів у різних соцмережах.

Що більш авторитарний устрій, то більше можна говорити про наявність мережі державних тролів. Вони є офіційними інструментами – учасниками атак із дестабілізації. Їхнім завданням на внутрішньому інформаційному полі може бути делегітимізувати всі канали інформації, які суперечать основній доктрині, наприклад, посіяти недовіру до опозиції. У випадку дій за кордоном – працюють просто як дестабілізатори внутрішньодержавної ситуації.

Терористичні структури також використовують тролів для розбудови бренду. Наприклад, терористична організація ІДІЛ створює словесну змістовну, а головне – емоційну картинку. У процесі дискусії далі перенаправляє користувачів на інші ресурси, де можна пройти вербування, залучення до активних дій. Теж саме проводять російські спецслужби, вербуючи зрадників у соцмережах. Спочатку вони починають спілкування, а згодом дають завдання зі збору інформації, диверсій і терористичних актів.

Завдання штучних користувачів:

- швидке поширення фейків та дезінформації;
- розпалювання ворожнечі, поширення стереотипів, зокрема образливих;
- відволікання уваги від важливих суспільних подій, заглушування конструктиву, перехід на особисті образи;
- створення ілюзії важливості тем, які вони просувають або коментують;
- провокації емоційних дискусій з реальними людьми, вплив на психоемоційний стан;
- організація інформаційних атак;
- цькування, залякування;
- збір інформації для ворога.

Згідно з даними ресурсу Statista, тільки за перший квартал 2022 року Facebook видалив 1,6 млн фейкових акаунтів. У X (Twitter), за різними оцінками, від 5 до 20% фейкових акаунтів, а в Instagram кожна десята сторінка є несправжньою.

Активісти. До подібних належать «конспірологи», «вічні борці проти всього поганого», громадяни, які постійно нікому не довіряють (зокрема власному уряду). Ними, як правило, легко маніпулювати, нав'язувати певну думку, яку вони продовжують транслювати вже від себе дуже активно. Прикладами таких активістів є антивакцинатори, прихильники масонської змови, плоскоземельці тощо.

Середній рівень: лідери думок (інфлюенсери), ЗМІ.

Інфлюенсери – це лідери думок. Думка цих людей має значення для певної аудиторії. Найчастіше вона взаємодіє зі своєю аудиторією через соціальні мережі: Тік-ток, Instagram, Facebook або YouTube. Інфлюенсери у звичайному варіанті діляться власними думками, розповідають про останні тенденції в будь-якій сфері: від приготування їжі до політики . Бути цікавим для аудиторії означає мати фінансовий прибуток від переглядів або за рахунок прихованої (чи навіть явної) реклами в пості чи відео. Але прибуток може бути і при «вкиданні» потрібних для інформаційної війни тез.

ЗМІ. Сьогодні традиційні ЗМІ виконують роль лише посилювачів тих чи інших тез. Як правило, небагато редакцій можуть тримати у своєму штаті якісних журналістів-творців оригінального контенту. Проте вони однозначно є учасниками (свідомо чи несвідомо) інформаційних спецоперацій.

Вищий рівень ІВ. На цьому рівні діють самі творці інформаційних кампаній, атак, стратегій війни, політтехнологи, психологи, спеціалісти з комунікацій, соціологи тощо. Перелік цих осіб може бути великим і включати цілі наукові установи. Це ті люди чи структури, які вивчають сферу діяльності, збирають, аналізують інформацію, створюють стратегії та планують війни чи просто окремі інформаційні операції. Майже всі вони є непублічними та невідомими широкому загалу.

2. «Ольгинські тролі» росії

російська особливість у використанні ботів та тролів - їхнє системне активне та цілеспрямоване використання в інформаційних операціях. Для їх учасників навіть з'явився термін - «Тролі з Ольгіна» або «фабрика тролів». Цією загальною назвою позначають користувачів-провокаторів (тролів), які за гроші в спеціально обладнаних офісах залишають дописи та коментарі під новинами інтернет-видань або на інших ресурсах у мережі з метою розповсюдження російської пропаганди в соціальних мережах. Це своєрідний вид роботи у росії; ці підрозділи підпорядковані ФСБ.

Це поняття походить від назви однієї з установ, «Агентства інтернет-досліджень», спеціально обладнаної для тролінгу офісу, який був викритий першим і став найбільш відомим. Його російські журналісти викрили у 2013 році в Ольгіно, історичному районі Санкт-Петербурга. Пізніше назви «тролі з Ольгіна» або «ольгінські тролі» стали загальними щодо тролів, які здійснюють російську державну пропаганду без прив'язки до офісу в Ольгіно.

Тривалий час припускали, що це агентство пов'язане з Євгенієм Прігожиним, а 2023 року він підтвердив це особисто. У свою чергу Прігожин – колишній кухар, а також довірена особа путіна, виконавець його специфічних завдань, творець приватної військової компанії «Вагнер».

Аналітики «Вокс Україна» провели масштабний аналіз понад 750 тисяч постів у соціальній мережі X (колишній Twitter), що пов'язані із «Агентством інтернет-досліджень». Спеціалісти дослідили тематику публікацій, визначили найбільш популярні події для висвітлення за 8 років. Аналітикам вдалося віднайти акаунти, які твітили майже 33 години підряд.

3. Ознаки ботів та тролів

Часом важко сказати, чи якийсь користувач – бот чи реальна людина з вкрай радикальною позицією, підозрілива до всього або працює в державній установі і не хоче демонструвати свою позицію. Втім, існує декілька ознак, якими можна охарактеризувати бота:

- відсутність аватарки або розмите нечітке фото, абстрактна картинка (квіти, котики, малюнки або синьо-жовта композиція) замість знімка. Це неоднозначна ознака, бо під псевдонімами з

фото квітів чи тварин можуть ховатися люди з окупованих територій, військові або волонтери, які приховують справжнє фото або ім'я з міркувань безпеки;
- відсутні світлини з різними ракурсами людини, є тільки одне старе або групове фото, за якими складно ідентифікувати особистість;
- неперсоналізовані публікації, думки тощо, замість власних постів — тільки репости;
- відсутні лайки або їх незначна кількість під дописами;
- недостовірна або зовсім не заповнена інформація в профілі;
- публікація коментаря з одним і тим самим текстом;
- часте використання посилань на сторонні сайти (боти в середньому в 3 рази частіше використовують посилання);
- дивне співвідношення дати реєстрації й кількість публікацій (наприклад, акаунт створений місяць тому, а вже налічує сотні однотипних публікацій);
- частота публікацій (наприклад, пост чи коментар кожні кілька хвилин);
- дивне ім'я акаунта. Наприклад, «Адольф Пінкевич» або «Василіна Горгульєва». Зрозуміло, що людина може мати дивне ім'я і прізвище, але тоді Google мав би показати результати іншої діяльності такої «Василіни» поза соцмережею. російські боти часом використовують імена «під слов'янську старовину» – Славомир, Пересвет, Владомир тощо;
- автоматичний переклад тексту як одна з найсмішніших ознак. Саме завдяки ботам і такому перекладу існують меми про «бавовну», «немає сечі терпіти ці пекельні борошна» (російською – «нету мочи терпеть эти адские муки»), «підлога країни без електрохарчування», ім'я «Насіння» (Семен у родовому відмінку) тощо.

Сукупність кількох таких ознак з більшою ймовірністю дає стверджувати, що профіль належить боту. Подібним чином можна встановити троля. Так, найголовніші ознаки тролів – поведінка в коментарях:

- зауваження НЕ за темою;
- відмова визнати неправоту;
- маніпуляції, напівправда, хибна аргументація;
- акцент на емоції, а не логіку;
- меми-картинки як реакції на змістовні дописи або коментарі;
- принизливий тон, агресивність;
- намагання змусити читача порушити правила спільноти, «вийти з себе»;
- перехід на особистості;
- звинувачення інших у продажності/ заангажованості;
- реагування на викриття не особисто, а за допомогою інших акаунтів (працюють групою);

- швидкі, «серійні» й довгі відповіді – троль отримує більшу оплату за довші коментарі.

Будь-яка реакція, спростування, дискусія з тролем беззмістовна. Натомість він отримує більшу зарплату за вашу реакцію.

АрміяInform провела власне дослідження про безпеку військових у соціальних мережах. За підсумками опитування, 25% військовослужбовців ЗСУ не знають, як часто до них у друзі долучаються боти, адже не завжди вміють їх розрізняти. Ще 6,3% опитаних військових відповіли, що під час користування соцмережами траплялися випадки, коли з невідомих акаунтів надходили повідомлення провокативного характеру, повідомлення-погрози і спроби вивідати певну інформацію.

4. «Заклики до миру» як технологія інформаційної війни

Завдяки ботам та інфлюенсерам (багато з яких, як припускається, роблять це за відповідну оплату) росія здійснює тиск на Україну для примусу до мирних переговорів. По суті, агресор, який вибудовував імідж непереможного, тепер закликає жертву припинити протистояти агресії з метою досягнення миру.

росія досить легко залучає до своїх спільників навіть світових інтелектуалів і лідерів думок від Папи Римського до найвідомішого сучасного німецького філософа Юргена Габермаса і феміністки Джудіт Батлер, які закликають українців «домовлятися», «комунікувати», йти на компроміс. Мовляв, це робиться для блага українців.

Подібний вислів прозвучав на дебатах між кандидатами (станом на 11 вересня 2024 року) на пост Президента США з уст Дональда Трампа: «Я хочу, щоб війна припинилася. Я хочу врятувати життя, які марно втрачають. Людей вбивають, мільйони. Їх мільйони».

Проте, якими благородними формулюванням це не прикривалося, по суті залишається простим закликом до безумовної і повної капітуляції перед агресором, а отже, сприянням злочину.

Якщо спроби підштовхнути Україну до переговорів не вдаються, хтось із російських діячів (пропагандисти, депутати або колишній маріонетковий президент Мєдвєдєв) починають погрожувати застосуванням ядерної зброї або проводять ядерні військові навчання. Це, на думку агресора, повинно лякати середньостатистичних жителів західних країн та посилювати їхнє бажання завершити війну, навіть шляхом втрати Україною територій.

Одним із інструментів для досягнення цілей росії у світі використовується «м’яка сила» (soft power) – усе, що формує позитивний імідж росії на міжнародній арені (культура, спорт, гуманітарні декларації тощо). Завдяки цьому в «миротворчому» процесі поєднуються несумісні позиції: протестні настрої консервативних прихильників політичного нейтралітету (наприклад, австрійські виборці, які переважно не підтримують постачання зброї – «не наша війна» або німецький пацифізм «ніколи знову»), обурення американських і європейських аполітичних виборців інфляцією («чому ми платимо за конфлікт у чужій

країні»), правих прихильників «сильної руки» («слабкий має поступитися сильному, бо все одно програє»), лівих прихильників компромісу за будь-яку ціну («усі війни безглузді і несправедливі, тому потрібно зробити все, щоб її зупинити»), космополітичних інтелектуальних лібералів («яка різниця, чий Крим, аби люди не вмирали»).

Приклад 1. Фільм «Росіяни на війні»

TVO – канадська державна фінансова організація та суспільний мовник у провінції Онтаріо виділила державні кошти на фільм російської режисерки Анастасії Трофімової «Росіяни на війні». Трофімова позиціювала фільм як антивоєнну історію про долю російських солдатів. Його встигли показати на Міжнародному кінофестивалі у Венеції.

Насправді фільм спотворює реалії російсько-української війни та поширює російські пропагандистські наративи, применшуючи злочини російських солдатів проти українських цивільних. Так, інші фільми Трофімової без перешкод транслювали на Russia Today, що є рупором російської пропаганди та перебуває під санкціями Канади. Крім того, режисерка незаконно перетнула державний кордон України. А головне – стрічка перекидає відповідальність за воєнні злочини конкретних учасників вторгнення – російських солдатів на щось аморфне, якусь «пропаганду» і «туман війни».

Після багатьох акцій та заяв протесту Конгресу українців Канади показ фільму в Канаді скасували.

Приклад 2. Діяльність Кіріла Сєрєбряннікова.

Режисер Кіріл Сєрєбряніков довгий час вважався нібито тим самим сміливим «російським дисидентом», який перебував під домашнім арештом і не міг покинути територію Росії. Але весною 2022 року виникла потреба в репрезентації «хороших русских» на світовій арені. Тому його арешт швидко зник, а сам режисер прямо під час пресконференції фільму в Каннах закликав припинити «кенселінг російської культури» та висловив співчуття російським військовим (якраз тоді стали відомі злочини в Бучі та інших містах Київщини). Він також закликав зняти санкції з російського олігарха Романа Абрамовича.

Того ж року Серебренніков поставив виставу в Гамбурзі, де чітко простежувався меседж: у війні страждають і росіяни, і українці. Таким чином прирівнюється агресор і жертва і розмивається відповідальність.

Висновки

Інформаційні війні мають свою чітку ієрархію учасників: низовий (боти, тролі, активісти), середній (лідери думок та ЗМІ), вищий (технологи). Для втілення своїх завдань використовуються численні «фабрики», які створюють видимість масової підтримки потрібної думки. Втім, є ознаки, за якими можна розпізнати учасників інформаційного впливу в соцмережах.

Сьогодні головне завдання ворожих учасників ІВ - примусити Україну погодитися на умови невигідного миру.

Заняття 3. Методи інформаційної війни (пропаганда, дезінформація, кібератаки, психологічні операції, інформаційні операції)

Мета заняття:

- дізнатися про головні психологічні ефекти, які використовуються під час інформаційних операцій;
- дізнатися про найпоширеніші методи впливу, які використовуються під час інформаційних воєн;
- на конкретних прикладах проаналізувати застосування росією методів інформаційних воєн проти України.

Вступ

Незважаючи на зміну обстановки, технологій, суспільного устрою, людська психологія залишається незмінною. Саме особливості реакції людини на ті чи інші події піддаються впливу під час інформаційних операцій.

1. Особливості поведінки людини у суспільстві

Головна особливість інформаційної війни – дуже швидка зміна, адаптація. Це пояснюється стрімким розвитком технологій та дешевизною застосування цифрових технологій.

Натомість один із найважливіших факторів реагування людини на нову обстановку (подію чи інформацію) – страх. Це одна з первинних емоцій, вона концентрує увагу на саму подію. Чим більше тривоги посіяно у групі, в якій перебуває людина,тим більше вона буде схилятися до поширення чуток. Натомість після появи страху раціональне сприйняття вже не спрацьовує, людина набагато важче може критично оцінити емоційно заряджену інформацію.

З цією метою поширення постів-залякувань чи чуток-страшилок є свідченням спроби “відключити розум”.

Ідеологічна основа сучасних комунікацій – політика післяправди – дії та мислення, які спираються на почуття та власні переконання, які насправді не мають під собою реальних підстав (фактів). Істина не фальсифікується, а просто відсувається, “відходить на другий план”. Це означає, що важливою для сприйняття є не подія (вона може бути навіть вигаданою), а реакція чи емоції на цю подію. І вже не важливо, чи був такий факт.

Найголовнішими чинниками, які сприяють такій політиці, є розвиток ЗМІ. Роздробленість джерел новин створює ситуацію, в якій брехня, плітки і чутки розповсюджують з надзвичайною швидкістю. Відомо, що журналістів навіть вчать, що найкраще поширюються новини, які мають 7 орієнтирів: Скандали, Сенсації, Страх, Смерть, Секс, Сміх і Гроші.

В соцмережах **вступає в дію ще один фактор: довіра між користувачами. Незнайомі люди вірять один одному більше, ніж навіть найбільш відповідальним ЗМІ. Тому брехня, яку поширюють політики чи їх прибічники в інтернеті в групах, може дуже швидко підмінювати правду.**

Поширення чуток і брехні є ситуацією не новою: відомою є картина “Істина, яка вибирається з криниці, озброєна батогом для покарання людства”, створена в 1896 році Жаном-Леоном Жеромом. Вона базується на легенді про Брехню, яка вкрала одяг Істини і тепер ходить по світу, а Істина тільки намагається її догнати. Ще один приклад – цитата, яку приписують Вільяму Черчілю “Брехня встигає обійти півсвіту, поки правда одягає штани». В українських народних приказках також застерігали, що “краще гірка правда, ніж солодка брехня”. Але на практиці люди більш охоче вірять у приємну брехню.

Чутки виникають та поширюються, коли люди невпевнені та стурбовані щодо теми, до якої мають особисте відношення (щось, що стосується рідних, місцевості проживання, релігії, політики або інших тем).

У сьогоднішньому мережевому світі люди також навмисно розповсюджують неправдиву інформацію та чутки як жарти з метою зібрати вподобайки, привабити послідовників (“фоловерів”) чи спровокувати паніку.

В інформаційній війні сторони використовують психологічні особливості людей, зокрема:

- ефект Даннінга-Крюґера. Він притаманний некомпетентним людям, які переоцінюють себе та схильні робити помилкові висновки (бо не орієнтуються в тематиці). Але при цьому вони більш упевнені у своїх висновках, ніж ті, хто насправді є спеціалістом.
- ефект приєднання до більшості (ефект наслідування). Ця форма групового мислення проявляється в тому, що популярність певних переконань збільшується у міру того, як їх приймає дедалі більше людей. Якраз на дану особливість націлені боти.
- ефект хибного консенсусу: люди вважають, що їхні переконання, думки та переваги є більш поширеними, ніж вони є насправді.

2. Засоби інформаційної боротьби.

Для розуміння ІВ важливо розуміти її засоби, тобто знаряддя, якими вона ведеться. До таких належать:

- програмно-комп’ютерні технології, які атакують комп’ютерні системи військового або державного управління. Завдяки їм можна спостерігати, блокувати чи руйнувати виробничі процеси ворога (найвідоміший приклад – комп’ютерні віруси, також логічні бомби та інші);
- радіоелектронна боротьба – спрямована на розпізнавання, виявлення та протидію системам супротивника. Включає в себе встановлення радіоперешкод, створення об’єктів-невидимок і придушення радіоелектронних засобів супротивника;
- лінгвістичні засоби, відомі як частина «мови ненависті», передбачають формування «образу ворога» в інформаційному суспільстві та його називання. Наприклад, відносно росіян тепер застосовуються такі терміни як русня, московити, рашики, рашисти, кацапи, свинособаки і піґ-доґи (замінник, щоб не блокували в соцмережах) та інші, менш культурні, тощо;
- чутки та плітки – поширення сумнівної інформації та неперевірених висловлювань;
- пропагандистська діяльність – формування моральних та етичних стандартів і світогляду, створення певних норм, встановлення зразків для наслідування та поширення міфів. Її реалізація здійснюється через різноманітні засоби, такі як словники, енциклопедії, підручники, відео- та аудіопродукція тощо;
- цензура – система контролю за ЗМІ та соцмережами, нагляд та управління інформаційним простором з боку влади;
- ЗМІ усіх видів.

3. Методи інформаційних операцій та воєн.

Методів, що застосовуються в інформаційній агресії, є доволі багато, але назвемо серед них наступні:

- дезінформування та маніпулювання;
- пропаганда;
- диверсифікація громадської думки;
- психологічний та психотропний тиск;
- поширення чуток.

Слід зазначити, ці методи застосовуються в комплексі. Крім того, їх дуже часто використовують політтехнологи під час виборів. Через це ворожа інформаційна діяльність не відрізняється від дій політичного опонента.

Під час інформаційної війни з метою отримання переваги над супротивником часто користуються методом обману або введення об’єкта спрямувань в оману щодо справжності намірів, справжнього стану справ, тобто викривлення реальності. Це є методом дезінформування.

Дезінформація змінює довіру людей до медіа чи влади та підриває їх авторитет. Основною метою дезінформації є руйнування довіри не до конкретного органу, а до правдивої інформації в цілому. І брехня дійсно швидше поширюється: вченими Массачусетського технологічного інституту під час тривалих досліджень було встановлено, що твіти з дезінформацією поширюються “живими” людьми набагато швидше, ніж правдиві. Таким чином загроза цього методу інформаційного впливу є ще більшою.

Натомість маніпулювання – це спосіб психологічного впливу, спрямований на зміну напряму активності аудиторії, її ідей, думок, поглядів тощо, який залишається непоміченим. Це також нав’язування ідей, установок, мотивів, стереотипів поведінки, вигідних маніпулятору.

Виділяють три рівні маніпулювання:

- посилення існуючих у свідомості людей потрібних маніпулятору ідей, установок, мотивів, цінностей, норм;
- часткові, малі зміни поглядів на ті чи інші події, процеси, факти, що також впливає на емоційне і практичне ставлення електорату до конкретного явища;
- докорінна, кардинальна зміна життєвих установок шляхом поширення серед виборців сенсаційних, драматичних, надзвичайно важливих для них повідомлень.

Маніпуляції здійснюються найчастіше за допомогою ЗМІ. Дане питання буде розглянуте в одній із пізніших тем.

Одна з важливих ознак маніпуляцій – ніхто нікого не примушує нічого робити. Людина, яка стала жертвою маніпуляції, вважає, що діє за власним бажанням і за власним вибором. І буде цей свій вибір захищати щосили (це особливо помітно на прикладі політичного вибору, зробленого під впливом маніпуляцій).

Пропаганда. Цей термін часто використовують як тотожний терміну “інформаційна війна”. Але насправді це форма комунікації, спрямована на поширення інформації у різному вигляді для впливу на суспільну думку. Пропаганда має свої чисельні методи та види.

Вважається, що існує 3 види пропаганди:

- біла (не допускає спотворення фактів задля політичних цілей);
- сіра (допускає незначні перекручування фактів);
- чорна (допускає будь-яке спотворення реальності заради досягнення завдань.

Важливість пропаганди стала зрозумілою після вивчення ведення кампаній ідеолога та пропагандиста нацизму Йозефа Геббельса. Він проводив цинічну пропаганду ідей нацизму та став фактичним творцем ідеї геноциду євреїв. Тому найгірші види пропаганди називають геббельсівською - навмисне перекручування фактів або неправда вперемішу зі справжніми фактами.

Принципи пропаганди Геббельса:

- принцип напівправди. У будь-якому облудному повідомленні має бути елемент усім відомої правди – так легше повірити в будь-що;
- принцип “Великої брехні”. Тут можна згадати всім відомі слова, які часто приписують Геббельсу: “Чим жахливіша брехня, тим охочіше в неї вірять”. Насправді він їх не казав і не писав – це цитата з “Майн Кампф” Гітлера. Проте міністр пропаганди регулярно дотримувався цієї настанови.
- принцип простоти. Послання має бути примітивним – тоді в нього повірять;
- принцип зрозумілості. Для конкретної аудиторії слід обрати мову, зрозумілу саме їй.
- принцип повторення. Одну й ту саму брехню треба постійно повторювати – тоді вона стане правдою.

Назвемо також кілька методів бойової спецпропаганди, яку застосовували в Радянському Союзі, в першу чергу проти політичних опонентів.

1. “Гнилий оселедець”.

Береться абсолютно хибне звинувачення, яке має бути максимально шокуючим, брудним і скандальним. Мета – викликати бурхливе обговорення, прив’язати ім’я жертви до бруду і скандалу. Таким чином він починає асоціюватися із неприємністю, “запахом гнилого оселедця”.

2. Велика брехня (повторює Геббельса).

Мета – викликати такий шок та негативні емоції, що громадянин ще довго не буде сприймати тему аргументовано, через логіку та розум.

3. Абсолютна очевидність.

Заявляючи якусь брехню, подається її так, ніби це всім зрозуміло і давно відомо. Психіка керує так, щоб людина прагнула приєднатися до більшості та не аналізувала поданий матеріал.

4. Невідомий герой.

Приписування діям своєї сторони благородних цілей (рос. варіант “боротьби з нацизмом”, “порятунок Донбасу”, “війна проти зла” тощо). Тому образ російських військових для свого суспільства – рятівники, визволителі.

5. Багаторазове повторення (ще один метод Геббельса).

“Брехня, яку повторюють, стає правдою”. До речі, за таким же принципом діють рекламні агенції, готуючи кампанії.

6. Напівправда.

Йде змішування брехні з правдою. Людина не може відразу заперечити, бо часткова правда ховає за собою брехню. Але ключові моменти, які змінюють зміст, якраз неправдиві.

7. Страшилки.

Порівняння великого і малого зла. Із ворога робиться образ великого, абсолютного зла. Тому менше зло у війні проти більшого, в

нашій свідомості виправдовує погані вчинки людей або держав. В ідеалі народ має сам вибрати найменше зло.

8. 40% на 60%.

Інформація подається 60% – на користь ворога, для підтримання довіри аудиторії, 40% – дезінформація. Приклад – радіостанція, яка працювала за цим методом під час Другої світової війни, орієнтована на британського та американського слухача. Багато хто вважав, що це британське ЗМІ, і лише після війни з'ясувалося, що то була частина гітлерівської пропаганди.

Сучасна росія часто застосовує ще одне тактику, «Вогнемет брехні»: засмічення інформаційного простору неправдивою інформацією настільки, щоб споживач втомився шукати правду і сприймав все, що йому сказано.

Дослідник пропаганди французький соціолог Жак Еллюль запропонував розрізняти вертикальний та горизонтальний види пропаганди. Вертикальна – це класичний варіант, інформаційний потік згори до низу з пасивним реагуванням аудиторії. Горизонтальну пропаганду Ж. Еллюль називає новим винаходом. Вона зветься горизонтальною, бо реалізується в певній соціальній групі, а не йде згори. У цій ситуації всі учасники є рівними, серед них немає лідера, а тому інформація сприймається з максимальною довірою. Такими соціальними групами сьогодні можна вважати спільноти в соцмережах.

Фахівці вважають, що пропаганда тільки тоді приречена на провал, коли вона зовні схожа на пропаганду. Тобто мова йде про непомітність як ознаку ефективності. Відповідно до цього критерію, більш ефективною буде горизонтальна пропаганда, бо вона не є зовнішньою, нав'язаною зі сторони, а ніби виходить із самої групи.

Явище пропаганди висвітлюють переважно в негативному світлі (в тому числі через нацистську і радянську). Проте це справедливо стосовно авторитарного режиму, коли інші джерела інформації недоступні. В іншому випадку все залежить від кінцевої мети: пропаганда може бути й позитивним інформаційним процесом, способом донести людям потрібну їм інформацію, поширення демократичних принципів, цінностей цілісності, єдності суспільства, патріотизму.

Диверсифікація громадської думки. У веденні інформаційних воєн за допомогою різних прийомів можна розпорошити увагу правлячої еліти держави (або навпаки – громадської думки) на різні штучно акцентовані проблеми. Тим самим або державу, або суспільство відволікають від вирішення першочергових завдань на щось другорядне.

Форми диверсифікації можуть бути різними:

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

Психологічний та психотропний тиск. Зараз є підстави говорити про виокремлення нового виду зброї – інформаційно-психологічної зброї (ІПЗ). ІПЗ – самостійний засіб ведення інформаційної війни. ІПЗ – насильницьке викривлення інформаційно-психологічного простору супротивника спеціально для ураження індивідуальної і масової свідомості. Мета такого впливу – придушення, знищення, дезорганізація та дезорієнтація об'єктів.

Ця зброя спроможна порушити психічне здоров'я населення, спонукати до спонтанних дій, спричинити тимчасові чи незворотні зміни чи навіть самознищення, підкорити свідомість (та підсвідомість) особистості і спрямувати її в необхідному для суб'єкта впливу напрямі. Ці зміни та дії проходять досить фатально для об'єкта, на який вони скеровані.

Психогенний вплив є наслідком: 1) фізичного впливу на мозок індивіда, результатом якого можуть стати порушення нормальної нервово-психічної діяльності; 2) шокового впливу навколишніх умов або будь-яких подій (наприклад, картин масових руйнувань, численних жертв і т.ін.) на свідомість людини, внаслідок чого вона не може раціонально діяти, втрачає орієнтацію у просторі, відчуває афект або депресію, впадає в паніку, ступор.

Чим менше підготовлена людина до психотравмуючих впливів навколишньої дійсності, тим більше вираженими будуть її психічні травми, що одержали назву психогенних втрат.

Окремим випадком психогенного впливу є вплив кольору на психофізіологічний і психічний стан людини.

Особливою складністю в Україні є той факт, що методи росії в інформаційній війні дуже часто є цинічними та аморальними, як методи політичних кампаній під час виборів (маніпуляції, дезінформація, чутки та психологічний тиск) або й частково методи відносин між владою і суспільством. За таких умов окремий громадянин піддається постійним інформаційним атакам з різних сторін від противника (противників) і від своїх же співгромадян-політиків.

4. Застосування росією інформаційних операцій у війні проти України

Ключовим в російських інформаційно-психологічних операціях (ІПСО) є поширення ідеології «російського світу» - "рускій мір". "Рускій мір" – термін, який первісно був придуманий російським філософом Щедровіцкім для визначення культурно-цивілізаційної, геополітичної і релігійної концепції, що мала на увазі об'єднання російськомовного населення по всьому світу. Згодом він був використаний владою для пропаганди рашизму – російського різновиду фашизму. Він базується на ідеях "особливої цивілізаційної місії" росіян, "старшості братнього народу", нетерпимості до елементів культури інших народів, здебільшого слов'янських (бо їх простіше русифікувати), а також до народів, що проживали в Російський імперії чи СРСР; ультранаціоналізмі,

використанні російського православ’я як моральної доктрини, геополітичних інструментах впливу (насамперед енергоносіях для європейських країн), військовій силі стосовно країн, що входять до сфери впливу рф. Головна мета рашизму – відновлення СРСР і включення (насильницьке або добровільне) колишніх республік до його складу.

За таких умов російська мова стала ознакою, а водночас метою поширення решти ідеологічних складових російщини: культури, світогляду, політичних переконань.

Традиційні вектори російського впливу на пострадянському просторі до 2022 р. реалізовувалися через агентурну мережу – московську православну церкву, агентство “Россотрудничество” і фонд “Русский мир”, які організовували контакти з близько 25 млн росіян, котрі проживають за кордоном.

Комунікативно-пропагандистська робота російської влади скерована на три основні напрямки:

- для власного населення;
- для російського населення в інших країнах;
- для населення світу.

ІПСО росії проти України застосовувалися як за допомогою ЗМІ, так і за участю великої кількості російських агентів, в тому числі у найвищих ешелонах влади.

Перший відомий її прояв – ситуація з нібито продажем Іраку, що перебував під санкціями, чотирьох станцій радіотехнічної розвідки “Кольчуга”. Факти ніколи не були підтвердженими, але скандал завдав потужного удару як по Леоніду Кучмі, так і по міжнародному іміджу України. Ця ситуація різко знизила рівень відносин України зі США.

Можна наводити приклади російських дій на очорнення Помаранчевої революції, Президента Віктора Ющенка та України до 2014 року (міфи, які були вкинуті у той час, використовуються дотепер громадянами, які навіть не намагаються перевірити інформацію). Звідси постає запитання: а чи є жертвами ті, хто вірять у пропаганду і навіть не намагаються перевірити факти або ж чи мають вони відповідати за свої переконання, сформовані під впливом пропаганди?

Російські ІПСО максимально використовують матеріал, який стосується реальної ситуації. Однак, вирізняє спецоперацію те, які висновки із проблеми нав'язуються. ІПСО не ведуть до конструктиву – а підштовхують до зневіри. Настрій, який масштабують маніпулятори, – “пропало” геть усе, боротися немає сенсу, довіряти нікому не можна тощо.

Також відомо, що один із основних способів розколу суспільства – протиставлення. Під час війни людям природньо хочеться розуміти, де свої, а де чужі. Цим ворог прагне скористатися. Особливо часто йде протиставлення громадян і влади або очорнення влади притаманне всім війнам, які досліджувались коли-небудь. Це буде відбуватися, будь-який ворог буде намагатися це зробити.

Одним із важливих методів, що застосовується під час інформаційної агресії у війні росії проти України, є залякування, переслідування, погрози, психологічний тиск.

Формами психологічного тиску є:

а) доведення до об'єкта відомостей про реальні чи неіснуючі загрози та небезпеки;

б) прогнози щодо репресій, переслідувань, убивств тощо;

в) шантажування;

г) здійснення вибухів, підпалів, масових отруєнь, захоплення заручників, інші терористичні акції.

ґ) "телефонний тероризм", тобто телефонні дзвінки з інформацією про нібито замінування місць масового скупчення людей (торговельні центри) або об'єкти інфраструктури (вокзали).

У сучасних українських реаліях залякуванням є навіть часті зльоти літаків, через що оголошується повітряна тривога. Часті звуки сирен, за задумом росіян, мають викликати масовий страх або ж роздратування. З цією ж метою – викликання страху та інших емоцій в українського суспільства – задумані неприховані вбивства українських військовополонених.

В інформаційній агресії проти України були застосовані також методи психотропної дії, а саме використання забороненої технології "25-го кадру". У Службі безпеки України заявили про те, що мають докази використання російськими телеканалами технології "25-го кадру" для інформаційно-психологічного впливу на глядачів. Багато фактів зафіксовано із використанням маніпулятивних технологій на державних новинах. Наприклад, під час випуску новин у куті екрана з'являються малопомітні написи: "підпал: "Правий сектор", "людей убивають бандерівці", "нацгвардія – вбивці". Також поширюють напівправду, показують деталізовані сцени вбивств і насильства й намагаються емоційно впливати на глядача.

Вплив може здійснюватися засобами інформаційних подразників з використанням усього спектру методів і форм технічного, візуального, звукового, медикаментозного, фізичного, больового, віртуального придушення волі.

Інформаційний вплив за допомогою текстових повідомлень здійснюється через різноманітні методи:

- замовчування (ухилення від розголошення важливої інформації, яка може вплинути на розуміння подій);
- подання неправдивого факту (використання в повідомленні маніпульованих чи недостовірних фактів);
- поєднання правдивих і неправдивих фактів і коментарів (комбінування правдивих елементів з тими, що можуть бути викривлені чи неправдиві, для створення конкретного контексту або враження);

- представлення випадкових явищ як типових і системних (зміна сприйняття шляхом виділення випадкових подій та намагання їх зобразити як загальний тенденційний характер);
- зміщення акцентів у повідомленні шляхом пропусків, підбирання маніпулятивних рубрик, заголовків, виділених цитат;
- введення в оману некоректним посиланням на джерела повідомлення: (використання завуальованих натяків на авторитетність або вказівки на неперевірені джерела, щоб зробити інформацію більш переконливою – “з надійних джерел отримано інформацію”);
- розголошення інформації, одержаної з неофіційних та ненадійних джерел;
- використання часових розбіжностей, зокрема історичних фактів для підтвердження сучасних повідомлень; викривлення хронології подій шляхом вказівки на події минулого з розрахунком на те, що деталей ніхто не пам’ятає;
- заглушування важливих фактів – тобто перенаправлення уваги аудиторії шляхом відображення другорядних повідомлень або створення мозаїки інформації про актуальні та неактуальні події з метою ускладнення формування пріоритетів у сприйнятті інформації реципієнтом.
- використання слів-подразників із зарядом емоцій – використання таких висловлювань, як “правда”, “свобода”, “демократія”, “патріотизм”, “зрада”, “фашизм”, “корупція”, з метою викликати конкретні позитивні або негативні асоціації; апеляція до почуттів та ефективне використання очікувань, таких як “достаток у домі”, “стабільність”, “впевненість у майбутньому”, “гордість за батьківщину”;
- використання штампів – застосування узагальнених висловлювань, таких як “глобальні проблеми” або “захист інтересів”, для створення загального враження або відзначення певних ситуацій;
- навішування ярликів, таких як “хунта” чи “країна, яка не відбулася”, з метою виокремлення та спрощення певних ситуацій чи образів, щоб вплинути на сприйняття аудиторії;
- використання дієслів наказового способу для спонукання до дії (застосування дієслів “проголосуй”, “не спи”, визначайся”, з метою прямого заклику до аудиторії виконати певні дії);
- “гіпнотизування” термінами, неологізмами, запозиченнями;
- домінування негативних та трагічних новин, створення образу загрози військового, екологічного та економічного характеру. Наприклад, акцентування уваги на публікаціях, які містять в собі виключно негативні аспекти та трагічний зміст, з метою створення образу загрози, наприклад, за допомогою заголовків, подій чи заяв, як от “Україну перетворюють на ядерний могильник”.

Висновки

У питаннях, пов’язаних із ЗСУ та війною, взагалі дуже часто трапляються приклади ІПСО. Річ у тому, що і солдат, і офіцер знає

ситуацію тільки на своєму відтинку. Але готовий свої висновки поширювати про всю лінію протистояння, отримувати перегляди, реакції...

Росія в рамках своїх складних інформаційних і дезінформаційних операцій активно взаємодіє з так званими неурядовими організаціями (екологічними організаціями, які працюють проти сланцевого газу), щоб зберегти європейську залежність від імпортованого російського газу

Поширення фейків небезпечне тим, що у людини знижується критичний поріг, і людина призвичаюється до фейків, втрачається відчуття реальності. Це означає, що наступного разу буде легше поширити будь-який фейк.

Заняття 4: «Роль критичного мислення в інформаційній війні»

Мета заняття:

- Зрозуміти важливість прийняття об'єктивних рішень.
  - Засвоїти головні принципи аналізу та правильної оцінки отриманої інформації.
  - Навчитися використовувати принципи критичного мислення у повсякденному житті.
  - Усвідомити власну відповідальність за дотримання інформаційної гігієни.

Вступ

Критичне сприйняття дійсності є головним способом отримати об'єктивну інформацію, протидіяти будь-яким маніпуляціям чи помилкам сприйняття та робити правильні висновки. Детальний аналіз та перевірка інформації також є важливим рушієм прогресу.

1. Поняття критичного мислення.

Особливістю людського сприйняття є схильність до спрощення, до дії за аналогією з попереднім досвідом. Наш розум економить зусилля, тому діє автоматично, готовий сприйняти шаблон – запропоновану «картинку» – або повторити висновок, сформований раніше.

Натомість критичне мислення усвідомлене, допомагає аналізувати інформацію та ухвалювати ретельно обмірковані й незалежні рішення. Головні властивості критичного мислення – усвідомленість та самовдосконалення. Тобто власне рішення не обов'язково буде істинним (бо може бракувати інформації чи можливостей), але воно буде свідомим, базуватиметься на аргументах з урахуванням контексту.

Перешкоди для критичного мислення:

- наші упередження або викривлення сприйняття при пізнанні нового;
- вплив і навіть перевага емоцій;
- суспільний тиск, наша готовність приймати рішення, які сподобаються нашому оточенню.

Критичне мислення є м'якою (гнучкою) навичкою (soft skill), важливою для людини у будь-якій сфері: бізнесі, науці, винаходах, політиці, державному управлінні, щоденній діяльності тощо. Оскільки критичне мислення – це навичка, яку можна розвивати, над цим треба працювати щодня.

Розвиток критичного мислення йде в парі з інформаційною гігієною – обмеженням впливу маніпуляторів. При цьому відповідальність за дотримання інформаційної, як і будь-якої гігієни, лежить на самих громадянах.

В умовах війни проти України критичне мислення часто замінюють терміном медіаграмотність.

2. Складові критичного мислення та способи його розвитку.

Складові критичного мислення:

Сумнів. Насамперед мова йде про сумнів у своїй правоті. Людина повинна пам'ятати про можливість помилки. Це спонукає її перевіряти інформацію.

Аналіз. Поділ інформації, проблеми, питання на складові. Вивчення усіх деталей може вказати на реальну ситуацію.

Запитання. Додаткова інформація дає змогу виділити важливі деталі.

Відкидання, відокремлення емоцій. Для оцінки фактів потрібні тільки факти. Всі емоції можуть змінити наше сприйняття та викривити висновки.

Вивчення причин і наслідків. Кожна інформація чи подія мають свої передумови і впливають на подальші події. Вивчення цих явищ дає розуміння істинності.

«Інший погляд». Ця складова є самоперевіркою, способом уникнути помилок власних уподобань, звичок, упереджень.

На основі розуміння складових можна виділити 3 інструменти для розвитку критичного мислення, які ми можемо застосовувати щодня:

- **Лупа** – це презумпція хибності: «усе почуте, прочитане чи навіть побачене може бути хибне, тому його варто піддавати сумніву».
- **Дзеркало**, щоб пам'ятати, що ми бачимо світ через власне «відображення»: власні уподобання, сприйняття, досвід. Вивчайте когнітивні викривлення і не давайте їм заманити вас у пастку.

- **Ваги** – інструмент, щоб ставати на бік опонента. Відома порада: перш ніж засуджувати іншого, візьми його взуття, пройди його шлях. Ця порада закликає зрозуміти позицію опонента або просто іншої людини. ЙІдеться не про виправдання чи схвалення, а про розуміння причин чиїхсь дій. Використовуючи цей інструмент, ми знаходимо набагато більше варіантів розв'язання проблеми.

У деяких країнах критичне мислення викладають у школах як окремий предмет. І ось чому це важливо:

Ухвалення обґрунтованих рішень. Критичне мислення дозволяє з більшою ймовірністю досягти бажаного результату під час вирішення завдань та прийняття рішень. Це особливо важливо у сферах, де ухвалення правильних рішень має високий пріоритет. Наприклад, у медицині, бізнесі чи політиці.

Підвищення інформаційної грамотності. Критичне мислення допомагає відрізнити правду від дезінформації у новинному потоці і, що надходить через ЗМІ та соцмережі.

Поліпшення комунікації. Критичне мислення допомагає людям висловлювати свої думки та аргументи більш чітко, зрозуміло та переконливо, що сприяє ефективній комунікації. Це одна з найважливіших гнучких навичок для успішної роботи в команді.

Вирішення конфліктів. Критичне мислення може допомогти у розв'язанні конфліктів, оскільки воно сприяє об'єктивному та справедливому підходу до оцінювання розбіжностей.

Найкраще розуміння навколишнього світу. Критичне мислення допомагає людям глибше розуміти світ навколо себе, аналізувати політичні та соціальні події.

Оскільки велика кількість маніпуляцій в Україні нині надходить через ЗМІ, необхідно дотримуватися певних кроків при ознайомленні з інформаційними матеріалами:

1. Звертайте увагу на заголовок.

   А. Якісні ЗМІ не застосовують слова-магніти (особливо написані великими літерами), як-от «СЕНСАЦІЯ»,, «ДО МУРАХ», «Дивитися всім», «Це підірвало мережу».

   Б. Не використовують емоційно забарвлену лексику лише для того, щоб привернути увагу; «Він не повірив, коли побачив...», «Стало відомо...» тощо.

   В. Якщо у назві є прізвища впливових осіб, можливо, матеріал замовний (сприймайте контекст, у якому їх згадують).

2. Перевіряйте візуальну складову матеріалу.

   А. Для якісного і повного розкриття теми журналісти створюють власний фото- та відеоконтент.

   Б. Якщо картинка занадто разюча та яскрава, варто перевірити, чи вона не опрацьована у графічних редакторах.

   В. За допомогою фотошопу легко створити сенсацію, якої взагалі не було насправді.

3. Звертайте увагу на джерела інформації.

А. Шукайте першоджерело.

Б. Канал, який покликається на інший ЗМІ або соцмережі, – привід для перевірки.

В. Використання у ролі «авторитета» непрофільної особи – ознака маніпуляції. Особливо це стосується астрологів, екстрасенсів та інших шарлатанів.

Г. Що більше анонімності, «власних джерел», «деяких даних» - то менше довіри до ЗМІ.

Висновки

З огляду на інформаційну війну, відсутність критичного мислення у населення є широким полем для впливу ворожих ІПСО. Натомість критичне мислення рятує, окрім усього іншого, ще й власне ментальне здоров'я, зупиняючи спроби нав'язати думку. Розвиток критичного мислення – справа не одного місяця чи навіть року, тому в Україні стоїть завдання вибудувати бар'єр для поширення неправдивої інформації. Таким бар'єром мали би стати кілька ЗМІ або інші джерела інформації, яким би довіряли та інформацію з яких перевіряли б менш прискіпливо.

Заняття 5: «Роль медіа в інформаційній війні»

Мета заняття:

- Дізнатися про роль ЗМІ в суспільстві.
- Вивчити приклади дій російських журналістів у війні проти України.
- Ознайомитися із прикладами участі журналістів в інформаційних атаках.
- Дізнатися про методи маніпуляцій в ЗМІ.
- Проаналізувати головні напрямки управлінських дій для протистояння будь-яким ІПСО.

Вступ

Класичні та новітні ЗМІ є головними джерелами інформації для суспільства. Від журналістів (офіційних та неофіційних) залежить подача правдивої інформації та рівень застосування маніпуляцій чи пропаганди. В умовах сьогодення людей буквально завалює величезною кількістю інформації. Тому сама людина не встигає критично її аналізувати. Для правильної оцінки матеріалів ЗМІ необхідно вміти застосовувати головні способи протидії чужому впливу.

Термін медіаграмотність, який в Україні є синонімом терміна «критичне мислення», також свідчить про медіа як про найпоширеніший шлях здійснення ІПСО.

1. ЗМІ як джерело інформації.

ЗМІ самі ж журналісти люблять називати «четвертою владою», натякаючи на вплив на події в державах, який можуть здійснити окремі ЗМІ чи навіть одиничні матеріали. Тим важливіше, що сьогодні професія журналіста стала нечіткою і незамкнутою у певному середовищі: новини тепер можуть створювати всі, хто бажає.

Медіа (як традиційні ЗМІ, так і сучасні у вигляді сторінок чи каналів у соцмережах) є прямими учасниками інформаційної взаємодії, а відповідно можуть бути учасниками інформаційної війни. Особливо це стосується соцмереж: високий темп конкуренції за першість і за увагу читача не дозволяє вчасно верифікувати матеріал. У випадку анонімності автора – взагалі не стоїть питання перевірки інформації. Інша причина вкиду інформації – «хайп» (ажіотаж), бажання отримати реакції на новини (коментарі або просто емодзі).

У коментарях можуть бути цілі «зграї» ботів і тролів, а наявність тих чи інших емодзі впливає на сприйняття інформації читачем, «підказуючи правильний» варіант сприйняття матеріалу.

Журналісти офіційних (зареєстрованих державою) ЗМІ переважно намагаються дотримуватися стандартів об'єктивності та кодексу етики українського журналіста. Проте це не стосується адміністраторів анонімних каналів чи сторінок, які всю опубліковану брехню чи маніпуляції виправдовують своїм особистим розумінням свободи слова. На практиці матеріали в зареєстрованих виданнях також подають з порушеннями етики; особливо це твердження справедливе у передвиборчих періодах.

На ЗМІ покладається роль оперативного джерела інформації. Особливим став формат цілодобових новин у прямому ефірі, т. зв. «Ефект CNN» (термін застосовується в політичній науці та медіазнавстві для опису впливу цілодобових новинних телеканалів на сприйняття міжнародних подій особами, які ухвалюють політичні (і особливо зовнішньополітичні) рішення на рівні урядів і міжнародних організацій. Тобто ЗМІ вже давно стали не тільки передавачами інформації, а вони прямо впливають на прийняття рішень особами високого рангу.

Однією з концепцій, що пояснюють вплив таких новинних каналів, як CNN, і джерел інформації в цілому, є концепція «глобального села» Маршалла Маклуена, який стверджував, що внаслідок розвитку нових технологій передачі інформації світ став «стисненим», а його устрій – більш схожим на устрій села, де з огляду на невеликі розміри кожен житель дізнається новини про життя людей поруч і про різні події відносно швидко. Винахід радіо, а потім поява телебачення, а також новинних агентств і компаній з глобальним охопленням дозволили дізнаватися інформацію про події та явища в будь-якій точці земної кулі.

У подачі інформації журналістами мала б виявлятися певна регуляторна сила держави. Але зі свого боку державні чиновники можуть бути зацікавлені у відсутності вільних ЗМІ, які б не перешкоджали

зосереджувати владу. Взаємовідносини ЗМІ і держави можна розділити на форми:

- Держава повністю контролює ЗМІ
- Держава опосередковано впливає на ЗМІ
- ЗМІ існує як повністю незалежний інститут.

Головними вимірами відносин медіа з державою і суспільством є такі опозиції:

- Контроль з боку держави – Незалежність
- Конформізм – Схильність до критики
- Орієнтованість на політику – Непов'язаність із політикою.

Також ЗМІ у формі соцмереж мають свою особливість. Проблеми реагування на інформаційні напади частково пов'язані з самою суттю соцмереж у демократичному суспільстві й такими аспектами:

- право на свободу слова;
- приватність,
- монополія,
- самовираження.

Ці аспекти будь-яка влада повинна враховувати, щоб не уподібнюватися росії.

2. ЗМІ та їхній вплив на маси

Роль міжнародно розповсюджуваних цілодобових новин досягла нової стадії, коли в 1991 році проведена США проти Іраку операція «Буря в пустелі» висвітлювалася у прямому ефірі, ставши першою важливою подією такого типу і змінивши сприйняття та подачу новин. Маси дізнавалися про конфлікт на Близькому Сході переважно з екранів телевізорів. Тож уявлення людей про війну не обов'язково відповідали саме и тому, що відбувалося у той час в Іраку, але тому, що було показано по телебаченню, а отже, можна говорити радше про вибудовування засобами масової інформації соціального конструкта, ніж про передачу об'єктивної інформації.

Пізніше основний фокус «ефекту CNN» змістився на прийняття зовнішньополітичними лідерами рішень про проведення гуманітарних інтервенцій з огляду на те, що по телебаченню передавалися докладні та неодноразові репортажі про вчинення у різних країнах геноциду та інших злочинів проти людяності. Наприклад, відомими є заслуги ЗМІ у висвітленні ситуації на території колишньої Югославії в 1990-і роки та підвищенні обговорюваності цих подій і стурбованості з приводу їх розвитку, що своєю чергою змушувало політиків приймати відповідні рішення.

Крім того, пізніше паралельно з ефектом CNN стали говорити про так званий ефект «Аль-Джазіри», названий так на підставі схожого впливу арабського телеканалу. Термін цей про вплив не стільки телебачення, скільки нових медіа та соціальних мереж, що часто використовувалися цим каналом для висвітлення подій

Фактично, сьогодні, якщо про війну не говорять і не показують журналісти, її не існує для світу.

Особлива і доволі вивчена сторінка впливу ЗМІ на мислення пов'язана із Руандою. Місцева радіостанція Вільне радіо і телебачення тисячі пагорбів (фр. Radio Télévision Libre des Mille Collines, RTLMC, RTLM) – руандійська радіостанція, яка вела мовлення з 8 липня 1993 р. по 31 липня 1994 р. і відіграла значну роль у геноциді в Руанді впродовж квітня-липня 1994 року. Під час цього геноциду етнічна більшість – народність хуту – знищила близько 900 тис осіб, 90% з яких були представниками меншості, народності тутсі.

Назва станції походить від самоназви Руанди як «Землі тисячі пагорбів». Вона одержувала підтримку з боку контрольованого урядом Радіо Руанди, яке від початку дозволяло RTLMC транслювати за допомогою свого обладнання.

Станція, що була вельми популярною серед усього населення, поширювала расистську пропаганду, спрямовану проти тутсі, бельгійців та місії Організації Об'єднаних Націй UNAMIR. На переконання багатьох руандійців (із чим погодився Трибунал ООН з військових злочинів), вона зіграла вирішальну роль у створенні в країні атмосфери, зарядженої расовою ворожістю, яка уможливила геноцид. Дослідження показує, що 9.9% насильства під час геноциду було прямо пов'язано з передачами RTLMC. Оцінки дослідження вказують, що приблизно 51.000 смертей були спричинені мовленням станції.

Радіостанція не просто розповідала про вигадані «злочини тутсі». Вона складала конкретні інструкції, називала місця, агітувала брати участь: «І ви, люди, які живете поблизу Руґунди, … виходьте. Ви побачите солом'яні хатини тарганів у болоті … Я думаю, що ті, у кого є зброя, повинні негайно піти до цих тарганів … оточити і вбити їх…» - Кантано Хабімана, ведучий (головна «зірка» радіо), випускник Ленінградського університету. Передача по RTLMC, 12 квітня 1994

Конкретними підрахунками впливу радіо на різанину між тутсі та хуту зайнявся доцент-економіст Гарвардського університету Девід Янаґізава-Дротт. Ґрунтуючись на фізичних законах поширення радіохвиль, він вивів наступну формулу. Оскільки в розпорядженні RTLM були два передавачі — один в Кігалі, другий на гірському піку Муе, а Руанда геть уся покрита горами, то вони (гори) перекривають шлях радіосигналу. Тому в деяких селищах немає прийому, або ж покриття часткове. За допомогою карти рельєфу вчений розрахував рівень сигналу в кожній точці країни. Виходячи з даних, скільки саме людей у кожному селищі було засуджено за геноцид, він виявив, що в зоні впевненого прийому радіо їх число було набагато більше, ніж у тих місцях, де сигналу не було. Таким чином, економіст публічно довів уплив радіопропаганди на виникнення різанини між тутсі та хуту.

3. російські ЗМІ – учасники війни проти України.

Міністр оборони росії сергій шойгу, визнаючи результати впливу на громадян своєї країни та розуміючи механізми втілення ідей, ще в 2015 році назвав засоби масової інформації рф «ще одним видом Збройних сил». Пропаганда є не тільки складовою авторитарної, а раніше тоталітарної держави, якою є росія, вона є основою для сучасної російської ідентичності

У росії для підвищення ефективності ведення інформаційної війни проти України було створено окремий Центр інформаційного протиборства (рос. Центры информационного противоборства) – управління у структурі окупаційних військ в Україні.

Структура Центру дає розуміння напрямків, на яких зосереджує свою діяльність ворог:

Відділ інформаційної ізоляції району бойових дій. Забезпечує тотальне домінування російських масмедіа в інформаційному просторі тимчасово окупованих територій України.

Відділ дезінформації і контрпропаганди. Здійснює дискредитацію політичного керівництва та командування Збройних Сил України.

Відділ військово-цивільної взаємодії. Створює негативний імідж сил АТО шляхом звинувачення українських військовослужбовців у скоєнні злочинів та протиправних дій стосовно цивільного населення.

Особливість полягає в тому, що російська державна пропаганда є тотальною, цинічною, брехливою і має прямим попередником радянську пропаганду, але також активно використовує досвід інших історичних авторитарних та тоталітарних режимів. Пропаганда в росії завжди застосовується в тандемі з цензурою: цензура відсікає будь-яке інакомислення, пропаганда змушує думати відповідно до інтересів і цілей владної верхівки. За таких умов станом на 2024 рік говорити про незалежні медіа в росії нема підстав; максимум – їм дозволяється грати роль більш ліберальних.

Основною рисою російської пропаганди є ідеї про множинність варіантів правди, те, що у кожної історії є дві сторони, а надійність джерел несуттєва.

Крім того, російській пропаганді притаманні:

- гнучкість та безпринципність, цинізм;
- постійне вкидання дезінформації в інформаційний простір ЗМІ;
- абсолютна брехливість, невідповідність дійсності та винахід потрібних «фактів» – моделювання та створення так званої «паралельної реальності»;
- одномоментність, ситуативність, протиріччя самій собі, тому, що було повідомлене нещодавно, – розрахунок на повну втрату пам’яті аудиторією;
- мета цього не переконати, як у класичній пропаганді, а зробити інформаційне поле «брудним», щоб ніхто нікому не довіряв. Коли інформаційне поле вбите, все, що залишається, – страхи, паніка та апатія.

Обирається грубий і простий спосіб комунікації з суспільством («Вона потонула», «У сортирі замочимо», «Якби бабуся мала вторинні статеві ознаки дідуся»). У найбільш крайніх проявах – від імені таких «діячів», як журавльов, жириновський та медведєв, а також у дипломатії – груба, зневажлива тональність лаврова, небензі та захарової.

Постійний «пошук ворогів» – українці, кавказці, таджики, євреї, американці – завжди є ворогами, які «заздрять і хочуть захопити», але яких треба зневажати.

Подвійні стандарти. Ключові постаті російського шовінізму можуть бути одночасно нацистами і гомофобами, але при цьому не є «чистокровними» (зі свого ж, нацистського, погляду) етнічними росіянами і геями. Тобто є тим, проти чого самі виступають. Найбільш яскравий приклад таких подвійних стандартів – жириновський. Він, при своєму шовінізмі, антисемітизмі і гомофобії, сам намагався уникати згадок власного єврейського походження і особистого життя. Інші приклади викритих у подібних подвійних стандартах – едуард лимонов, антон красовський, філіп кіркоров, в'ячеслав володін.

Апеляція до чужого досвіду («от в Китаї», «от американці...»). Такими поясненнями можна було обґрунтовувати все, що завгодно.

Апеляція до емоційного мислення замість раціонального. Формування містичного, нераціонального мислення через забобони, конспірологію та релігію (згадайте реклами і передачі про астрологів, ворожок, екстрасенсів. В Україні також намагалися запровадити такі ж програми).

Постійна згадка про чужі проблеми при замовчуванні власних. «А в Америці дискримінація кольорового населення» – популярна позиція радянської пропаганди 70-х років використовується дотепер у росії.

Апеляція до авторитету окремих осіб, які підтримують російську думку, навіть якщо ці люди вже не такі популярні, їхні погляди не є загальноприйнятими (Жерар Депардьє, Олівер Стоун, Такер Карлсон, Роджер Уотерс та інші).

Апеляція до осіб та організацій, що перебувають ніби осторонь конфлікту та над ним. Приклади – Папа Римський, Ілон Маск, ООН тощо. Просування власних суб'єктивних тез під виглядом незалежної точки зору третіх сил

Зайва категоричність, формування чорно-білої картини світу («Чи ви за нас, чи ви фашист», «Сила у правді!»). В інших випадках – навпаки, вкидання величезної кількості версій з метою розмивання розуміння, створення відчуття, що «У кожного своя правда» та «А можливо, все не настільки однозначно?»

Очорнення найбільш послідовних опонентів – Великобританії, поляків і фінів, країн Балтії та України, спроба представити їх як несуб'єктні та несуверенні товариства, які діють не з власної волі, а «за вказівкою із США».

Традиційними для росії є спроби представити себе (і свій суспільний лад з його цілком конкретними недоліками) як жертву обставин непереборної сили. Наприклад:

1). У нас такий рівень життя не тому, що режим злочинний, а тому, що клімат холодний.

2) росіяни завжди крали. Тому це вже така звичка.

3) У нас погані комунікації через низьку щільність населення, а не від дій чи бездіяльність місцевої влади.

4) У нас особливий шлях розвитку, відмінний від західного.

5) Переключення уваги населення із внутрішніх питань на зовнішні. Як результат – пересічний росіянин більше буде обговорювати вигадані проблеми інших країн, ніж недоліки у своєму населеному пункті.

У поєднанні з покараннями і навіть вбивствами незгодних така політика створює тотальне схвалення дій держави. Своєю чергою абсолютна більшість населення росії є прихильниками війни проти України добровільно, не бажаючи застосовувати критичне мислення чи діяти відповідно до загальнолюдських принципів.

Пропаганда / ЗМІ в росії почали масово використовувати «новомову» – описаний Джорджем Орвелом в його антиутопії «1984» спосіб подачі інформації. Це штучне словотворення з підміною реальних понять евфемізмами для пом'якшення сприйняття населенням різних подій, стихійних та воєнних явищ.

Для прикладу, в гітлерівській Німеччині відступи називали «вирівнюванням лінії фронту», термін «концентраційний табір» приховував табори смерті, «евакуацією» називали депортації тощо.

З 2010-х років новомова стала масово застосовуватися в росії. Так, навіть дуже сильні вибухи, зі значною кількістю жертв називають «хлопок» (ляск, плескання). Може використовуватися зі словом «вспышка» (укр. спалах), у той час як щодо інших країн використовують звичайне «взрыв». Інші приклади:

задымление (укр. задимлення) – пожежа, возгорание (запалювання) – велика пожежа;

корректировка цен (укр. коригування цін) – зростання цін;

отрицательный рост (укр. від'ємне зростання) – зниження, погіршення певного показника. Наприклад, рецесія – це «від'ємне зростання економіки».

Такі терміни є наслідком агітаційного підходу, що росія – найкраща, нічого негативного не може статися, а про погане не треба говорити.

На фоні сказаного не дивно, що війну офіційно називають «спеціальною воєнною операцією, СВО». СВО створила ще кілька термінів новомови: «Жест/шаг доброй воли» (укр. жест/крок доброї волі) – відступ окупантів внаслідок поразки. Таку риторику використовували під час відступу з півночі України у квітні 2022, а потім під час відходу з острова Зміїного в червні 2022 року. Згодом були створені інші варіанти: передислокация (укр. передислокація), перегруппировка (укр. перегрупування), отвлекающие мероприятия (укр. заходи для

відвертання уваги). «Крейсер потерял устойчивость и погиб в условиях штормового моря» (укр. крейсер втратив рівновагу і загинув в умовах шторму) – такий офіційний опис затоплення крейсера «Москва» українськими ракетами.

Велика роль впливу на громадську думку інших країн через ЗМІ відводиться з початку війни. Розвідки багатьох країн викривали мережі впливу, які поєднували ЗМІ та ботоферми, які формували позитивну щодо росії та негативну щодо України картинку з масовим застосуванням дезінформації, маніпуляціями тощо. Вони намагаються створити собі образ противаги традиційним медіа, яким створюють образ брехунів.

На початок війни первісними джерелами брехні були Телеканал RT (Russia Today) з багатьма каналами мовлення та охопленням аудиторії близько 700 млн осіб у всьому світі, платформа цифрового мовлення Sputnik News. Russia Beyond the Headlines – онлайн-портал, а також буклет, який поширюється разом із провідними газетами та журналами. У соцмережах постійно створюються нові групи, канали чи сторінки, які діють в рамках загального плану.

Буквально недавно, 17 вересня 2024 року компанія Meta (Facebook, Instagram, WhatsApp і Threads) закрила доступ до усіх своїх платформ російській пропагандистській медіагрупі Russia Today через втручання та спроби вплинути на вибори.

4. Методи журналістських маніпуляцій.

Є багато різних способів маніпулювати читачами. Згадаємо головні з них:

1. Спотворити інформацію за допомогою неповної, односторонньої подачі, т.зв. фрагментарний спосіб поширення: масив інформації подрібнюють на менші масиви, а також коли інформація подається єдиним неопрацьованим потоком, що не дозволяє пересічному індивіду сформувати цілісну картину подій.
2. Відредагувати, додавши власні домисли і коментарі (значна частина спотворень спричиняється індивідуальними психологічними особливостями поширювачів інформації, політичними симпатіями тощо).
3. Інтерпретувати у вигідному світлі.
4. Приховати, акцентуючи увагу на окремих сторонах події, замовчуючи інші, що створює додаткову можливість маніпулювати аудиторією. Це ж стосується порушення балансу, тобто висвітлення позиції однієї сторони.
5. Створити «інформаційний шум», тобто знизити сприйняття фактів за рахунок подачі такої кількості новин, за якої стає неможливим їхнє сортування.
6. Вигадати її, тобто повідомляти відверту брехню (фейк – це сфабрикована інформація, розрахована на те, що читач або глядач навряд чи почне перевіряти факти, цифри, цитати).

7. Оперативно подавати навіть неперевірену інформацію. Тут діє т .зв «закон випередження», що будь-яке перше повідомлення про подію справляє значно сильніший вплив на аудиторію, ніж наступні.
8. Поширювати певний погляд на інформацію як її єдино правильний варіант.
9. Покликатися на недостовірні джерела (ознака – використання загальних фраз типу «відомий спеціаліст із…», або «один із провідних експертів у сфері…», чи «як повідомляють британські/французькі/німецькі ЗМІ…»).
10. Висмикування з контексту. Це спотворює зміст *(Відомий учений сказав, що все, що він каже, не має сенсу, якщо це вирвано з контексту; наступного дня газети вийшли з заголовком: «Вчений заявив, що все, що він каже, не має сенсу»).*
11. Використання «загальновідомих» речей та безсумнівних суджень («Усім відомо, що…», «зрозуміло, що…», «як завжди...»; «як відомо…»);

ІЛЮСТРАЦІЇ

http://mediadriver.online/manipuliatsiyi_ta_propahanda/yak-manipulyuyut-informatsiyeyu/

5. Шляхи протидії ворожим ІПСО.

Сьогодні в Україні немає ЗМІ або іншого джерела інформації, яке б доносило інформацію тотально, до всіх. Українська аудиторія досить розшарована: йдеться про вікові відмінності, про культурні, освітні і навіть ментальні. Для кожної групи відповідно потрібні свої форми подачі інформації. Хтось поважає виважені великі тексти, а для когось вистачає декількох слів зі «смайликами». Для початку повномасштабної фази війни вдалим рішенням був вибір формату щоденного відео від Президента. Але згодом він почав втрачати свою роль, бо не враховував різниці аудиторії та не мав новизни формату.

Розшарування особливо чітко відстежується в соцмережах. Вважається, що Facebook – для тих, хто вміє читати великі тексти, Telegram – для тих, хто читає кілька речень, Instagram – для любителів картинок, а в Tik-Tok текст взагалі є неприйнятним.

Держави у кризових та воєнних умовах повинна дотримуватися певних принципів комунікацій.

1. Узгодження.

Потрібно узгоджувати меседжі та позиції державних відомств та налагодити централізований моніторинг інформаційного простору. Це потрібно для того, щоб адекватно та вчасно реагувати на інформаційні виклики.

2. Дружні стосунки з іноземними журналістами.

Вони допоможуть формувати в їхніх країнах позитивне ставлення до країни та налагоджувати міжнародні комунікації на державному рівні. Маємо більше негативних прикладів, коли журналістів не пускали на місце події, бо не хотіли брати додаткові завдання з їхнього супроводу.

3. Медіаграмотність

Це зона відповідальності кожного громадянина за ту інформацію, яку він допускає в особистий інформаційний простір. Важливо навчитись не реагувати на неперевірену інформацію, на фейки, на емоційні заклики, гучні сенсації.

4. Відповідальність ЗМІ.

Журналісти мають усвідомлювати, яку інформацію вони поширюють, як вона впливає на аудиторію і до яких наслідків може призвести.

5. Захист від кібератак.

Враховуючи руйнівний потенціал кібератак, слід приділяти увагу кіберзахисту у співпраці з НАТО та ЄС і використовувати їхній досвід та технологічні досягнення.

6. Дія на випередження.

Пресслужбам державних органів у кризових ситуаціях варто давати коментарі та роз'яснення рішень на випередження, щоб уникнути інтерпретацій чи домислів у публічних дискусіях. Правдива інформація, подана із затримкою на кілька годин, може охопити менше людей, ніж фейкова новина, подана швидко.

7. Чіткий план для пресслужб.

Державним органам варто створити чіткий план дій для представників пресслужб під час суспільно резонансних подій (інцидентів). А також продумати систему заохочень і покарань (до відсторонення від посади) для тих працівників, які недобросовісно виконують свою роботу.

8. Роз'яснення державної інформаційної політики.

Працівники держорганів повинні оприлюднювати суспільно значущу інформацію (якщо вона не є секретною). Вони мають якомога детальніше роз'яснювати державну інформаційну політику. Особливо це стосується політики щодо тимчасово окупованих територій.

9. Оціночні судження.

Представникам держорганів не рекомендується вживати оцінних суджень та емоційно забарвлених термінів в офіційних інформаційних повідомленнях. А також до рішення суду називати підозрюваних «злочинцями», «шахраями», «вбивцями», тощо.

10. Державні органи у соцмережах.

Державним органам варто ухвалити правила використання офіційних сторінок у соціальних мережах для уникнення непорозумінь та створення фейкових профілів.

Висновки

У сучасних умовах роль медіа в інформаційній війні є надзвичайно значущою. ЗМІ — як традиційні, так і цифрові — формують громадську думку та можуть бути як джерелом правди, так і інструментом маніпуляцій. Тому здатність критично оцінювати інформацію, розпізнавати фейки та протидіяти інформаційно-психологічному впливу є необхідною навичкою кожного громадянина. Медіаграмотність — ключ до розуміння і захисту в інформаційному просторі, а її розвиток — важливий крок до свідомого, відповідального суспільства.

Заняття 6. Роль штучного інтелекту в інформаційній війні

Мета заняття:

- вивчити сфери застосування ШІ у воєнній сфері;
- вивчення можливостей застосування ШІ в роботі з інформаційним полем;
- засвоєння завдань із протистояння використанню ШІ в російських ІПСО.

Вступ

Штучний інтелект (ШІ, англ. AI) – система інтелектуальних технологій, які базуються на комп'ютерних нейронних мережах і здатні виконувати завдання, що зазвичай потребують людського інтелекту. Його діяльність передбачає певний рівень самонавчання на досвіді, розпізнавання закономірностей і ухвалення рішень на основі вхідних даних. Використання ШІ спрощує і прискорює виконання низки завдань, пов'язаних із великим обсягами нетипових матеріалів. Теперішній рівень моделей ШІ останніх поколінь дозволяє аналізувати тексти, зображення чи відео та створювати правдоподібні відповідники статей, малюнків чи роликів на задану тематику.

1. Штучний інтелект у війнах

Є декілька головних напрямків використання нейронних мереж (та ШІ) для військових потреб.

По-перше, у системах управління фінансами і персоналом, а в оборонному секторі – логістика та робота з медичними записами в госпіталях. Для України це важливо при надходженні закордонної військової допомоги. До речі, ШІ спростив задачу розселення українських біженців за кордоном: лише Британію за допомогою ШІ-додатку Homes for Ukraine потрапило близько 100 тисяч наших громадян.

По-друге, ШІ може допомагати в оптимізації розподілу ресурсів, плануванні місій і тактичних операцій. Різновиди ШІ працюють з дуже великими обсягами даних, неструктурованих, неоднорідних, які

дублюють одні одних. Нейронки створюють цілісну картину, на основі якої командування і ухвалюватиме рішення. Про ефективність застосування технології говорить статистика: ще 20 років тому командування могло відстежувати 10 цілей на день, а сьогодні той самий підрозділ може відстежувати 300.

Чинний український аналог системи внесення, обробки та передачі інформації називається Griselda. Її технологія інтегрована зі системою ситуаційної обізнаності Delta, застосунками для артилеристів і танкістів «Броня», «Кропива», «Укроп» та «ГісАрта». Окремо виділимо можливості ШІ у протидії кіберзагрозам, або навпаки – у кібератаках.

По-третє, використання ШІ в динамічних умовах, пов'язаних із бойовими зіткненнями: у системах ведення вогню на полі бою, бойових турелях або в системах наведення БПЛА, ракет і високоточних снарядів. Це важливо, зокрема, в умовах протидії ворожих РЕБ, коли завдання зі знищення цілі виконується навіть без участі людини. При цьому потрібна постійна ідентифікація цілей, яку найкраще здійснює ШІ.

Проводячи семантичний аналіз відкритих публікацій, можемо проаналізувати потреби ворожих підрозділів, їхнє забезпечення і навіть морально-психологічний стан.

А задля захисту нейромережі використовуються в системах ППО та ПРО, які допомагають помітити, розпізнати загрозу, поінформувати людину, яка має ухвалювати рішення, а у випадку екстреної небезпеки в деяких варіантах, припускається, дозволена опція самостійно зреагувати (зліквідувати).

При цьому слід пам'ятати про вразливість самого ШІ перед цільовими апаратними чи програмними атаками.

2. Можливості та загрози нейронних мереж в інформаційній війні

Сучасна війна вже не обходиться від того чи іншого рівня використання ШІ.

Так, серед напрямків інформаційної війни є ті, що вимагають аналізу даних. Так, Компанія Primer Technologies, яка створює системи для аналізу великих наборів даних, в Україні за допомогою ШІ аналізувала перехоплені розмови окупантів. Записи були автоматично транскрибовані, перекладені та проаналізовані за допомогою кількох алгоритмів ШІ, розроблених Primer. Для компанії це стало непоганою PR-кампанією, оскільки на цивільному ринку вона продає алгоритми ШІ, навчені транскрибувати та перекладати телефонні дзвінки.

Центр стратегічних комунікацій та інформаційної безпеки за допомогою ШІ проводить моніторинг медіапростору та аналіз масиву онлайн-публікацій. Інструмент допомагає виявляти інформаційні тренди, відстежувати зміни реагування користувачів соціальних мереж на інформаційні приводи, виявляти мову ненависті тощо. Також можна швидко аналізувати зображення та виявляти шкідливий контент. Серед способів дій – машинне навчання (оцінка тональності повідомлень,

рейтингування джерел, прогнозування розвитку інформаційних динамік), кластерний аналіз (автоматизоване групування текстових повідомлень, виявлення сюжетів, формування сюжетних ланцюжків), комп'ютерна лінгвістика (для виявлення сталих словосполучень та наративів), формування, кластеризація та візуалізація семантичних мереж (для визначення зв'язків та вузлів, розбудови когнітивних мап) та кореляційний і вейвлет аналіз (для виявлення інформаційних операцій).

Це допомагає розрізняти органічне та скоординоване розповсюдження контенту, виявляти автоматизовані системи розповсюдження інформації, оцінювати вплив на аудиторію різних облікових записів користувачів соцмереж, відрізняти ботів від реальних користувачів тощо.

За даними компанії-розробника OpenAI, штучний інтелект для поширення дезінформації щодо подій у світі вже використовують росія, Іран та Китай. Зокрема, росія поширювала коментарі та новини різними мовами на підтримку війни в Україні для соцмереж. Одна із причин частого застосування цих інструментів – їх простота та доступність навіть непідготовленій людині.

На ШІ базується відео- та аудіомонтажу **deepfake**. Вона дозволяє простіше створювати аудіовізуальні підробки (хоч первісно вона була призначена для фільмів). Тобто це не лише заміна обличчя на відео, а й доповнення рухами губами і тілом людини, синхронізування з фальшивою чи реальною аудіодоріжками.

Спецслужби рф мають великий досвід застосування фото- та відеомонтажу для створення фейків. Діпфейк було використано, зокрема, для створення фейкового відеозвернення президента Зеленського про капітуляцію, вкинуте в інфопростір у березні 2022 року. З огляду на низьку якість цього «продукту», оперативну реакцію державних комунікацій, президента, який особисто спростував фейк, і журналістів, це «не зайшло». Відео не досягло своєї мети ні в Україні, ні за кордоном. Наступна спроба – звернення начальника Генштабу Валерія Залужного зі звинуваченням Зеленського в намірах вчинити замах.

Іншим ШІ, що допомагає під час війни, є система розпізнавання облич, розроблена американською компанією ClearView AI. За допомогою неї ідентифікують росіян, що загинули, після чого сповіщають їхнім родинам про смерть. Ця система має доступ до 10 мільярдів фотографій, що розміщені в соціальних мережах. Її почали використовувати на території України ще в березні 2022 року. Також ця технологія частково використовується на пунктах пропуску або блокпостах.

Завдяки можливостям ШІ використовуються такі техніки для дезінформаційних кампаній:

1. Боти, що просувають проросійські наративи.

2. Цільове таргетування – на основі аналізу обсягу всіх даних формувати «інформаційну бульбашку», яка базується на інтересах,

політичних поглядах або інших характеристиках аудиторії. Це підвищує ефективність маніпуляцій та робить їх більш правдоподібними.

3. Фейкові сайти, що маскуються під відомі ресурси. Використовуються медіаресурси з назвами та/або логотипами, подібними до відомих видань. Неуважні користувачі можуть поширювати, вважаючи, що новина з надійного джерела.

4. Діпфейки з українськими військовими.

5. Фейкороби «рідною» мовою. Хоча бувають і проколи, наприклад «Годинниковий Яр» (Часів Яр). Класичні текстові варіанти перекладу російського тексту – «підлога країни», «нема сечі терпіти ці борошна» та інші.

Для боротьби з фейками створені відповідні інструменти для перевірки втручання ШІ (наприклад, голос – Descript's Overdub, відео – Deepware Scanner, контент – Truly Media). Але більшість читачів не буде їх використовувати для кожної новини, яку читають з телефона.

3. Шляхи запобігання негативному впливу ШІ з боку росіян

Сьогодні у світі розробляються різні проєкти ШІ. Водночас відсутні єдині підходи до оцінки ШІ та етичних норм його застосування, а відповідно – відсутність законодавчого регулювання дій цих технологій. Навіть прості варіанти ШІ легко переорієнтувати на продукування шкідливих продуктів, а розвиток ШІ випереджає створення запобіжників від його недоброчесного і зловмисного використання чи формування правил його регулювання. У травні 2024 року законодавці ЄС погодили «Акт про ШІ» – перший у світі комплексний набір правил для цієї технології, проте до кінця залишається незрозумілим, наскільки суворо будуть виконуватися ці правила. Відповідний «Кодекс практики» не буде юридично обов'язковим, коли набуде чинності в кінці 2025 року, проте він стане керівництвом для компаній щодо дотримання правил. Компанія, яка заявляє про відповідність закону, але ігнорує кодекс, може зіткнутися з правовими проблемами. Тобто зараз людство перебуває тільки на початку шляху регулювання використання ШІ.

Небезпека використання машинних текстів у маніпуляціях чи дезінформації полягає у їх правдоподібності. Можна легше і швидше створювати несуперечливі повідомлення, імітувати тексти людей із конкретними поглядами і видавати коментарі, тексти для форумів і пости, які не відрізняються від коментарів інших користувачів. Таким чином ШІ легше входити в довіру, готуючи ґрунт до впливу на свідомість живої людини (нагадаємо, довіра є ключовою і найбільш вразливою особливістю соцмереж).

В одному із варіантів – GPT-3 – повний код доступний лише Microsoft, яка отримала ліцензію. Крім того, навіть для роботи з неповним та відкритим кодом розробники обмежили сферу застосування своєї моделі. Наприклад, правилами компанії заборонено створення додатків із використанням GPT-3, які:

- не повідомляють користувачів, що вони спілкуються з ШІ або текст створений ШІ;
- дозволяють генерувати й публікувати повідомлення в соціальних мережах насамперед у твіттері й інстаграмі; використання заборонено навіть тоді, коли в публікації або написанні повідомлень частково бере участь людина;
- класифікують людей за певними характеристиками (наприклад, расового чи етнічного походження, релігії, політичних поглядів або особистих даних про здоров'я);
- намагаються вплинути на політичні рішення або на думку груп, тобто ті, які допомагають створювати таргетовані інформаційні кампанії;
- витягають захищену особисту інформацію, зокрема дані про фінанси, медичні діагнози й так далі. Також заборонені боти, які пропонують медичні поради або інструменти, призначені для діагностики або лікування будь-яких захворювань;
- створюють і розсилають спам.

Але це тільки одна з багатьох моделей ШІ. Як приклад наведу конспірологічний текст однієї з закритих російських програм ШІ. Саме такого типу фейки поширені в соцмережах. Хоча соцмережі дружно декларують готовність боротися проти появи матеріалів, створених за участі ШІ, але на практиці його не дотримуються.

Інструменти, які дозволяють виявити великі тексти, створені програмою, існують. Наприклад, «Grover» для протидії фейкових генерованих програмою новин. Але він може визначити, що текст створений GPT-2 на 90%; а ось для GPT-3 він визначить, що текст був згенерований лише з точністю 70%. Наступні покоління ШІ поки не розглядалися.

Коментарі розпізнати важко, оскільки вони короткі, не містять багато інформації. Можливо, їх можна буде визначити за допомогою аналізу самої мережі й активності користувачів. Це сфера відповідальності адміністрації соцмережі. Там бачать, чи є занадто висока активність якихось користувачів, чи підозрілі групи таких користувачів, які коментують чи репостять одне одного, якась інша неприродна поведінка. Тобто соцмережі мають інтегрувати механізми, щоб виявляти аномальну активність ботів і таким чином запобігати поширенню брехні й маніпуляцій. Але кожного разу такі тексти стають кращими, а боти – складнішими, тому для протидії потрібно постійно наздоганяти.

Натомість на прикладі застосування ШІ в мережі Facebook бачимо велику кількість помилок, які призводять до періодичного видалення абсолютно мирних / цивільних / нейтральних постів.

Українську розробку протидії фейкам – Mantis Analytics – презентували в Міністерстві цифрової трансформації України. Вона вміє моніторити, аналізувати події та виявляти маніпуляції в інформаційному просторі. Mantis в режимі реального часу обробляє тисячі повідомлень та гігабайти даних зі ЗМІ, соцмереж, інформаційних платформ. Потім

компонує все на інтерактивній карті. Дані допомагають ефективніше протидіяти дезінформації й ворожій пропаганді, бо кожен може бачити, як росіяни поширюють фейки та обмінюються інформацією.

Компанія заявляє про інші можливості програми:

- виявлення в реальному часі скоординованих інформаційних атак і наративних кампаній та протидія їм;
- детальний автоматичний аналіз новин і дописів;
- інтерактивні дашборди зі спеціалізованими інструментами для дослідницького аналізу інфопростору;
- розумне узагальнення за допомогою ШІ (тисячі новин і публікацій подаються в кількох реченнях);
- автоматичне виявлення маркування дезінформації. Вказівки на конкретні маніпулятивні технології, спрямовані на послаблення когнітивної безпеки аудиторії, такі як пропаганда, фейкові новини та інші методи впливу;
- збір та зберігання даних з соціальний мереж, месенджерів, телебачення, радіо та медіа;
- «прогнозування майбутнього», можливо, мається на увазі створення припущень про подальший розвиток дезінформаційної кампанії на основі зібраних даних.

Використання ШІ в інформаційній війні – постійна гонка озброєння: на кращу протидію йде новий рівень нападу, який вимагає ще кращої протидії. І так починається новий раунд протистояння.

Висновки

Штучний інтелект став потужним інструментом в інформаційній війні, здатним як до поширення, так і до протидії дезінформації. Алгоритми ШІ активно використовуються для створення фейкових новин, глибоких фейків (deepfake), генерації пропагандистських матеріалів і маніпуляцій у соціальних мережах. Водночас ШІ допомагає в моніторингу інформаційного простору, виявленні фейків, ботів і координації кібербезпеки. Важливо навчати молодь критичному мисленню та правилам інформаційної безпеки, оскільки лише поєднання людського аналізу й технологій ШІ здатне ефективно протидіяти ІПСО. У майбутньому саме етичне використання ШІ стане визначальним у формуванні безпечного інформаційного середовища.

Заняття 7. Кібербезпека в умовах інформаційної війни

Мета заняття:

- ознайомитись з поняттям кібербезпека та основними засадами кібергігієни.
- дізнатися про можливості кібератак, цілі та завдання кібервоєн.
- вивчити приклади успішних кібератак між країнами.
- ознайомитися з головними подіями історії протистоянь в кіберпросторі України і росії.
- вивчити головні поради для захисту приватних облікових записів від кібершахрайства.

Вступ

Сьогодні людство повністю залежить від інформаційних технологій. Напружені війни проводяться в кіберпросторі як державами, так і окремими групами, що створюєвеликий прибуток для ініціаторів кібератак. Головна умова для нападу – це цілковита анонімність агресора. Для війн такого роду визначальною є технічна перевага, розвиток технологій (де-)шифрування, рівень комп'ютерних спеціалістів. Через кібератаки та боротьбу з їхніми наслідками бізнес щорічно втрачає 400 мільярдів доларів.

1. Кібербезпека людини та державиКібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору. Це стан захищеності систем передавання, опрацювання та зберігання даних, у якому забезпечено конфіденційність, доступність і цілісність даних.

Кіберзахист – це постійний процес захисту даних від знищення, копіювання, зміни, використання; а приладів і систем – від будь-якого стороннього впливу,тому неможливо створити систему, захист якої не можна буде зламати. Головне завдання: створення такого механізму захисту, вартість зламу якого буде дорожчою за інформацію, яку можна отримати.

Цілі кібервійни не відрізняються від цілей традиційних протистоянь: здійснення впливу на об'єкт, зміна поведінки супротивника та встановлення над ним своєї влади. Різниця у методах

Окрім того, кібервійна має свої особливості:

1. Впливає на інформаційні потоки, на техніку, на системи. Вона може спрямовувати, фальсифікувати або перешкоджати потокам інформації для впливу на думку суспільства, державних чиновників або військових.

2. Атаки на критичну інфраструктуру (електроенергетичні мережі, транспортні системи, фінансові установи, зв'язок тощо). Це призводить або до паралізування управління державою, або впливає на життя громадян і може змусити виконувати вимоги агресора.

3. Включає кібершпигунство та кібершантаж. Збір конфіденційної (зокрема, економічної) інформації про супротивника та подальший шантаж.

4. Проведення дестабілізації та психологічного тиску. Суспільство настільки залежне від комп'ютерних інформаційних технологій, що їх порушення створює небезпеку для життя та здоров'я, створює справжній хаос.

Безпосередніми цілями атак зловмисників та ворогів стають:

1. комунікаційні системи, в яких обробляються національні інформаційні ресурси та які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань;
2. об'єкти критичної інформаційної інфраструктури;
3. комунікаційні системи, які використовуються для забезпечення суспільних потреб та реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу (енергетика, зв'язок, залізниця, банківська система тощо).

«Кіберзброя», яка застосовується в атаках – це відповідні інструменти, технології або методи, які використовуються в кіберпросторі для здійснення кібератак, кібервійськових операцій або впливу на інформаційні системи та мережі. Її призначення разом з розвідкою, руйнуваннями, шпигунством, впливати на суспільну думку або завдавати шкоди ворогові.

Прикладами кіберзброї є:

1. Віруси та програми-шпигуни — збір конфіденційної інформації або виконання певних дій на комп'ютері без дозволу користувача.

2. Віруси-троянці ховаються у вигляді корисної програми або файлу і виконують шкідливі дії під час активації.

3. Комп'ютерні черви здатні самостійно розповсюджуватися через комп'ютерні мережі і використовують вразливості у програмному забезпеченні.

4. DDoS-атаки (Distributed Denial of Service) спрямовані на перевантаження вебсерверів або мережевих інфраструктур шляхом надмірного надходження запитів або трафіку.

5. Фішинг — один із видів соціально-інженерної атаки – маскування зловмисника як легальної особи або організації для отримання конфіденційної інформації. Технічний фішинг – маскування комп'ютерної системи якегальної. Згідно з даними дослідження Deloitte, 91% всіх кібератак починається з фішингового листа, а 32% всіх успішних проникнень у системи передбачає використання інструментів фішингу.

6. Кіберзброя на основі штучного інтелекту використовується для виявлення вразливостей, розвідки, аналізу великих даних та розробки нових методів атак.

Всі ці варіанти застосовуються за допомогою соціальної інженерії, щоб знайти вразливу точку. Соціальна інженерія – це спосіб «зламу», в якому використовуються психологічні методи для обману людини.

Очікувані наслідки кібератак:

1. Втрата функціональності об’єкта, зупинка роботи його систем або неправильна робота. Наприклад, зупинка роботи важливих систем керування або призупинення роботи критичних інфраструктурних об’єктів.

2. Знищення, пошкодження чи зміна даних. Це може мати серйозні наслідки для діяльності об’єкта та його здатності виконувати свої функції.

3. Порушення конфіденційності інформації, несанкціонований доступ до секретної інформації об’єкта.

4. Зміна або викривлення інформації, що призводить до помилкових рішень чи спричиняє втрату довіри до об’єкта.

5. Підрив робочих процесів, порушення діяльності об’єкта, зменшення продуктивності або збої в роботі систем та процесів.

6. Психологічний тиск та деморалізація. Кібератаки можуть викликати психологічний тиск на персонал об’єкта, призвести до деморалізації та зниження ефективності роботи.

2. Ефективність кібервтручання в діяльність систем супротивника.

Приклади кібервтручання не завжди стають відомими, оскільки об’єкт атаки намагається не повідомляти про свою вразливість. Але відомими стають деякі особливі факти.

У розпал холодної війни, у червні 1982 року, американський супутник раннього попередження виявив великий вибух у Сибіру. Це був вибух на радянському газопроводі. Причиною цього була несправність системи управління комп’ютером, яку радянські шпигуни викрали у фірми в Канаді. Вони не знали, що спеціалісти ЦРУ втручались у програмне забезпечення і зробили так, що воно через певний інтервал часу перестало працювати, скидало оберти насосу та налаштування клапанів. Це спричинило створення надмірного тиску для з’єднань та зварних швів трубопроводів. Отримані збитки були значними на той час.

У 2008 р. під час проведення операції «Олива» сирійські ППО та радіоелектронна розвідка були заблоковані методами кібервійни.

У 2010 р. спеціально розроблений вірус Stuxnet втрутився в роботу автоматизованої системи, що забезпечувала технологічний ланцюжок атомної промисловості в Ірані. Внаслідок цього центрифуги, на яких збагачувався уран для створення атомної зброї, розігналися до недопустимих швидкостей і зламалися. Це гарантовано призупинило ядерну програму Ірану на декілька років.

У 2012 році співробітники британської MI6 зламали сайт Аль-Каїди і замінили інструкцію з виготовлення саморобної бомби рецептом приготування коксів.

У 2000-их роках Китай проводив низку кібероперацій для промислового шпигунства у США та країнах Європи.

2015 р. у шведському центрі управління польотами цивільної авіації вимкнулися комп’ютери, зокрема диспетчерів. Тоді причиною несправності офіційно був названий потужний сонячний шторм. Проте у

квітні 2016 року ЗМІ повідомили, що насправді шведська влада направила термінові повідомлення до НАТО про потужну кібератаку на інформаційну систему управління польотами разом із застосуванням засобів радіоелектронного придушення радарів з боку російських військових. Також іншою жертвою кібератаки з боку російських спецслужб була інформаційна система енергетичної компанії Vattenfall.

З 2011 року в Північній Кореї із найкращих програмістів набирають групи хакерів, яким надають заробіток і нормальне харчування (для Північної Кореї це розкіш). Ціль їхніх кібератак – криптобіржі у всьому світі; мова про вкрадені мільярди доларів.

Кіберпротистояння є настільки важливим, що країни вже давно вводять відповідні підрозділи до складу своїх армій та/або залучають групи цивільних хакерів.

3. російсько-українська кібервійна.

Під час Революції Гідності було зафіксовано посилення втручання груп нетботів й атаки на телефони лідерів опозиції з метою заблокувати зв'язок з ними, проте це був дуже спрощений рівень.

Під час дочасних Президентських виборів в Україні 2014 фахівцями Ситуаційного центру забезпечення кібербезпеки СБУ було знешкоджено атаки на автоматизовану систему «Вибори». За декілька днів до проведення виборів ця система була повністю виведена з ладу. Завдяки залученню фахівців приватної компанії "Датагруп" роботу системи відновили, але залишили один з виявлених «сюрпризів», попередньо його знешкодивши. І ця пастка для російських спецслужб спрацювала – росіяни повірили даним і подали інформацію про нібито виграш Дмитра Яроша на «президентських перегонах».

У 2015 р. відбулася атака на «Прикарпаттяобленерго». Було вимкнено близько 30 підстанцій у 3 областях, близько 230 тисяч мешканців залишились без світла від однієї до шести годин.

У 2016 році внаслідок атаки на «Київобленерго» було відключено 30 вузлових підстанцій, від яких живилася низка стратегічних об'єктів, понад 80 тисяч споживачів були без електрики протягом однієї-трьох годин.

29 грудня 2016 року, на засіданні РНБО України, Президент України Петро Порошенко заявив, що тільки за останні два місяці в Україні було зафіксовано 2,5 тисяч кібератак.

У 2017 році росія провела масову атаку на різні установи вірусом Petya, який розшифрував і знищував усі дані.

Згодом, після обрання нового Президента, Міністр цифрової трансформації України Михайло Федоров злегковажив питання кібербезпеки і свою думку озвучив привселюдно. Ці слова стали свідченням зміщення фокусу уваги в цифровому просторі України. Напередодні та з початком повномасштабної фази війни Україна зазнала відчутних кіберударів, а інтенсивність тільки зростала, тому довелося не тільки посилювати захист, але й розробляти дії у відповідь.

З того часу успішною масштабною кібердією росії стала атака на оператора зв'язку «Київстар» у грудні 2023 року. Для побутових споживачів вона була відчутною, оскільки поєднувалася із відключеннями електроенергії внаслідок ракетних обстрілів електростанцій. Натомість українці зламували провайдерів і запускали українські трансляції у різних регіонах, блокували банківські системи та органи влади, викрадали та після цього знищували великі обсяги інформації російських установ і компаній.

4. Основні рекомендації для кібергігієни

Індивідуальний захист громадян важливий, оскільки масові проблеми (злами і втрати облікових записів), крім особистих труднощів для жертв атаки, неминуче вплинуть на інформаційне поле держави.

Щоб зменшити ризик стати ціллю шахраїв у соцмережах, кілька порад:

1. Вимкніть передачу геолокації в метаданих фотографій на вашому смартфоні. Під час відправлення фото можуть передаватися й дані про місце зйомки. Це одна з причин, чому також важливо не фотографувати й не розповсюджувати світлини з місця прильотів.
2. Налаштуйте двофакторну аутентифікацію. Завдяки їй зловмисникам буде набагато важче отримати доступ до вашого акаунту.
3. Для конфіденційних розмов доцільно використовувати тільки програми із найвищим рівнем шифрування. Найкраща серед таких — Signal.
4. Обмежте видимість у соцмережах свого номера телефону, персональних даних і профілю, щоб ці дані були доступні лише вашим контактам.
5. Вимкніть автоматичне завантаження файлів, щоб уникнути контакту з потенційно небезпечними програмами.
6. Не передавайте свої дані незнайомим контактам або сумнівним сервісам. Звертайте увагу на повідомлення про підозрілий вхід чи спробу входу з невідомого пристрою.
7. Уникайте переходу за підозрілими посиланнями і не приймайте викликів від незнайомців. Це знизить ризик фішингових атак.
8. Не використовуйте телеграм, вайбер чи фейсбук для авторизації на сторонніх сайтах або сервісах. Це зменшить ризик передачі акаунту зловмисникам.
9. За можливості, користуйтеся вебверсіями месенджерів, оскільки в них легше контролювати доступ до мікрофона, камери, геолокації та телефонної книги.

Дані рекомендації повинні бути дотримані військовослужбовцями вже як обов'язкові до виконання. Це не тільки посилить особисту безпеку, але й безпеку всіх військовослужбовців підрозділу.

Рекомендації на базі CERT-UA з основ кібіергігієни наступні:

1. Використовуйте ліцензійні/легалізовані операційні системи, інші програмні продукти, своєчасно й систематично їх оновлюйте.

2. Користуйтеся антивірусним програмним забезпеченням з технологією евристичного аналізу.

3. Використовуйте програмний міжмережевий екран (брандмауер) та штатні засоби захисту від шкідливого програмного забезпечення.

4. Здійснюйте регулярне резервне копіювання даних, зберігайте резервні копії на зовнішніх носіях інформації (SSD, HDD тощо) та налаштуйте функцію «відновлення системи».

5. Не підключайте флешки та зовнішні диски, не вставляйте CD та DVD тощо у ваш комп'ютер, якщо ви не довіряєте повністю їх джерелу. Існують техніки зламування комп'ютера ще до того, як ви відкриєте файл на флешці і задовго до того, як ваш антивірус його просканує. Якщо пристрій знайшли всередині чи отримали його поштою, чи хтось попросив роздрукувати документ або просто відкрити та перевірити його вміст – пристрій може бути небезпечним.

Відключайте автоматичний запуск змінних носіїв інформації (захист від autorun.inf).

6. Не зберігайте автентифікаційні дані в легкодоступних місцях (наприклад, на робочому столі). Використовуйте для зберігання паролів спеціальні програмні засоби (наприклад, KeePass). Використовуйте стійкі, складні та окремі для кожного акаунту паролі

7. Уникайте використання інтернет-банкінгу, електронних платіжних систем, введення автентифікаційних даних під час доступу до інтернету через загальнодоступні (незахищені) безпроводові мережі (в кафе, барах, аеропортах та інших публічних місцях).

8. Будьте особливо обережними з відкриттям вкладень до електронної пошти від невідомих. Найактуальнішим засобом розсилання шкідливого програмного забезпечення є електронна пошта.

9. Іноді, особливо під тиском часу, буває важко відрізнити шкідливі файли від легітимних. Користуйтеся сервісом VirusTotal для перевірки підозрілих файлів шляхом їх одночасного сканування більш ніж 50 антивірусами; але це теж не виключає того, що файл може бути шкідливим.

10. Під час користування інтернет-ресурсами (інтернет-банкінгом, соціальними мережами, системами обміну повідомленнями, новинами,онлайн-іграми) не відкривайте підозрілі посилання (URL), особливо ті, що вказують на вебсайти, які ви зазвичай не відвідуєте.

11. Будьте уважним до проявів інтернет-шахрайства. Найпоширенішим засобом уведення в оману в мережі "Інтернет" є фішинг. Особливу увагу варто звертати на доменне ім'я інтернет-ресурсу, що запитує автентифікаційні дані, перш ніж натиснути на посилання: зловмисники можуть замаскувати доменне ім'я, щоб воно виглядало знайомим (facelook.com, goooogle.com тощо) або мати вигляд, схожий на справжню.

12. Використовуйте VirusTotal для перевірки підозрілих і скорочених посилань так само, як для сканування файлів.

13. Будьте обережні щодо спливаючих вікон та повідомлень.

14. Під час використання віддаленного доступу необхідно обмежити доступ за допомогою «білого списку» (IP whitelisting).

15. Установіть обмеження кількості введення помилкових логінів/паролів.

Дотримання вимог кібергігієни значно зменшує ризик втрати даних!

Висновки

Кібербезпека є надзвичайно важливою складовою національної безпеки в умовах сучасної інформаційної війни. Основними загрозами в кіберпросторі залишаються атаки на державні ресурси, інфраструктуру, банківську систему, а також поширення фейкової інформації через хакерські зломи. Особиста цифрова гігієна – це перша лінія захисту кожного користувача. Вона включає безпечне користування паролями, перевірку джерел інформації, обачність у використанні пристроїв і програм. Розвиток кіберкультури та освіти з кібербезпеки є запорукою стійкості держави до інформаційно-кібернетичних загроз.

Заняття 8. Розвідка на основі відкритих джерел (OSINT)

Мета заняття:

- ознайомитись з основними засадами OSINT.
- дізнатися можливості розвідки у відкритих джерелах;
- вивчити джерела OSINT та дізнатися сферу застосування результатів розслідувань;
- дізнатися про етичні та правові рамки застосування OSINT.

Вступ

Колишній керівник розвідувального управління Міністерства оборони США (1976-1977) генерал-лейтенант Самуель Вілсон зазначав, що «90% розвідданих приходить із відкритих джерел і лише 10 % – завдяки роботі агентури. Знання про потенціал використання відкритих джерел інформації є важливим як для розвідки, так і для протидії ворожим діям.

1. OSINT та джерела розслідувань.

OSINT (англ. Open source intelligence) – розвідка на основі відкритих джерел. Це концепція, методологія й процес збору, аналізу та

інтерпретації інформації, зберігання цих даних, а далі – використання отриманих військових, політичних, економічних та інших даних без спеціального доступу з відкритих джерел, без порушення законів. Така розвідка використовується для ухвалення рішень у сфері національної оборони та безпеки, фінансової аналітики та правоохоронних органів, журналістських розслідувань тощо.

Основні етапи OSINT

1. Визначення джерел

Перед початком збору визначаються релевантні відкриті джерела для конкретного завдання. Потенційні джерела можуть включати:

- інтернет-сайти: форуми, блоги, новинні портали, інформаційні агрегатори;
- соціальні мережі: Facebook, Instagram, X (Twitter), LinkedIn, TikTok, YouTube, російські ресурси vk, «однокласніки», livejournal та інші;
- державні та урядові публікації: звіти, законодавчі акти, реєстри компаній;
- медіа та новинні джерела: традиційні ЗМІ, такі як радіо, телебачення та онлайн-ресурси. Йде відстеження публікацій, а також – поведінкових моделей і зв'язків користувачів. Онлайн-медіа використовуються для відстеження подій у реальному часі;
- «сіра» література: патенти, технічні звіти;
- спостереження: радіо, аерофотозйомки;
- комерційні дані: зображення, фінансові та промислові оцінки, бази даних;
- моніторинг заяв офіційних осіб;
- наукові статті та аналітичні звіти.

2. Збір інформації

На цьому етапі відбувається безпосередній пошук інформації. Методи можуть варіюватися від простого використання пошукових систем до складних технік збору даних:

- пошукові системи: Google та інші (залежно від обраного пошуковика результати можуть відрізнятися) або із застосуванням спеціальних запитів (наприклад, Google Dorks для пошуку специфічної інформації);
- інструменти для автоматичного збору даних: програми для вебскрейпінгу;
- соціальні мережі: пошук публікацій, профілів та зібраної інформації з мережевих платформ;
- спеціальні бази даних та каталоги: пошук у спеціалізованих базах даних, таких як реєстри компаній або наукові бібліотеки.

Для пошуку застосовуються як загальноприйняті, так і спеціалізовані інструменти (Shodan, пошук уразливих інтернет-пристроїв, Maltego, аналіз взаємозв'язків між цифровими артефактами (IP-адреси, домени), TheHarvester, пошук електронних адрес і метаданих про

домени, SpiderFoot, автоматизований пошук інформації про безпеку, пошук витоків і вразливостей).

3. Аналіз та фільтрація даних

Після збору великого обсягу інформації виникає потреба її структурувати і проаналізувати:

- фільтрація шуму: вилучення нерелевантної або дубльованої інформації;
- класифікація даних: організація зібраної інформації за категоріями або типами;
- верифікація джерел: перевірка надійності та достовірності джерел, особливо якщо йдеться про конфліктну або чутливу інформацію;
- аналіз тенденцій: пошук закономірностей, зв'язків або змін у зібраних даних.

4. Інтерпретація та використання інформації

На основі зібраних і проаналізованих даних формується звіт або інший результат, який може бути використаний для:

- прийняття рішень: підтримка урядових, корпоративних або особистих рішень;
- створення прогнозів: аналіз трендів та передбачення майбутніх подій або змін;
- оцінки ризиків: виявлення можливих загроз або вразливих місць.

Сфери застосування OSINT:

1. Національна та військова розвідка:
   - виявлення потенційних загроз через моніторинг соціальних мереж;
   - спостереження за військовими об'єктами та пересуванням військ за допомогою відкритих джерел;
   - OSINT використовується і доповнює такі види розвідки як агентурна розвідка, радіоелектронна розвідка, геопросторова розвідка, аеророзвідка тощо.
2. Кібербезпека:
   - виявлення кіберзагроз та вразливостей у мережах;
   - моніторинг підпільних форумів для виявлення атак або зламів.
3. Бізнес-розвідка:
   - аналіз діяльності конкурентів, фінансових звітів, бізнес-партнерів;
   - оцінка нових ринкових можливостей, тенденцій та споживчих настроїв.
4. Журналістика та розслідування:
   - перевірка інформації та розслідування міжнародних подій;
   - використання супутникових зображень для відстеження руйнувань чи незаконних дій;
   - виявлення прихованих зв'язків між людьми, подіями, організаціями чи комерційними фірмами.

5. Правоохоронні органи:
   - моніторинг діяльності кримінальних угруповань та підозрілих осіб;
   - виявлення фінансових злочинів через аналіз транзакцій у відкритих базах даних.

2. Етичні та правові аспекти OSINT

Законність:

OSINT обмежується використанням тільки тих джерел, які є відкритими і доступними без порушення закону. Використання закритих або приватних даних без згоди є незаконним і карається.

Конфіденційність:

Розвідка з відкритих джерел не повинна порушувати права на приватність осіб. Зокрема, збір особистих даних без згоди суб'єкта може порушувати етичні та правові норми. Результати розслідування не мають бути поширеними (мова не йде про публічних осіб).

Первинна інформація з відкритих джерел після її аналітико-синтетичної обробки може стати цінними знаннями, які зі свого боку статають секретними, якщо не належать до категорії інформації, яка не може бути державною таємницею

Етичність:

Важливо вживати заходів для запобігання неправомірному використанню зібраної інформації, а також уникати маніпуляції даними для дискредитації або шантажу. Таким чином розслідувач, який зібрав інформацію, є відповідальним за її збереження.

Переваги OSINT

Широка доступність: дані можуть бути отримані з публічно доступних джерел.

Низькі витрати: на відміну від закритої або спеціалізованої розвідки, OSINT зазвичай не вимагає великих фінансових ресурсів.

Доступність особистої інформації: сучасні реалії такі, що тим, хто хоче дізнатися якнайбільше інформації, її вже не треба збирати у різних матеріальних джерелах. Люди самі пишуть на себе досьє у соціальних мережах, коментарями під постами друзів і т.д. Розвіднику чи розслідувачу потрібно лише проаналізувати весь той обсяг інформації, який йому дають і структурувати її.

Найголовніша перевага розслідувань – підвищення рівня прозорості суспільства, підзвітності державних структур.

Висновки

OSINT є важливим інструментом для збору даних і аналізу інформації в багатьох сферах. Він надає можливості для глибокого розуміння ситуацій та прийняття обґрунтованих рішень на основі доступної інформації. Проте важливо дотримуватися етичних і правових норм під час збору і використання даних.

Заняття 9. Цілі та завдання OSINT. Інструменти та методи OSINT

Мета заняття:

- перейти до більш практичних кроків у вивченні OSINT і спробувати застосувати окремі інструменти розслідувань;
- на практиці засвоїти окремі методи OSINT;
- приклади резонансних розслідувань.

Вступ

OSINT (розвідка з відкритих джерел) став потужним інструментом для журналістів-розслідувачів, громадських активістів та аналітиків, дозволяючи виявляти важливу інформацію без доступу до закритих джерел. Ось кілька відомих і резонансних прикладів OSINT-розслідувань, які привернули увагу усього світу.

1. Приклади резонансних розслідувань

«Панамські документи».

На початку 2016 року було оприлюднено витік понад 11,5 мільйонів (орієнтовно 2,6 терабайта даних) фінансових та юридичних документів юридичної фірми «Mossack Fonseca» в Панамі. Ці документи були проаналізовані за допомогою інструментарію OSINT, що дозволило викрити систему приховування доходів, отриманих різними шляхами за допомогою таємних офшорних рахунків. Загалом, цей витік повідомив про понад 214 000 податкових гаваней, до яких були залучені високопоставлені урядовці та юридичні особи з 200 різних країн.

Початкове розслідування зайняло понад рік аналізу. Перші матеріали були опубліковані 3 квітня 2016 року. З моменту оприлюднення витоку минуло понад 8 років. Але розслідування та журналістські репортажі все ще тривають і повідомляють нові дані.

Серед викритих, завдяки панамським документам злочинних і таємних шляхів, цікавим є віолончеліст Сергій Ролдугін – найкращий друг путіна, який, як виявилося, перебуває в центрі схеми приховування коштів із російських державних банків на офшорних рахунках. І цей грошовий слід опосередковано веде назад до російського президента.

До речі, одним із важливих завдань у ході даного розслідування було оцифрування та збереження такого об’єму даних. Усі дані зберігалися в кімнаті з обмеженим доступом до комп’ютерів, які ніколи не були підключені до інтернету. Це допомогло гарантувати, що саботувати роботу буде важче, а дані будуть у безпеці.

Застосовані методи OSINT:

Аналіз відкритих баз даних. Журналісти використовували відкриті реєстри компаній, судові записи та інші публічні бази даних для підтвердження власників офшорних компаній.

Аналіз соціальних мереж та медіа:

- аналіз публікацій у соцмережах і ЗМІ дозволив пов'язати компанії та рахунки з конкретними особами;
- фотографії, публічні виступи та новини використовувалися для виявлення підозрілих транзакцій або бізнес-відносин.

Перевірка даних за допомогою геолокації та супутникових зображень. Використання супутникових знімків для ідентифікації офісів і нерухомості, пов'язаної з офшорними компаніями.

Розслідування отруєння Сергія Скрипаля (Bellingcat)

У 2018 році колишнього російського шпигуна Сергія Скрипаля та його дочку Юлію отруїли в Солсбері, Велика Британія. Група журналістів-розслідувачів Bellingcat за допомогою OSINT-інструментів з'ясувала справжні імена російських агентів, які здійснили замах.

Застосовані методи OSINT:

- використання відкритих баз даних для пошуку паспортних даних підозрюваних;
- аналіз фотографій і відео з камер спостереження;
- порівняння біографічних даних підозрюваних із загальнодоступними військовими записами та соціальними мережами.

Це розслідування допомогло встановити причетність агентів ГРУ до операції, а також підтвердити використання хімічної зброї (нервово-паралітична отруйна речовина «Новічок»).

MH17: збиття малайзійського Boeing (Bellingcat)

Катастрофа літака рейсу MH17 влітку 2014 року над територією України стала однією з найбільших трагедій. Команда Bellingcat провела тривале незалежне розслідування, використовуючи OSINT, щоб довести, що літак був збитий російським ЗРК «Бук», який було доставлено з території росії.

Застосовані методи OSINT:

- аналіз супутникових зображень та відео, завантажених на YouTube і в соціальні мережі;
- відстеження руху ЗРК «Бук» через фотографії в соціальних мережах;
- перевірка геолокації зображень та відео за допомогою Google Earth.

Ці дані допомогли скласти маршрут пересування «Бука» з росії до місця запуску ракети, яка збила літак.

Розслідування хімічних атак у Сирії (Bellingcat, The New York Times)

Протягом війни в Сирії було кілька хімічних атак, в яких звинувачували уряд Башара Асада. Bellingcat і журналісти із The New York Times використовували OSINT для підтвердження фактів цих атак, включно з атакою у Думі у 2018 році.

Застосовані методи OSINT:

- аналіз відео з місця подій, опублікованих місцевими жителями;
- порівняння супутникових знімків до і після атак;
- визначення типів зброї і боєприпасів за фото та відео.

Це розслідування допомогло встановити, що в атаці використовувалася хімічна зброя, попри офіційні заперечення уряду Сирії та росії.

Розслідування російських приватних військових компаній (Bellingcat, The Insider)

Одним з відомих розслідувань стало вивчення діяльності російської приватної військової компанії «Вагнер», яка активно діє у багатьох країнах, включно з Сирією, Україною та країнами Африки.

Застосовані методи OSINT:

- аналіз соціальних мереж найманців та публікацій із зон бойових дій;
- вивчення реєстрів компаній і публічних контрактів;
- супутникові знімки місць розташування баз і пересування бойовиків.

Це розслідування дало змогу краще зрозуміти, як працюють російські приватні військові компанії та їхній вплив на міжнародні конфлікти. Також допомогло усвідомити сферу інтересів росії.

Розслідування у справі Ісламської Держави (ISIS, українська абревіатура ІДІЛ)

Група журналістів та розслідувачів використовувала OSINT для моніторингу діяльності терористичної організації ISIS. Вони відстежували активність бойовиків через соцмережі, аналізували відео з пропагандою та координували роботу з місцевими журналістами.

Застосовані методи OSINT:

- вивчення пропагандистських відео та фото для визначення локацій;
- моніторинг облікових записів у соціальних мережах;
- аналіз супутникових зображень для ідентифікації тренувальних таборів і баз.

Завдяки цьому вдалося зібрати дані про мережу бойовиків і місця їхньої активності.

Отруєння Олексія Навального та роль OSINT у розслідуванні

Отруєння Олексія Навального стало однією з найбільш резонансних політичних подій у 2020 році. Хоча для України він

відігравав більше негативну роль, проте Захід в ньому вбачав опозиційного політика, надію на зміни в росії. Його було отруєно нервово-паралітичною речовиною з групи «Новічок» у серпні 2020 року. Група розслідувачів з **Bellingcat**, у співпраці з іншими медіа, включно з **The Insider**, **CNN**, та **Der Spiegel**, за допомогою OSINT змогла розкрити деталі цієї операції і встановити причетність російських спецслужб.

Ключові моменти розслідування OSINT:

1. *Аналіз даних про переміщення підозрюваних:*
    - Використовуючи **дані з телефонів і бази авіарейсів**, журналісти ідентифікували групу співробітників ФСБ, які слідували за Навальним протягом кількох років. Ці особи подорожували з ним під час поїздок росією, зокрема до міста Томськ, де сталося отруєння.
    - Інформація про бронювання авіаквитків і телефонні дзвінки, зібрана через витоки баз даних, була проаналізована для виявлення узгоджених маршрутів співробітників ФСБ.
2. *Використання відкритих баз даних:*
    - За допомогою відкритих російських баз даних, таких як реєстри власності і телефонні книги, розслідувачі змогли підтвердити особи співробітників ФСБ, які діяли під вигаданими іменами.
    - Ці дані дозволили встановити зв'язок між підозрюваними і науковими установами, які займаються дослідженням нервово-паралітичних речовин.
3. *Телефонні розмови та дзвінки:*
    - Завдяки OSINT-аналітиці та зібраним телефонним записам вдалося встановити зв’язки між окремими особами, які брали участь в отруєнні. Розслідувачі отримали інформацію про контакти між виконавцями та їх керівниками у ФСБ.
4. *Супутникові дані і геолокація:*
    - **Геолокація** фотографій і відеоматеріалів, зібраних із соціальних мереж і джерел на місці подій, допомогла реконструювати події до і після отруєння. Це також підтвердило присутність оперативників у Томську, де Навальний зазнав атаки.
5. *Пряма конфронтація та зізнання одного з агентів:*
    - У грудні 2020 року Навальний здійснив розмову з одним із підозрюваних співробітників ФСБ, який під час телефонного дзвінка визнав деталі отруєння. Цей дзвінок був записаний і опублікований, що стало ключовим доказом у справі.

Основні результати:

Розслідування встановило, що за отруєнням стоїть спеціальна група з **ФСБ**, яка працювала над операцією протягом кількох років. Це розслідування показало, як OSINT-методи можуть бути використані для ідентифікації не тільки виконавців злочину, а й державних структур, які стояли за цим.

Також відомо, що OSINT-методи використала команда Дональда Трампа для перемоги у виборах 2016 року. Через опитувальники у Facebook вони зібрали дані про інтереси жителів США і змогли таргетувати рекламні банери на мікрогрупи, виходячи з інтересів добре дослідженої аудиторії.

2. OSINT в російсько-українській війні, як частина захисту держави.

Війна росії проти України привернула увагу багатьох OSINT-аналітиків, які використовували відкриті джерела для документування воєнних злочинів, виявлення пересування російських військ, перевірки ворожої пропаганди.

Інструменти OSINT у воєнних питаннях мають свої особливості:

- використання супутникових знімків для моніторингу військової активності (наприклад, Maxar, Planet Labs);
- геолокація фотографій та відео, опублікованих солдатами і місцевими жителями у соцмережах;
- Геолокація, метадані, вивчення пейзажу, техніки та інших деталей фотографій та відео з поля бою можуть дати уявлення про місце, час і обставини події;
- мобільні додатки. Відкриті дані з додатків, як-от Flightradar24 (для відстеження літаків) або MarineTraffic (для відстеження суден), можуть надавати важливу інформацію про переміщення військових об’єктів або вантажів;
- вивчення залишків зброї, яка використовується у бойових діях, для ідентифікації її походження;
- вивчення фотографій зброї та боєприпасів для ідентифікації їх походження;
- ЗМІ та блоги, аналітичні матеріали або новини можуть містити корисну інформацію щодо тактики та дій ворога. Цінними є матеріали в коментарях так званих «воєнкорів»;
- форуми та закриті групи: моніторинг дискусій на закритих платформах, де учасники обговорюють бойові дії, може допомогти розкрити плани або логістику супротивника.

OSINT також допоміг виявити і підтвердити численні воєнні злочини, включно з бомбардуванням цивільних об’єктів і масовими похованнями.

Українські проєкти, засновані на OSINT:

InformNapalm: Це українська волонтерська розвідувальна спільнота, яка спеціалізується на аналізі даних з відкритих джерел. Вона з 2014 року займається виявленням і доведенням російської військової присутності в Україні та в інших конфліктах. InformNapalm оприлюднює докази використання російської техніки та військовослужбовців в Україні.

Bellingcat: Міжнародна група розслідувачів, що використовує OSINT для аналізу конфліктів та воєнних злочинів. Хоча Bellingcat не є українською організацією, їхні аналітики активно досліджують російсько-український конфлікт, виявляючи факти агресії та воєнні злочини РФ.

Миротворець: Український проєкт, який займається збором і публікацією даних про осіб, які причетні до сепаратизму та терористичної діяльності на території України. Частково використовує OSINT для верифікації отриманих даних.

WarSpotting та DeepState: Онлайн-платформи, які займаються відстеженням та аналізом перебігу війни в реальному часі, використовуючи супутникові знімки, відео з полів бою та інші відкриті джерела.

Також можна назвати OsintFlow (громадська організація з головною місією збору інформації про воєнні злочини росії вчинені на території України), OSINT Бджоли (встановлюють не тільки воєнних злочинців, але також і колаборантів), Molfar (професійні осінтери, які займаються також і комерційними розслідуваннями), Tokar.

Центр «Миротворець».

У своїй діяльності OSINT-групи намагаються встановлювати дані ключових військових злочинців – представників вищого командування, льотчиків та моряків (тих, хто завдає ракетних ударів по містах) тощо. Також шукають повну інформацію про військовослужбовців, які причетні до конкретних злочинів проти мирного населення. Не оминають увагою пропагандистів, колаборантів і членів їх сімей та додаткову увагу звертають на їхнє майно.

Зібрана інформація вже зараз використовується правоохоронними органами, а після перемоги її буде залучено для пошуку та покарання винуватців у міжнародному суді.

Що ж стосується поточних завдань воєнного типу, то розслідувачі встановлюють місця дислокації ворога для їх знищення. За тією ж методикою вони ідентифікують точні координати місцевості та передають інформацію для роботи артилерією чи ударними дронами. Також займаються висвітленням російських фейків та воєнних злочинів, вчинених окупантами.

Серед важливих прикладів роботи українських OSINT-спільнот є розбір на півтори тисячі російських солдатів, які були причетними до звірств у Бучі. На них усіх були зібрані дані й опубліковані.

Також українські розслідувачі ведуть базу російських та підконтрольних росії світових пропагандистів. Це дає змогу оперативно спростовувати їхні фейки.

3. Інструменти поглибленого OSINT

Дані з усіх OSINT-джерел можна збирати й аналізувати вручну, без будь-якого додаткового програмного забезпечення,щоб зробити цей

процес швидшим і простішим, можна завантажити доступні для всіх потрібні програми.

Більшість інструментів OSINT доступна навіть у зовнішній мережі,зокрема на GitHub. Однак деякі з них, особливо ті, які призначені для глибокого аналізу, можна знайти лише в Darknet. Деякі спеціальні інструменти, призначені для дій, які можна легко класифікувати як шпигунське ПЗ, виставляються на продаж на форумах Darknet або торгових платформах.

Тобто ще раз: немає нічого поганого в перевірці наявної інформації без будь-яких злих намірів. Але пошук із благородною метою може легко перетворитися на зловмисний. Азарт може завести людину занадто далеко, щоб отримати інформацію. Пошук в інтернеті – це нормально, а фішингова кампанію, щоб отримати інформацію від співробітників – це кримінальне правопорушення.

Основні інструменти пошуку за відкритими джерелами є інструменти для:

- збору інформації;
- аналізу та візуалізації (особливо корисно, якщо йде повноцінне розслідування, із представленням результатів);
- моніторингу появи нової інформації де-небудь (корисно, якщо ви використовуєте соцмережі для розвідки, а ціль активно їх веде);
- аналізу сайтів та пошук вразливостей на серверах (це питання пов’язане із недотриманням об’єктом розслідування вимог кібербезпеки).

Висновки

OSINT є важливою складовою сучасної інформаційної діяльності, що дозволяє отримувати цінну інформацію без порушення закону. Основними цілями OSINT є збір, аналіз та перевірка інформації з доступних джерел для отримання точного та об'єктивного уявлення про події, об'єкти чи осіб. Завдання OSINT охоплюють моніторинг соціальних мереж, аналіз ЗМІ, роботу з геолокацією, верифікацію фото та відео, пошук за зображеннями тощо. OSINT-розслідування стали потужним інструментом у боротьбі з дезінформацією, розвінчанні пропаганди та викритті воєнних злочинів, особливо під час війни в Україні. Володіння навичками OSINT розвиває аналітичне та критичне мислення, формує новий рівень інформаційної грамотності та є надзвичайно корисним у сфері безпеки, журналістики й громадянської активності.

Заняття 10: Верифікація джерел. візуальний аналіз

Мета заняття:

- Ознайомити ліцеїстів із принципами верифікації джерел інформації.

- Навчити ліцеїстів основам візуального аналізу зображень для перевірки достовірності.

Навчальні і виховні цілі:

- Зрозуміти, що таке верифікація джерел.
- Розвинути навички аналізу зображень для виявлення маніпуляцій або фальсифікацій.
- Розібратися, як використовувати різні інструменти для перевірки достовірності візуальних матеріалів.

Вступ

Сьогоднішнє цифрове середовище сповнене чуток та недостовірних матеріалів, що змушує журналістів активно відсортовувати правдиву, справжню інформацію від брехні. Верифікація – процедура перевірки, доказ того, що твердження є істинним, тобто перевірка сказаного (написаного, озвученого) на правдивість. Достовірна інформація може стати рятівною під час гуманітарних криз.

1. Що таке верифікація джерел?

Верифікація джерел — це процес перевірки достовірності інформації, яка походить із певного джерела. Важливо розуміти, що не вся інформація в інтернеті є правдивою. Основна мета верифікації — з'ясувати, чи можна довіряти отриманій інформації, чи це спроба маніпуляції або дезінформації.

Основні принципи верифікації джерел:

Авторитет джерела: перевірте, чи є джерело надійним. Авторитетні джерела зазвичай пов'язані з державними або міжнародними організаціями, науковими установами чи відомими медіа, які мають добру репутацію.

Автор публікації: хто написав статтю або надав інформацію? Досвід і репутація автора відіграють ключову роль. Якщо інформація анонімна або походить від незнайомої особи, варто бути обережним.

Актуальність інформації: чи є інформація новою або відображає сучасні реалії? Перевірте дату публікації та з'ясуйте, чи є матеріал релевантним.

Крос-перевірка інформації: порівняйте дані з іншими джерелами. Якщо кілька незалежних авторитетних джерел підтверджують одні й ті ж факти, це збільшує їхню достовірність.

Прозорість джерела: чи вказані джерела первинної інформації у статті? Наукові та журналістські публікації повинні посилатися на конкретні дослідження, експертів або документи.

Типи джерел інформації:

Первинні джерела: це оригінальні документи або дані, отримані безпосередньо від першоджерела. Наприклад, наукові дослідження, офіційні документи, звіти.

Вторинні джерела: це інтерпретація або аналіз первинних джерел. Статті в медіа або аналітичні огляди.

Третинні джерела: це ресурси, що систематизують інформацію з різних джерел, наприклад, енциклопедії, довідники та оглядові роботи.

Доступно багато різних інструментів для перевірки фактів та їх верифікації:

Google Scholar: для пошуку наукових статей.

Snopes.com: для перевірки фейкових новин.

FactCheck.org: для перевірки політичної інформації.

StopFake.org: українська платформа для виявлення фейкових новин.

Фактчекери в Україні – це професійні журналісти або експерти, які займаються перевіркою достовірності інформації, що поширюється в медіа, соціальних мережах та інших джерелах. Їхня основна мета – виявляти фейки, маніпуляції, дезінформацію та неточності, а також допомагати суспільству розрізняти правду і брехню. Фактчекери аналізують публікації, офіційні заяви, новини та інші інформаційні матеріали для перевірки їхньої правдивості на основі відкритих даних, офіційних документів та інших джерел.

В Україні є кілька ключових фактчекінгових організацій та платформ:

1. StopFake

Один з найвідоміших українських фактчекінгових проєктів, заснований у 2014 році. Його мета – боротьба з дезінформацією, особливо в контексті російської пропаганди під час війни в Україні.

Діяльність: StopFake перевіряє новини, фото- та відеоматеріали, спростовує фейки та пояснює, як відрізняти правдиву інформацію від фальшивої. Вони регулярно публікують аналітичні статті про фейки у ЗМІ та соцмережах.

Сайт: www.stopfake.org/uk/golovna/

2. VoxCheck

Проєкт аналітичної платформи VoxUkraine, заснований у 2015 році, спеціалізується на перевірці публічних заяв політиків, економічних та соціальних новин. Це одна з найвідоміших платформ в Україні, що займається фактчекінгом.

Діяльність: VoxCheck аналізує публічні заяви політиків та важливі соціально-економічні новини, перевіряє їх на правдивість та публікує звіти з рейтингом «правда», «брехня», «маніпуляція» тощо. Особливо корисний ресурс під час виборчих кампаній, коли фейкові новини часто використовуються для маніпуляції громадською думкою.

Сайт: voxukraine.org/voxcheck

3. БезБрехні

Фактчекінговий проєкт, що зосереджується на перевірці новин та заяв, які поширюються в українському інформаційному просторі. Його мета – спростовувати фейки та маніпуляції в медіа.

Діяльність: Проєкт «БезБрехні» аналізує новини, соціальні мережі та інші джерела, перевіряючи інформацію на достовірність. Вони також навчають громадян критичному мисленню та тому, як самостійно перевіряти інформацію.

Сайт: https://without-lie.info/

Крім того, є просвітницькі ресурси, які вчать більш прискіпливо ставитися до інформації в Інтернеті.

Нота Єнота https://www.facebook.com/notaenota1

Інститут масової інформації (IMI) Сайт: imi.org.ua

Роль фактчекерів у суспільстві:

Фактчекери допомагають:

- захистити громадськість від дезінформації;
- підтримувати прозорість та відповідальність політичних діячів;
- розвивати критичне мислення та медіаграмотність серед громадян;
- спрощувати доступ до правдивої інформації, особливо під час кризових подій, таких як війни, епідемії чи виборчі кампанії.

Фактчекери в Україні відіграють важливу роль в інформаційному полі, допомагаючи суспільству краще орієнтуватися в потоці інформації, зберігати довіру до медіа та не впадати в емоційні гойдалки.

2. Аналіз зображень і відео

У сучасному світі зображення та відео можуть бути використані як засоби маніпуляції, фейків або пропаганди. Здатність аналізувати візуальні матеріали та визначати їхню достовірність є важливим елементом верифікації інформації.

Ключові методи візуального аналізу:

Аналіз метаданих (EXIF):

Метадані (EXIF-дані) – це технічна інформація, яка зберігається в цифрових файлах (зображення, відео) і містить такі дані, як дата та час створення, тип пристрою (камери), налаштування об’єктива, локація (GPS).

За допомогою метаданих можна виявити, чи не змінювалась дата створення або чи відповідає місце зйомки заявленій інформації.

Інструменти: ExifTool, Metapicz.

Пошук зображень у зворотному напрямку:

За допомогою Google Images чи TinEye можна завантажити зображення або вставити покликання на нього та отримати результати з

інших сайтів, де це зображення використовувалось раніше. Це дозволяє виявити, чи є воно оригінальним, або чи було взяте з інших ресурсів (наприклад, зі старої новини або підробленого джерела).

Інструменти: Google Images, TinEye.

Аналіз пікселів та редагувань:

Сучасні зображення часто редагуються для маніпуляції. За допомогою аналізу пікселів можна виявити сліди фотошопу або інших інструментів редагування. Відмінності у текстурах, кольорах, освітленні чи тінях можуть вказувати на підробку.

Інструменти: FotoForensics, JPEGsnoop.

Контекст зображення та відео:

Аналізуйте, чи відповідає контекст зображення заявленим фактам. Наприклад, якщо зображення чи відео заявляють як доказ певної події, важливо перевірити, чи дійсно воно відображає цю подію, чи зняте в іншому місці та в інший час.

Зверніть увагу на деталі: чи відповідають погодні умови, архітектурні елементи, стилі одягу людям, яких зображено, певному часу і місцю.

Інструменти для аналізу зображень:

FotoForensics: дозволяє аналізувати можливі редагування зображення на основі аналізу пікселів і виявлення аномалій.

Google Images та TinEye: для пошуку походження зображення та перевірки, чи використовувалось воно раніше.

InVID: інструмент для перевірки автентичності відео та пошуку його початкового джерела.

Ризики та типові помилки під час верифікації та візуального аналізу:

Фейкові джерела: деякі сайти імітують вигляд авторитетних ресурсів, але є джерелами дезінформації.

Редаговані зображення: навіть невеликі зміни в зображеннях можуть сильно змінити їхній контекст. Будьте пильними до деталей.

Емоційний контент: дезінформація часто намагається викликати емоційну реакцію, відволікаючи від критичного аналізу інформації.

Висновки

OSINT є частиною загальної стратегії захисту України, важливим елементом загальної системи інформаційної та військової безпеки України. Використання відкритих даних дозволяє зменшити залежність від закритих джерел розвідки та сприяє швидшому прийняттю рішень. Інформація, отримана через OSINT, допомагає військовим, урядовим структурам, міжнародним організаціям і громадськості ефективно реагувати на загрози.

OSINT також відіграє важливу роль у боротьбі за інформаційний простір, допомагаючи Україні протистояти пропагандистським атакам і забезпечувати міжнародну підтримку на основі перевірених фактів.

Заняття 11. Особливості професій, пов'язаних із сучасними цифровими технологіями. Військові професії та перспективи

Мета заняття:

- ознайомити учнів з особливостями професій, пов'язаних із сучасними цифровими технологіями, розкрити специфіку військових професій у цифрову епоху та окреслити перспективи кар'єрного розвитку в цій галузі;
- сприяти формуванню усвідомленого вибору професійного шляху та розумінню важливості цифрової грамотності у військовій справі.

Вступ

Сучасні військові професії відображають складність і технологічний прогрес, що характерний для XXI століття. Традиційні ролі (піхота, артилерія, танкісти) доповнюються новими спеціальностями, які використовують цифрові та інформаційні технології, що дозволяє значно покращити ефективність ведення бойових дій і керування військовими ресурсами.

1. Особливості професій, пов'язаних із цифровими технологіями

Війни усе частіше переходять у цифровий формат, де ключову роль відіграє інформація та її управління. Тому зростає потреба у спеціалістах, які працюють із даними, кіберпростором і цифровими системами.

Кіберспеціалісти

Однією з ключових сучасних військових професій є кіберфахівці, які займаються як обороною, так і наступом у кіберпросторі.

Основні завдання: захист критичної інфраструктури від кібератак, виявлення вразливостей у власних системах, впровадження нових засобів кібербезпеки.

Наступальні операції: кіберспеціалісти можуть здійснювати хакерські атаки на інфраструктуру ворога, зламувати бази даних, виводити з ладу системи управління.

Фахівці з інформаційних систем і технологій

Військові фахівці з інформаційних систем відповідають за розробку, впровадження та експлуатацію технологічних рішень, що допомагають військам на полі бою та в стратегічному управлінні.

Основні завдання: керування комп'ютерними мережами, базами даних і системами управління боєм, інтеграція нових цифрових рішень.

Технології: застосування штучного інтелекту для обробки великих масивів даних, автоматизація процесів командування.

Фахівці з безпілотних літальних апаратів (БПЛА).

Оператори безпілотників – ще одна важлива професія, яка стала невід'ємною частиною сучасних військових операцій.

Основні завдання: управління розвідувальними та бойовими безпілотниками для збору даних або здійснення ударів по цілях.

Технології: складні комп'ютерні системи управління, супутникові комунікації, використання штучного інтелекту для автоматизації польотів і обробки зображень.

2. Професії, пов'язані з інформаційною війною

Інформаційна війна стала критично важливою складовою сучасних конфліктів. Військові операції тепер ведуться не лише на полі бою, але й в інформаційному просторі. Завдяки новітнім цифровим технологіям та масовій комунікації, інформаційні операції можуть змінювати суспільні настрої та впливати на політичні рішення.

Фахівці з інформаційно-психологічних операцій (ІПСО)

Ці професіонали спеціалізуються на управлінні інформацією для досягнення психологічного впливу на ворога чи цивільне населення.

Основні завдання: маніпуляція інформацією з метою деморалізації ворога, формування потрібної громадської думки або мобілізація підтримки.

Методи: використання соціальних мереж, ЗМІ, поширення дезінформації, кіберпропаганда, фальшиві новини.

Приклад: інформаційні кампанії під час російсько-української війни, які мали на меті підрив морального духу українського населення або дискредитацію західних союзників.

Фахівці з OSINT (Open Source Intelligence)

OSINT-аналітики збирають і аналізують інформацію з відкритих джерел: інтернет-ресурсів, соціальних мереж, новин, публічних баз даних.

Основні завдання: моніторинг інформаційного простору, збір даних про противника, виявлення інформаційних операцій ворога.

Приклад: розслідування групи Bellingcat щодо участі російських спецслужб у міжнародних злочинах (збиття MH17, отруєння Навального).

Кіберпропагандисти

Ці фахівці поєднують технічні навички з інформаційними атаками для впливу на противника через інтернет-простір.

Завдання: розповсюдження пропаганди через соцмережі, форуми та інші онлайн-платформи, вплив на громадську думку через маніпуляцію контентом.

Фахівці з аналізу великих даних (Big Data)

Ці спеціалісти аналізують великі обсяги інформації для виявлення трендів та прогнозування розвитку ситуацій на полі бою або в суспільстві.

Завдання: обробка даних із соціальних мереж, супутникових знімків, інформаційних потоків для виявлення загроз або моделювання результатів військових операцій.

3. Спеціальності вищих військових навчальних закладів, пов'язані з цифровими технологіями.

В Україні добре розвинута школа підготовки військових спеціалістів, які стануть спеціалістами у сфері інформаційного протиборства. Курсанти здобувають ступені вищої освіти "бакалавр" та "магістр" із врученням диплома державного зразка, отримують військове звання "лейтенант" і скеровуються для подальшої служби на офіцерських посадах у Збройних Силах та інших силових структурах України.

Освітні програми Житомирського військового інституту імені С.П. Корольова.

1. Автоматизація та комп'ютерно-інтегровані технології.
2. Автоматизована обробка розвідувальної інформації.
3. Безпілотні системи тактичного класу.
4. Електроенергетика, електротехніка та електромеханіка.
5. Засоби спеціального контролю.
6. Кібербезпека.
7. Комп'ютеризовані засоби інформаційного впливу.
8. Обробка даних космічної розвідки.
9. Озброєння та військова техніка підрозділів і частин охорони державної таємниці.
10. Організація захисту інформації з обмеженим доступом та автоматизація її обробки.
11. Радіоелектронні системи бортових та наземних засобів космічних комплексів.
12. Системи радіоелектронної розвідки.
13. Системи та засоби радіоелектронної боротьби.
14. Системи та комплекси радіозв'язку спеціальної розвідки.
15. Телекомунікації та радіотехніка.

Освітні програми Військового інституту телекомунікацій та інформатизації імені Героїв Крут (м. Київ).

1. Комп'ютерні науки та інформаційні технології.

2. Кібербезпека в інформаційно-телекомунікаційних системах.
3. Кіберрозвідка, системи та комплекси спеціального призначення.
4. Інформаційні системи та технології.
5. Телекомунікаційні системи та мережі.
6. Управління діями підрозділів зв'язку.
7. Спецозброєння та робототехнічні військові комплекси.

Освітні програми Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського"

1. Комп'ютерні системи і технології спеціального зв'язку.
2. Безпека державних інформаційних ресурсів.
3. Спеціальні системи електронних комунікацій.

Освітні програми Національної академії Служби безпеки України.

1. Національна безпека (кіберзахист, забезпечення державної безпеки в інформаційній сфері), кіберзахист у сфері інформаційних технологій та кіберпросторі.
2. Національна безпека (кіберзахист, забезпечення державної безпеки в інформаційній сфері), організація захисту інформації з обмеженим доступом.

Освітня програма Національної академії Державної прикордонної служби України імені Богдана Хмельницького

1. Електронні комунікації та радіотехніка.

Висновки

Професії, пов'язані із сучасними цифровими технологіями у військовій сфері, з кожним роком набувають усе більшого значення. Найбільший акцент робиться на спеціальностях, що пов'язані з інформаційними війнами, кібербезпекою та управлінням великими даними. Інформаційна війна, яка ведеться за допомогою сучасних цифрових технологій, стає так само важливою, як і традиційні бойові дії. Спеціалісти з інформаційних технологій, кібербезпеки, ІПСО та з OSINT є критично важливими для успішного захисту та наступу в сучасних конфліктах.

Додаткова література до опрацювання модуля:

1. Левченко О. Інформаційні війни: як перемагати росію у світовому інфопросторі. - Режим доступу: https://zahidfront.com.ua/news/Informacijni-vijni-yak-peremagati-rosiyu-svitovomu-info-prostori.html

2. Шемчук В. Інформаційна функція та її місце в системі функцій сучасної держави. - Режим доступу: http://juris.vernadskyjournals.in.ua/journals/2018/4_2018/9.pdf
3. Задубінний А. Сьогодні інформаційна війна — це стрижнева конструкція будь-якої війни. — Ганна Маляр. — Режим доступу: https://armyinform.com.ua/2023/02/27/sogodni-informaczijna-vijna-cze-stryzhneva-konstrukcziya-bud-yakoyi-vijny-ganna-malyar-2/

Література з тематики для поглибленого вивчення:

4. Смаль Ю. Як я була ботом. – Київ : Видавничий дім “Комора”, 2019. – 152 с.
5. Огнева М. Боти на роботі. Як фейкові акаунти у соцмережах підіграють росії. – Режим доступу: https://bahmut.in.ua/boty-na-roboti-yak-fejkovi-akaunty-u-soczmerezhah-pidigrayut-rosiyi/
6. Б. А. Уявні (не)друзі: як викрити тролів і ботів? - Режим доступу: https://provse.te.ua/wp-content/uploads/2023/10/YAk-vykryty-botiv-i-troliv.pdf
7. Відео-цикл “Під маскою пропаганди” на youtube-каналі “2 +2”.
8. Б. А. 8 методів пропаганди: як люди перетворюються на зомбі. – Режим доступу https://zib.com.ua/ua/print/151037.html
9. Бабенко Ю. Інформаційна війна – зброя масового знищення! – Режим доступу: https://www.pravda.com.ua/rus/articles/2006/04/20/4399050/
10. Макаренко Л. Еволюція форм та методів ведення інформаційної війни. – Режим доступу: https://www.researchgate.net/publication/350008570_EVOLUCIA_FORM_TA_METODIV_VEDENNA_INFORMACIJNOI_VIJNI
11. Як не стати жертвою маніпуляцій ЗМІ? Розповідає Юлія Дукач. – Режим доступу: https://inrespublica.org.ua/bez-kategoriyi-uk/yak-ne-staty-zhertvoyu-manipulyatsij-zmi-rozpovidaye-yuliya-dukach.html
12. Куцепал С. Критичне мислення як засіб спротиву в інформаційній війні. – Режим доступу: http://fil.nlu.edu.ua/article/view/265682
13. Б. А. Протистояння інформаційним війнам та пропаганді у сучасному світі. – Режим доступу: https://welfare.green/protistoyannya-informacijjnim-vijjnam-ta-propagandi-u-suchasnomu-sviti/
14. Горбань Ю., Олійник О. Медіаграмотність як чинник захисту інформаційного простору від ворожої дезінфомації в час війни. – Режим доступу: http://ukrinfospace.knukim.edu.ua/article/view/300896
15. Пилипів І. Війну виграють технології. Як штучний інтелект допоможе перемогти у війні з РФ? – Режим доступу: https://www.epravda.com.ua/publications/2023/12/4/707197/

16. Б. А. Штучний інтелект і дезінформація: можливості та ризики в умовах війни. – Режим доступу: https://www.ukrinform.ua/rubric-technology/3691961-stucnij-intelekt-i-dezinformacia-mozlivosti-ta-riziki-v-umovah-vijni.html
17. Б. А. Як штучний інтелект допомагає в сучасних війнах: чи зможе він замінити військових на фронті. – Режим доступу: https://weukraine.tv/top/yak-shtuchnyj-intelekt-dopomagaye-v-suchasnyh-vijnah-chy-zmozhe-vin-zaminyty-vijskovyh-na-fronti
18. Даниленко В. Інформаційні війни та штучний інтелект у боротьбі за виживання України. – Режим доступу: https://www.uacenter.media/-/133410-nformac-yn-v-yni-ta-shtuchniy-ntelekt-u-borot-b-za-vizhivannya-ukra-ni.html
19. Печерський А. Інтерв'ю зі штучним інтелектом: що Chat GPT "думає" про російсько-українську війну. – Режим доступу: https://armyinform.com.ua/2023/02/26/intervyu-zi-shtuchnym-intelektom-shho-chatgpt-dumaye-pro-rosijsko-ukrayinsku-vijnu/
20. Петрів О. Дезінформація та штучний інтелект: (не)видима загроза сучасності. – Режим доступу: https://cedem.org.ua/analytics/dezinformatsiya-shtuchnyi-intelekt/
21. Баловсяк Н. Фабрика брехні. Як штучний інтелект допомагає в інформаційній війні проти України. – Режим доступу: https://novynarnia.com/2024/08/13/fabryka-brehni-yak-shtuchnyj-intelekt-dopomagaye-v-informaczijnij-vijni-proty-ukrayiny/
22. Вікіпедія. Стаття "Російсько-українська кібервійна".
23. Горбенко В. Кібервійни та кібербезпека у сучасному світі. Курс лекцій. – Режим доступу: https://moodle.znu.edu.ua/course/view.php?id=6844
24. Б. А. Що таке OSINT (Open Source Intelligence, розвідка на основі відкритих джерел)? – Режим доступу: https://thetransmitted.com/adlucem/shho-take-osint-open-source-intelligence-rozvidka-na-osnovi-vidkrytyh-dzherel/
25. Куля А. Як працює OSINT-розвідка та чому небезпечно публікувати інформацію в інтернеті. Режим доступу: https://fakty.com.ua/ua/ukraine/suspilstvo/20220429-yak-praczyuye-osint-rozvidka-ta-chomu-nebezpechno-publikuvaty-informacziyu-v-internet/
26. Старосек А. OSINT в Україні: хто і як допомагає фронту під час війни? – Режим доступу: https://www.pravda.com.ua/columns/2023/01/23/7386112/
27. Посібник з верифікації. Режим доступу: https://verificationhandbook.com/book_ua/