інтегруються в єдину екосистему. Такий підхід, у поєднанні з традиційними інструментами кримінального аналізу, підвищує здатність Національної поліції України ефективно реагувати на сучасні виклики та зміцнює позиції країни в міжнародній системі безпеки.

Список використаних джерел

1. Nyman Gibson Miralis, Digital technology and dissemination at the heart of INTERPOL's 2023 annual report, January 23 2025.

2. Making international police messaging more effective and accurate. URL: https://www.interpol.int/en/How-we-work/I-CORE-our-vision-for-change/NEXUS.

3. Ахтирська Н. М., Міжнародне співробітництво під час кримінального провадження: теоретичні та практичні аспекти, Київ: Логос, 2019.

4. Зуєв В. В. та ін., Міжнародне співробітництво у кримінальному провадженні, Одеса: НУ «ОЮА», 2022.

5. Ovsianiuk D. Intelligence cycle as the basis of analytical activity in combating drug-related crime. Law Journal of the National Academy of Internal Affairs. 2024. Vol. 14, no. 2. P. 95–104.

6. Федчак І. А., Основи кримінального аналізу, Львів: ЛДУВС, 2021.

Петров Вадим Амінович,
заступник начальника 1-го управління (аналітичного) – начальник 1-го відділу (кримінального аналізу) Департаменту кримінального аналізу Національної поліції України

МЕДІААНАЛІЗ. СУЧАСНІ ПІДХОДИ ТА МЕТОДИ БОРОТЬБИ З ДЕЗІНФОРМАЦІЄЮ

У світі, де більшість процесів – від особистого спілкування до державного управління – цифровізовано, саме інформація стає головним ресурсом, інструментом впливу та об'єктом боротьби.

В умовах, коли швидкість обміну даними, доступ до знань і вміння розрізняти правду від брехні мають вирішальне значення. Інформація стала важливішою за фізичну силу. Водночас вона перетворилася на об'єкт атак: її викривляють,

спотворюють, використовують для маніпуляцій. Сьогодні йде боротьба не лише за території чи ресурси – точиться боротьба за свідомість людини.

Аналіз міждисциплінарних досліджень (у сферах кібербезпеки, соціальної психології, інформаційної безпеки та медіаграмотності) свідчить, що маніпуляції – одна з найнебезпечніших і водночас найпоширеніших форм цифрових загроз. Їхня суть полягає у цілеспрямованому викривленні інформації з метою впливу на думки, емоції та поведінку людей.

Оскільки близько 80–90 % інформації людина сприймає візуально, маніпулятори активно використовують зображення, відео, інфографіку. Їхня мета – створити видовищний і переконливий продукт, що пробуджує сильні емоції: страх, гнів, розпач, тривогу. Це дозволяє їм формувати потрібну громадську думку або нав'язувати певні дії.

Сьогодні найпоширенішими каналами поширення фейків є новинні сайти, соціальні мережі, блоги та електронні розсилки. Вони можуть бути спрямовані як на конкретні країни, так і на міжнародну аудиторію.

Найтиповіші форми інформаційних маніпуляцій включають:

– медіаманіпуляції: редагування фото/відео, зміна контексту, створення фейкового контенту;

– новинні маніпуляції: викривлення заголовків, подання думки як факту, замовчування деталей;

– фейкові експертизи: цитати псевдоекспертів, перекручування заяв, маніпулятивні аналітичні довідки;

– інформаційні фейки: вигадані повідомлення, посилання на неіснуючі джерела;

– маніпуляції дослідженнями: використання слабких методик, викривлені інтерпретації результатів.

Все це створює ілюзію достовірності й водночас підриває довіру до справжніх джерел.

Для виявлення джерел дезінформації та фейкових вкидів використовують інструменти OSINT (Open Source Intelligence) – розвідки за відкритими джерелами [1, с. 169]. Це підхід, за якого дані збираються не зі спецслужб чи закритих баз, а з публічно доступних джерел: вебсайтів, реєстрів, соцмереж, новин, відео тощо.

У Департаменті кримінального аналізу Національної поліції України активно застосовуються такі напрями OSINT:

– медійна розвідка – аналіз новин (державних та іноземних);

– інтернет-розвідка – перевірка вебсайтів, форумів, блогів;

– SOCMINT – моніторинг соцмереж, публікацій, коментарів;

– GeoOSINT – визначення місця подій за фото, відео, супутниковими знімками;

– Документарна розвідка – пошук і аналіз інформації в публічних базах, реєстрах, судових документах.

OSINT дозволяє розпізнавати джерела фейків, верифікувати факти, відстежувати поширення інформаційних атак та збирати докази для подальших дій.

Сьогодні інформація – це не просто потік новин. Це зброя, яку активно використовують для послаблення суспільства, деморалізації населення, дестабілізації держав. Через фейки, маніпуляції, «експертні» думки без джерел або патріотичні гасла, що сіють паніку, нас змушують сумніватися у власній державі, у собі, у правді.

Протидіяти цьому можна лише комплексно:

– розвиваючи критичне мислення;
– використовуючи OSINT для перевірки фактів;
– дотримуючись правил кібергігієни;
– підвищуючи інформаційну обізнаність.

Лише поєднання технологічних інструментів і людського усвідомлення може стати ефективною відповіддю на загрози інформаційного поля.

Усе це – не лише про особистий захист. Це про стійкість суспільства в умовах гібридної війни. А значить – і про перемогу.

Список використаних джерел

1. ОДУВС ДНДІ МВС Реалізація філософії «Intelligence-LED Policing» в системі кримінального аналізу Національної поліції України, 2024.