

Шило Ігнат Єгорович

курсант 1 курсу факультету № 1
Донецького державного університету
внутрішніх справ, рядовий поліції

Габорець Ольга Андріївна

доктор філософії, доцент, доцент
кафедри оперативно-розшукової
діяльності та інформаційної безпеки
Донецького державного університету
внутрішніх справ

СТРАТЕГІЇ БОРОТЬБИ З ДЕЗІНФОРМАЦІЄЮ У МЕРЕЖІ ІНТЕРНЕТ ПІД ЧАС ВОЄННОГО СТАНУ

У сучасному світі, який насичений технологіями та змінами, мережа Інтернет стала не лише основним джерелом інформації, але й ареною для боротьби за вплив та контроль над масовою свідомістю. У зв'язку з цим, проблема дезінформації, особливо у контексті воєнного стану, набуває нових вимірів та небезпек.

Воєнні конфлікти, незважаючи на свої прямі військові аспекти, часто відбиваються на сфері інформаційної війни, де використання дезінформації стає потужним інструментом. Умови воєнного стану створюють ідеальні умови для розповсюдження фейкових новин, маніпуляції громадською думкою та впливу на масову свідомість через Інтернет. Така дезінформація може мати серйозні наслідки, включаючи паніку серед населення, підірвання довіри до державних інституцій та навіть збройні конфлікти.

У юридичній літературі, захист інформації - це сукупність організаційно-технічних заходів і правових норм для запобігання заподіяння шкоди інтересам власника інформації та осіб, які користуються інформацією [1].

Для того щоб ефективно боротися з дезінформацією у мережі Інтернет під час воєнного стану, потрібно розробити комплексні стратегії, які поєднують в собі технологічні, правові та освітні підходи. Ось деякі з можливих стратегій:

- моніторинг та аналіз інформації: важливо мати систему, яка постійно моніторить інформаційний простір, виявляє потенційну дезінформацію та аналізує її походження та поширення. Це може включати в себе використання алгоритмів штучного інтелекту для виявлення шаблонів та трендів у поширенні дезінформації;

- контрдезінформаційні кампанії: для протидії дезінформації потрібно активно впливати на інформаційний простір шляхом запуску контрдезінформаційних кампаній. Це може включати в себе публікацію фактів, розкриття маніпуляцій та викриття дезінформаторів;

- залучення громадськості та експертів може виявитися ключовим у боротьбі з дезінформацією. Для цього можна створити платформи, на яких громадяни зможуть виявляти та відстежувати поширення дезінформації. Також важливо співпрацювати з науковими установами та журналістами для аналізу та розкриття дезінформаційних кампаній.

Освітня робота: важливо проводити освітню роботу серед населення щодо виявлення та протидії дезінформації. Це може включати в себе навчання критичного мислення, навичок перевірки джерел та впізнавання маніпуляцій.

Співпраця з міжнародними партнерами: важливо співпрацювати з іншими країнами та міжнародними організаціями для обміну інформацією та координації зусиль у протидії дезінформації.

Ці стратегії, які поєднують технологічні та освітні підходи, можуть сприяти ефективній боротьбі з дезінформацією у мережі Інтернет під час воєнного стану. Однак їх успішне впровадження вимагатиме спільних зусиль з боку уряду, громадськості та міжнародних партнерів.

Список використаних джерел:

1. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 р. №80/94-ВР URL: <https://zakon.rada.gov.ua/laws/show/80/94-вр#Text>.

Шляхова Валерія Олександрівна
студентка 201_СПД навчальної групи
ННІ № 3 НАВС

Науковий керівник:
Кудінов Вадим Анатолійович
кандидат фізико-математичних наук,
доцент, професор кафедри
інформаційних технологій та
кібербезпеки ННІ № 1 НАВС

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ОСНОВНИХ ІНФОРМАЦІЙНИХ ПІДСИСТЕМ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ «ІНФОРМАЦІЙНИЙ ПОРТАЛ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ»

Від початку процесу інформатизації органів і підрозділів внутрішніх справ України минуло вже більше 50 років. За цей час накопичений чималий досвід використання різноманітних інформаційних та інформаційно-комунікаційних систем оперативно-розшукового та інформаційно-довідкового призначення.