

ВПЛИВ ПІДРОЗДІЛІВ КІБЕРПОЛІЦІЇ НА ПРОТИДІЮ ДЕЗІНФОРМАЦІЇ В УМОВАХ РОСІЙСЬКОЇ АГРЕСІЇ ПРОТИ УКРАЇНИ

Роман Русланович ОРЛОВ,

*магістр, старший інспектор
управління протидії кіберзлочинам
в місті Києві Департаменту кіберполіції
Національної поліції України
<https://orcid.org/0000-0002-6505-470X>*

THE INFLUENCE OF CYBERPOLICE UNITS ON COUNTERING DISINFORMATION IN THE CONDITIONS OF RUSSIAN AGGRESSION AGAINST UKRAINE

Below is a report on the introduction of cyberpolicy divisions in defense of disinformation in the minds of Russian aggression against Ukraine. The actual analysis of the role and effectiveness of cyberpolitics in the context of information warfare is further aimed at determining the strategic and technological aspects that contribute to the accumulation and counteraction of disinformation. Virtual dynamic cyber downloads and the need for innovative solutions, work can find optimal approaches and tools for the effective fight against the manipulation of information in the minds of high-tech aggression

Дезінформація під час війни стає важливим аспектом кіберзлочинності, викликаючи серйозні загрози для національної безпеки та глобальної стабільності. Цей вид кіберзлочину використовується з метою впливу на суспільство, зміни геополітичного ландшафту та психологічної обстановки під час конфліктів.

Поширення неправдивої інформації через кіберпростір під час війни може включати в себе фейкові новини, маніпуляції зображеннями та відео, а також створення штучних атмосфер паніки та хаосу. Це спрямовано на збен-теження супротивників, підрив авторитету влади та психологічне враження населення [1].

Однією з основних проблем дезінформації в кіберпросторі під час війни є важкість визначення джерел та перевірки достовірності інформації. Зловми-сники можуть використовувати анонімні мережі, псевдоніми та інші техноло-гії, щоб ускладнити виявлення та притягнення до відповідальності.

Для протидії дезінформації під час війни необхідний комплексний підхід, так наприклад, Департамент кіберполіції Національної поліції України пра-цює за наступними напрямками в даній сфері, а саме:

- Виявлення та розслідування кібератак;
- Міжнародна співпраця;
- Законодавчі ініціативи;
- Інформаційні кампанії;
- Розробка спеціальних технічних засобів.

Кіберполіція України виявляє та розслідує кібератаки, спрямовані на поширення дезінформації та маніпуляції інформацією, через ряд дієвих стратегій та методів:

– кіберполіція проводить систематичний моніторинг кіберпростору для виявлення незвичайної активності, аномалій та можливих загроз, пов'язаних із поширенням дезінформації.

– спеціалізовані аналітичні підрозділи кіберполіції аналізують кіберзагрози, що містять елементи дезінформації. Це включає вивчення методів атак, використання фейків та поширення фальшивої інформації.

– кіберполіція вступає в тісну взаємодію з кіберспільнотою, включаючи приватні кібербезпечні компанії та інші урядові агентства. Це дозволяє обмінюватися інформацією та об'єднувати зусилля для боротьби із кіберзагрозами.

– підрозділи протидії кіберзлочинам використовують цифрові методи дослідження для встановлення походження кібератак, ідентифікації зловмисників та реконструкції сценаріїв атак.

– у рамках виявлення дезінформації кіберполіція зосереджує увагу на протидії кібершпигунству, спрямованому на вплив на інформаційний ландшафт.

Ці стратегії дозволяють кіберполіції ефективно виявляти та розслідувати кібератаки, спрямовані на дезінформацію, забезпечуючи тим самим кібербезпеку та інформаційну безпеку країни [2].

Кіберполіція України виявляє високий рівень ефективності в сфері міжнародної співпраці з іншими країнами та міжнародними партнерами в контексті кібербезпеки, а саме:

– кіберполіція активно співпрацює з агентствами інших країн, обмінюючи інформацією щодо виявлення та аналізу кіберзагроз. Цей обмін сприяє швидкій реакції на нові кіберзагрози та дозволяє партнерам ефективно протидіяти їм.

– підрозділи протидії кіберзлочинам беруть участь у спільних кібервправах разом із міжнародними партнерами. Це дозволяє взаємодіяти в реальному часі та об'єднувати зусилля для розслідування та припинення кіберзлочинності.

– кіберполіція долучається до розробки та впровадження міжнародних стандартів у галузі кібербезпеки. Спільні підходи та стандарти дозволяють країнам ефективно співпрацювати, дотримуючись єдиної методології.

– кіберполіція активно бере участь у міжнародних форумах, конференціях та зустрічах, де обговорюються актуальні питання кібербезпеки. Це не лише розширює мережу співпраці, але й сприяє обміну передовими практиками та ідеями.

Загалом, ця міжнародна співпраця допомагає кіберполіції України оперативно реагувати на кіберзагрози та спільно з іншими країнами розв'язувати проблеми, пов'язані із кібербезпекою [3].

Департамент кіберполіції приділяє значну увагу вдосконаленню законодавства, спрямованого на протидію особам, які втручаються у кіберпростір для розповсюдження дезінформації, а саме:

– кіберполіція активно здійснює аналіз існуючого законодавства, виявляє його прогалини та потребу в модернізації для більш ефективного протидії кіберзлочинності та дезінформації.

– забезпечує активну участь у розробці та внесенні пропозицій до законодавчих ініціатив, спрямованих на покарання осіб, які здійснюють кібератаки для поширення дезінформації. Це може включати в себе нові закони або зміни до існуючих.

– враховуючи швидкий розвиток кіберзагроз, кіберполіція прискорено впроваджує сучасні законодавчі практики для ефективного реагування на нові виклики у кіберпросторі.

– регулярно співпрацює з іншими відомствами та органами влади для взаємодії у сфері законодавства та виявлення оптимальних шляхів вирішення кіберправопорушень.

Такий підхід дозволяє кіберполіції реагувати на зміни в кіберзагрозах та швидко вдосконалювати законодавство для забезпечення ефективного захисту кіберпростору від дезінформації.

Інформаційні кампанії та сприяння створенню обізнаного суспільства є ключовими складовими стратегії для протидії дезінформації та зміцнення інформаційної безпеки. Інформаційні кампанії фокусуються на поширенні правдивої інформації та проведенні освітніх заходів щодо розпізнавання дезінформації. Це може включати в себе створення публікацій, відеоматеріалів, веб-семінарів і т.д. Кампанії спрямовані на різні цільові аудиторії, включаючи громадян, журналістів, державних службовців та інші групи, які можуть бути вразливі до дезінформації.

Ці заходи спрямовані на те, щоб не лише реагувати на дезінформацію, але й активно залучати громадян у формуванні обізнаного суспільства, яке вмє аналізувати інформацію та розрізняти факти від маніпуляцій.

Щодо розробки технічних засобів, кіберполіція розробила бот у месенджері Telegram для блокування сервісів дезінформації “stoprussiachannel”. За допомогою боту можна заблокувати Telegram-канали, YouTube-канали, Facebook-групи, Instagram-профілі, які розповсюджують дезінформацію, а також інформацію щодо місць дислокацій ЗСУ. Даний бот є важливим ресурсом для боротьби з дезінформацією на кіберфронті [4].

Вплив підрозділів кіберполіції на протидію дезінформації в умовах російської агресії проти України визначається як критично важливий для забезпечення інформаційної безпеки та захисту від кіберзлочинності. Системний підхід, використання сучасних технологій та співпраця з іншими гілками влади та міжнародними партнерами стають ключовими аспектами успішної боротьби із дезінформацією. Забезпечення інформаційної безпеки вимагає не лише ефективних технічних рішень, але і постійного моніторингу, аналізу та освіти громадськості для виявлення та відповідального сприйняття інформації.

Список використаних джерел:

1. Атака на інформаційному фронті - поради кіберполіції щодо захисту гаджетів від витоку даних URL: <https://cyberpolice.gov.ua/article/ataka-na-informacijnomu-fronti---porady-kiberpolicziyi-shhodo-zaxystu-gadzhetiv-vid-vytoku-danyx-8131/> (дата звернення: 28.11.2023).

2. Закон України “Про основні засади забезпечення кібербезпеки України” № 2163-VIII від 05.10.2017 р. URL: <https://ips.ligazakon.net/document/T172163?an=1> (дата звернення: 28.11.2023).

3. Кіберполіція провела 9 міжнародних операцій із викриття хакерських угруповань
URL: <https://cyberpolice.gov.ua/news/u--rocz-i-kiberpolicziya-provela--mizhnarodnykh-operaczij-iz-vykryttya-hakerskykh-ugrupovan-402/> (дата звернення: 28.11.2023).

4. Кіберполіція розробила Telegram чат-бот для блокування сервісів дезінформації
URL: <https://cyberpolice.gov.ua/news/kiberpolicziya-rozrobyla-telegram-chat-bot-dlya-blokuvannya-servisiv-dezinformacziyi-1699/> (дата звернення: 28.11.2023).