

УДК 351.751

Дмитро Володимирович ШВЕЦЬ,

доктор юридичних наук, доцент,

заслужений працівник освіти, полковник поліції,

перший проректор Харківського національного університету внутрішніх справ;

ORCID: <https://orcid.org/0000-0002-1999-9956>

ЗАГРОЗИ НАЦІОНАЛЬНІЙ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ В ПЕРІОД ПАНДЕМІЇ COVID-19

У період поширення вірусу COVID-19 набуває великого значення захист інформаційної безпеки держави від цілої низки загроз. Сучасне

інформаційне суспільство є вкрай уразливим до зловмисних дій окремих елементів в інформаційному просторі мережі Інтернет та медіапросторі. Перш за все, йдеться про неправдиві повідомлення, що можуть розміщуватись як з метою спричинення негативних наслідків, так і для задоволення потреби певних елементів у відомості чи суспільному резонансі.

До таких загроз можна віднести поширення неправдивої інформації щодо самої хвороби (фейкова інформація про кількість загиблих/хворих, симптоматику, кількість ускладнень після хвороби тощо), лікування (фейкова інформація щодо ефективності певних ліків чи методик лікування, ефективності та небезпечності певних видів щеплень тощо), джерела хвороби (вже відомі фейкові повідомлення про розповсюдження COVID-19 завдяки використанню веж 5G, непідтверджені витоки щодо штучного поширення вірусу певними державами чи іншими суб'єктами, релігійний контекст розповсюдження вірусу тощо) та інших факторів, пов'язаних з протидією пандемії (фейкові новини стосовно умов лікування у лікарнях, умов у місцях примусової обсервації та цілої низки різних факторів).

Для вдалої протидії зазначеним загрозам інформаційній безпеці у цій сфері необхідно створити ефективно діючий механізм правових засобів протидії таким загрозам та законодавчо його закріпити.

Слід зазначити, що існує позитивний закордонний досвід протидії певним таким загрозам. Так, на одному з інформаційних ресурсів Європолу зазначено, що «злочинці швидко адаптували свої методи, щоб використовувати наші страхи навколо пандемії COVID-19, головна їх мета – отримання прибутку будь-якими необхідними засобами». Водночас на цьому ж ресурсі зазначається ціла низка засобів протидії такій злочинній діяльності [1]. Слід наголосити, що пропонується розширити визначення, дане Європолом, оскільки головною метою розповсюдження неправдивої інформації щодо COVID-19 не завжди є отримання прибутку. Це може бути стимулювання панічних настроїв, недовіри до наявної влади (як один з методів гібридної війни) і просто отримання позитивних емоцій від популярності постів злочинця в мережі Інтернет.

Також украй важливою частиною механізму протидії загрозам національній інформаційній безпеці в період пандемії COVID-19 має стати планування. Так, в Європейському Союзі були ухвалені Кодекс практики проти дезінформації [2] та План дій проти дезінформації [3]. Саме на основі цих документів пропонується розробити загальнодержавний план протидії інформаційним загрозам у період пандемії COVID-19.

Наразі законодавство майже не передбачає відповідальності за поширення неправдивої інформації щодо пандемії COVID-19. Водночас, ураховуючи його велику небезпеку для національних інтересів, слід посилити відповідальність за розміщення завідомо неправдивої інформації про COVID-19, яка може призвести до несприятливих наслідків. Слід зазначити, що правоохоронні органи нашої держави вже активно діють у

цьому напрямку – так, ще навесні 2020 року Служба Безпеки України почала активно притягати до відповідальності осіб, що поширювали завідомо неправдиву інформацію стосовно пандемії COVID-19 (зокрема, інформацію стосовно кількості хворих, кількості померлих, кількості койко-місць у лікарнях тощо) [4].

Крім того, під час пандемії COVID-19 багато суб'єктів перейшли на дистанційний режим роботи (зокрема, заклади освіти). Наприклад, усі освітні заняття перейшли у відеоформат з широким використанням таких сервісів, як «Moodle», «Discord», «Zoom» і «Skype». Водночас усі сервіси можуть стати ціллю хакерських атак з метою отримання доступу до персональних даних, саботування діяльності суб'єктів, що є користувачами, крадіжки електронних акаунтів тощо. Тому важливою складовою правового механізму засобів забезпечення національної інформаційної безпеки має стати особливий режим захисту таких сервісів від атак під час пандемії COVID-19.

Також важливим є запровадження державних програм із підвищення інформаційної грамотності як серед громадян, так і серед суб'єктів господарювання, що функціонують у сфері медіа. Для цього необхідно проводити спеціальні масові заходи (у формі лекцій, онлайн-семінарів, каналів на Youtube, постів у соціальних мережах та меседжерах тощо). Доцільно залучати до участі в таких заходах як представників наукової спільноти, так і фахівців правоохоронних органів.

Висновок. Ураховуючи періодичність виникнення нових пандемій, необхідно створити такий механізм захисту національної інформаційної безпеки вже зараз, оскільки невідомими є як наслідки пандемії COVID-19, що триває, так і наслідки майбутніх захворювань. Водночас створення ефективно діючого правового механізму засобів забезпечення національної інформаційної безпеки у сфері охорони здоров'я дозволить захистити національні інтереси від недобросовісних дій окремих суб'єктів.

Список бібліографічних посилань

1. Staying Safe During COVID-19: What You Need to Know // Europol : сайт. 12.11.2020. URL: <https://www.europol.europa.eu/activities-services/staying-safe-during-covid-19-what-you-need-to-know> (дата звернення: 01.02.2021).
2. Code of Practice on Disinformation // European Commission : сайт. 18.01.2021. URL: <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation> (дата звернення: 01.02.2021).
3. Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Action Plan against Disinformation. Brussels, 05.12.2018. URL: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56166 (дата звернення: 01.02.2021).
4. СБУ притягає до відповідальності осіб, які поширюють фейки про коронавірус // Служба безпеки України : офіц. сайт. URL: <https://ssu.gov.ua/-/novyny/7300> (дата звернення: 01.02.2021).