УПРАВЛІННЯ КРИЗОВИМИ КОМУНІКАЦІЯМИ ТА МЕХАНІЗМИ ПРОТИДІЇ ІНФОРМАЦІЙНИМ АТАКАМ

MANAGEMENT OF CRISIS COMMUNICATIONS AND MECHANISMS FOR COUNTERING INFORMATION ATTACKS

УДК 316.77:005.931.1
DOI https://doi.org/10.32782/pma2663-5240-2023.33.40

Чуб С.В.
здобувач кафедри публічного адміністрування,
Міжрегіональна Академія управління персоналом,
https://orcid.org/0009-0001-3703-9414

Стаття присвячена проблемам управління кризовими комунікаціями та механізмам протидії інформаційним атакам в державних органах при виникненні надзвичайних кризових ситуацій. Особливий акцент зроблено на такій кризовій ситуації, як воєнний стан та військове протистояння зовнішньому агресору, які є реаліями української держави на момент написання статті. Автором на основі аналізу наявної літератури, нормативно-правової бази та наявних міжнародних практик, здійснена спроба детального висвітлення системи та векторів діяльності державних органів у процесі управління кризовими комунікаціями. Наголошено на необхідності врахування постійного розвитку інформаційних технологій та використання їх у дослідженому процесі. Окремо акцентовано увагу на тому, що управління кризовими комунікаціями включає розподіл інформації на три складові: ту яку необхідно у стислі строки донести найбільшим масам; ту яка має бути перевіреною або поданою з затримкою задля національної безпеки в умовах воєнного стану та ту, яка не може бути подана масам доки діє воєнний стан. Досліджуючи механізми протидії інформаційним атакам, автором розроблені власні рекомендації щодо протидії інформаційним атакам, на які має звертати увагу представники органів державної влади. Механізми протидії інформаційним атакам для органів державної влади в умовах воєнного стану передбачають створення кризового комунікаційного центру, підвищення обізнаності персоналу, моніторинг медіа та соціальних мереж, захист важливої інформації, публічність і відкритість, аналіз інформації, співпрацю з міжнародними партнерами, публічні інформаційні кампанії, аналіз суспільного настрою та резервні канали зв'язку. У висновках автор зазначає, що управління кризовими комунікаціями та механізми протидії інформаційним атакам є складним завданням, яке вимагає комплексного підходу та співпраці всіх зацікавлених сторін.

Ключові слова: *національна безпека, державне управління, механізми державного управління, надзвичайний стан, кризові комунікації, інформаційна атака, органи державної влади, взаємодія з громадськістю.*

The article is devoted to the problems of managing crisis communications and the mechanisms of countering information attacks in state bodies in the event of emergency crisis situations. Special emphasis is placed on such a crisis situation as martial law and military confrontation with a foreign aggressor, which are the realities of the Ukrainian state at the time of writing the article. Based on the analysis of existing literature, the legal framework and existing international practices, the author made an attempt to provide a detailed coverage of the system and vectors of the activities of state bodies in the process of managing crisis communications. The need to take into account the constant development of information technologies and their use in the researched process is emphasized. Particular attention is paid to the fact that the management of crisis communications includes the distribution of information into three components: that which must be conveyed to the largest masses in a short period of time; one that must be verified or submitted with delay for national security under martial law and one that cannot be submitted to the masses while martial law is in effect. Researching the mechanisms of countering information attacks, the author has developed his own recommendations for countering information attacks, which representatives of state authorities should pay attention to. Mechanisms for countering information attacks for state authorities under martial law include the creation of a crisis communication center, staff awareness raising, media and social network monitoring, protection of important information, publicity and openness, information analysis, cooperation with international partners, public information campaigns, analysis of public mood and backup communication channels. In the conclusions, the author notes that the management of crisis communications and countermeasures against information attacks is a complex task that requires a comprehensive approach and cooperation of all interested parties.

Key words: *national security, public administration, mechanisms of public administration, state of emergency, crisis communications, information attack, public authorities, interaction with the public.*

Постановка проблеми. У сучасному інформаційному суспільстві, де інформація летюча, нестримна і миттєва, важливість управління кризовими комунікаціями та механізмів протидії інформаційним атакам надзвичайно актуальна. Зміни у медіа-ландшафті, зростаючий вплив соціальних мереж та можливості широкої розповсюдження інформації створюють серйозні виклики для організацій та владних структур. Управління кризовими комунікаціями є невід'ємною складовою стратегічного управління, зокрема у державних установах. Кризи можуть виникати внаслідок різних обставин: від природних катастроф і аварій до інформаційних криз, що поширюються в соціальних мережах. Для сучасної України такою майже щоденною кризою є загроза повітряних атак. Відправною точкою ефективного управління кризовими ситуаціями є вчасна та обізнана реакція, яка зменшує можливі збитки та допомагає відновити довіру громадськості. Механізми протидії інформаційним атакам стають все більш суттєвими у зв'язку зі зростанням кількості цифрових загроз і маніпуляційною активністю в інтернеті. Захист від дезінформації, фейкових новин і

кібератак стає необхідністю для забезпечення безпеки як національної, так і корпоративної. Вдосконалення технологій та стратегій для виявлення та реагування на такі загрози стає важливим завданням сучасного інформаційного управління.

Метою статті визначено дослідити сутність та етапність управління кризовими ситуаціями та розробки авторських пропозицій механізмів протидії інформаційним атакам для органів державної служби, з акцентуванням уваги на воєнний стан.

Аналіз останніх досліджень та публікацій. Проблематика управління кризовими комунікаціями та протидія інформаційним атакам не нова. Ще на початку XXI ст. науковці звернули активну увагу необхідності виявлення небезпечної інформації та побудові стратегій інформування громадськості про наявні кризи. Можемо виокремити роботи Т. Руденко [6], З. Бржевської [4], С. Толюпи [7], С. Носок [8], Однак, в умовах військової агресії РФ подана проблема набуває нового звучання та потребує уточнення і доопрацювання з урахуванням реалій сучасного інформаційного простору.

Галузь управління кризовими комунікаціями є відносно молодою для світової науки та її виникнення обумовлено розвитком інформаційного суспільства. З одного боку, поданий розвиток надав змогу швидко передавати інформацію, розпочати створення так званої «держави у смартфоні», надавши громадянам більш легкий доступ до оформлення більшості документів. З іншого боку – за рахунок кібератак існує ймовірність розповсюдження приватної інформації, а також подання недостовірної, фейкової або пропагандистської інформації, що є прикладом гібридних технологій ведення війни, притаманних РФ.

У нашому досліджені, управління кризовими комунікаціями ми розглядаємо, як стратегічний процес планування, координації і виконання комунікаційних заходів під час кризових ситуацій або надзвичайних обставин, які можуть загрожувати репутації, стабільності або функціонуванню організації, компанії, установи або державної структури. Управління кризовими комунікаціями спрямоване на ефективну взаємодію із зацікавленими сторонами, такими як громадськість, медіа, клієнти, партнери, акціонери та інші, з метою збереження та відновлення довіри, врегулювання ситуації та мінімізації можливих негативних наслідків.

Важливо також враховувати, що управління кризовими комунікаціями – це процес, який постійно змінюється та адаптується до нових викликів і технологій. Організації повинні бути готові до реагування на найновіші тренди в інформаційному середовищі, такі як соціальні мережі, інтернет-платформи та масові медіа.

Механізми протидії інформаційним атакам в свою чергу – це система заходів та стратегій, які вживаються для виявлення, запобігання та реагування на різновиди інформаційних загроз і атак, які можуть завдати шкоди національній безпеці, громадському порядку і довірі до інформації. Органи державної влади відіграють важливу роль у забезпеченні безпеки інформаційного простору та захисті національних інтересів.

Наукова література визначає наступні аспекти управління кризами через призму органів державної влади включають:

1) Аналіз ризиків та підготовка до кризи. Державні органи мають проводити оцінку можливих надзвичайних ситуацій та розробляти плани дій на випадок кризи.

2) Координація та співпраця. Важливо забезпечити ефективну взаємодію між різними владними органами, агентствами та іншими структурами під час кризи. Виникає потреба у розробці механізмів співпраці, обміну інформацією та ресурсами, а також призначення відповідальних за керівництво кризовими ситуаціями.

3) Комунікації. Державні органи мають бути готові до ефективного інформування громадян про ситуацію та рекомендації щодо дій у надзвичайних обставинах. Це включає в себе розробку планів комунікацій та використання різних каналів, включаючи засоби масової інформації та соціальні мережі.

4) Управління ресурсами. Державні органи мають забезпечити належне розподілення та використання ресурсів, включаючи фінансові, людські та матеріальні ресурси, для ефективного реагування на кризову ситуацію.

5) Оцінка та вдосконалення. Після завершення кризи, державні органи мають проводити аналіз подій та результатів управління кризами, з метою виокремлення сильних та слабких сторін та вдосконалення планів на майбутнє [1; 4, с. 45–52].

Першим кроком у розробці стратегії управління кризовими комунікаціями є розуміння важливості цього процесу. Кризи можуть виникнути з різних причин, включаючи природні катастрофи, технічні аварії, правопорушення. Управління кризовими комунікаціями допомагає зберегти репутацію організації, зменшити можливі збитки та відновити довіру громадськості. Розуміння важливості управління кризовими комунікаціями стає особливо актуальним у випадках великих надзвичайних

подій, таких як війна або ракетні атаки, які стали наразі українською буденністю. В умовах воєнних конфліктів і загроз безпеці управління кризовими комунікаціями стає невід'ємною складовою зусиль уряду та організацій для забезпечення безпеки та врегулювання кризових ситуацій. Очевидно, що розуміння її важливості стає ключовим завданням для збереження життя, майна та стабільності в подібних надзвичайних обставинах. В цьому випадку на наш погляд доречним є дотримання наступних аспектів:

– запобігання паніці та хаосу (ефективна комунікація допомагає зменшити страх і непорозуміння шляхом надання чіткої, об'єктивної та авторитетної інформації);

– підтримка морального духу (управління кризовими комунікаціями може включати в себе публічні звернення лідерів держави або інших осіб для підтримки морального духу громадян та заохочення до спільної дії у надзвичайних обставинах);

– планування евакуації та захисту (розробка та пояснення планів евакуації, методів захисту та процедур безпеки, що можуть зберегти життя та майно громадян);

– взаємодія з іншими країнами та міжнародними партнерами (співпраця з іншими країнами та міжнародними організаціями для обміну інформацією та координації дій);

– збереження національного єднання (ефективна комунікація допомагає зберегти згуртованість і відчуття солідарності серед громадян) [4, с. 90; 8, с. 126–128].

Важливою складовою управління кризовими комунікаціями на початковому етапі полягає у розробці кризової стратегії. Ця стратегія визначає план дій та принципи взаємодії організації чи держави з громадськістю та іншими зацікавленими сторонами під час кризової ситуації.

Найпершим етапом цієї стратегії виступає створення групи «швидкого реагування» – тих, хто уповноважені говорити від певної установи (речники, ключові особи, які подають офіційну перевірену інформацію). Ця група складається зі спеціалістів та експертів, які визначаються перед кризовою ситуацією та уповноважені негайно реагувати, координувати дії команди та забезпечувати ефективну комунікацію в умовах надзвичайних обставин.

Група «швидкого реагування» відповідає за комунікацію з медіа, громадськістю та іншими стейкхолдерами. Вони розробляють та поширюють офіційні повідомлення, надають інформацію та відповідають на запитання. Також вона має аналізувати реакцію громадськості, виявляти потенційні проблеми та реагувати на них. Вони також відстежують медіа і соціальні мережі, щоб знати, які інформаційні повідомлення поширюються [3, с. 89–90].

Наступна складова – аналіз ризиків. Важливо визначити, які саме питання будуть надходити від громадськості в умовах надзвичайної ситуації та підготувати відповіді на них, особливо це доречно з тими питаннями – які можуть бути найбільш складними або провокаційними (у випадку ЗМІ, з урахування можливої інформаційної війни). Це можна представити у вигляді таблиці, де ліва колонка містить перелік ризиків, а права колонка – відповіді.

Визначення ключових повідомлень є критичним етапом у процесі управління кризовими комунікаціями. Ключові повідомлення – це ідеї або інформація, яку доречно передати аудиторії під час кризової ситуації. Варто також врахувати, що для прикладу в умовах воєнного стану, не вся інформація мусить оперативно доноситися, адже може бути використана ворогом. Ці повідомлення повинні бути чіткими, конкретними і спрямованими на досягнення певних цілей, таких як збереження репутації, забезпечення безпеки або надання необхідної інформації. Повідомлення повинні бути зорієнтовані на потреби та очікування аудиторії і враховувати основні цілі вашого комунікативного плану.

Залучення партнерів є важливою складовою стратегії управління кризовими комунікаціями. У разі кризової ситуації співпраця з іншими організаціями, громадськими групами та партнерами може бути надзвичайно корисною для ефективного реагування та мінімізації негативних наслідків. Варто заздалегідь розуміти через які ЗМІ, організації буде відбуватися інформування громадськості щодо надзвичайних ситуацій. Залучення партнерів у процес управління кризовими комунікаціями допомагає розширити ресурси та експертизу, необхідну для ефективної реакції на кризову ситуацію і забезпечення захисту інтересів вашої організації чи держави.

Під час кризи важливо бути відкритим та транспарентним у комунікації з громадськістю та зацікавленими сторонами. Приховування інформації або намагання змінити обставини можуть призвести до втрати довіри. Замість цього, організація повинна дотримуватися принципів відкритості та виносити на загальний огляд реальну інформацію про кризову ситуацію, а також регулярно оновлювати громадськість щодо подальшого розвитку подій. Такий підхід допомагає зберегти довіру та підтримку у важких моментах.

Водночас, існує масив інформації, яка в період дії воєнного стану не має бути

розповсюдженою або ж інформування мусить відбутися із затримкою задля збереження обороноздатності країни. За цих умов варто мати масив тем, розподілених категорії: швидке інформування, інформування з затримкою, не підлягає розповсюдженню.

В умовах сьогодення уряд (державна установа) не обмежується виключно стандартними ЗМІ в контексті комунікації з громадянами, використання «нових ЗМІ» (соціальні мережі, ютуб-канали) також є важливим. Важливо вибирати та адаптувати канали комунікації відповідно до характеру кризи та аудиторії. Також слід враховувати, що кожен канал має свої особливості та аудиторію, тому вибір та адаптація каналів комунікації повинні відповідати конкретним потребам та характеру кризової ситуації.

Звернемо детальніше увагу на сучасні канал комунікації.

– Офіційні заяви на вебсайті організації (допомагають зберігати репутацію та надавати інформацію у вигляді ресурсу для громадськості).

– Розсилки електронних листів (у випадку якщо організація має базу даних або підписників, електронна розсилка може бути ефективним способом повідомлення аудиторій про кризову ситуацію).

– Повідомлення в соціальних мережах (соціальні мережі є важливим каналом для швидкого розповсюдження інформації та спілкування з аудиторією. Потрібно активно моніторити та реагувати на повідомлення та коментарі у соціальних мережах) [6].

– Прес-конференції (у разі важкої кризи проведення прес-конференцій може допомогти висвітлити ситуацію в мас-медіа та відповісти на запитання журналістів, що дозволяє забезпечити швидкий і точний обмін інформацією з громадськістю).

– Інтерактивні платформи (онлайн-консультації, вебінари чи форуми, на яких громадськість може ставити питання та отримувати відповіді в режимі реального часу. Але поданий варіант доречніше для знайомства з ймовірної кризою, а не такої, яка тільки но виникла).

Після завершення кризи, необхідно провести аналіз управління кризовими комунікаціями та ідентифікувати можливі зони вдосконалення. Цей етап допомагає покращити стратегію та план дій на майбутнє та зменшити ризик подібних ситуацій у майбутньому.

Механізми протидії інформаційним атакам – це комплекс заходів, методів і стратегій, спрямованих на виявлення, запобігання та відвернення інформаційних атак, а також на захист від їхніх негативних наслідків. Ці механізми використовуються для забезпечення інформаційної безпеки, захисту конфіденційності, цілісності та доступності інформації в організаціях, державних установах та інших сферах.

Характер сучасної війни проти РФ є гібридним, і як результат, інформація стає вагомим напрямом боротьби, адже ворог досить часто використовує фейкову інформацію задля подання України в негативному ключі (шляхом розповсюдження фейкових новин), що мусило б призвести до зменшення підтримки держави світовою спільнотою. Соціальні мережі та різні канали новин часто розповсюджують таку неперевірену інформацію задля отримання нових підписників, не розмірковуючи про наслідки, які вона може призвести для державного апарату в інформаційному полі [2].

Надалі нами розроблені рекомендації щодо механізмів протидії інформаційним атакам для державного сектору. Їх дотримання хоча і не нівелює відповідні загрози, але зробить їх менш дієвими.

1. Створення кризового комунікаційного центру. Створіть спеціальний центр для управління кризовими комунікаціями, який буде відповідати за моніторинг і реагування на інформаційні загрози. Цей центр повинен мати чітко визначену структуру та визначену відповідальність.

2. Підвищення обізнаності персоналу. Навчіть персонал органів державної влади розпізнавати інформаційні загрози та приймати заходи щодо їхнього запобігання. Організуйте регулярні навчальні семінари та тренінги. Доречним буде наявність відповідних структурних підрозділів, які на час дії воєнного стану займатимуться виключно у поданій сфері.

3. Моніторинг медіа та соціальних мереж. Спостерігайте за інформаційним простором, включаючи медіа та соціальні мережі, для виявлення негативних повідомлень та дезінформації. Важливо мати можливість швидко реагувати на них та виправляти невірну інформацію.

4. Захист важливої інформації. Забезпечте захист конфіденційної інформації та засобів зв'язку. Використовуйте шифрування та інші технічні заходи для захисту важливих документів та комунікацій.

5. Публічність і відкритість. Зберігайте відкритість та публічність щодо важливих подій і рішень уряду. Це допоможе запобігти поширенню дезінформації та сприятиме довірі громадськості.

6. Аналіз інформації. Використовуйте аналітичні інструменти для виявлення та аналізу

дезінформації та інформаційних атак. Співпрацюйте з експертами та аналітиками для отримання об'єктивної оцінки ситуації.

7. Співпраця з міжнародними партнерами. Встановіть зв'язки та співпрацюйте з іншими країнами та міжнародними організаціями для обміну інформацією та спільної боротьби з інформаційними загрозами.

8. Публічні інформаційні кампанії. Проводьте публічні інформаційні кампанії з метою надання достовірної інформації та освіти громадськості щодо інформаційних загроз.

9. Аналіз суспільного настрою. Використовуйте соціологічні дослідження та аналіз суспільного настрою для виявлення потенційних точок напруги та антиурядових настроїв.

10. Резервні канали зв'язку. Розробіть резервні канали зв'язку, які можуть бути використані у випадку обмежень чи відмови в основних системах зв'язку.

Таким чином, в умовах кризових ситуацій зокрема таких як ведення війни проти зовнішнього агресора, вагомим елементом виступають управління кризовими комунікаціями. Державні органи мають розбудувати стратегію на різні характери криз. Ця стратегія повинна включати в себе аналіз ризиків, створення кризового комунікаційного центру та розробку ключових повідомлень, які допоможуть ефективно взаємодіяти з аудиторією під час кризи. Один із важливих аспектів управління кризовими комунікаціями – це моніторинг медіа та соціальних мереж. Він є невід'ємною частиною процесу управління кризовими комунікаціями, оскільки дозволяє виявляти негативні повідомлення та дезінформацію, які можуть пошкодити репутацію організації. Також важливим принципом є транспарентність та відкритість у комунікації з громадськістю і зацікавленими сторонами. Механізми протидії інформаційним атакам для органів державної влади в умовах воєнного стану, у свою чергу, передбачають створення кризового комунікаційного центру, підвищення обізнаності персоналу, моніторинг медіа та соціальних мереж, захист важливої інформації, публічність і відкритість, аналіз інформації, співпрацю з міжнародними партнерами, публічні інформаційні кампанії, аналіз суспільного настрою та резервні канали зв'язку. У підсумку, управління кризовими комунікаціями та механізми протидії інформаційним атакам є складним завданням, яке вимагає комплексного підходу та співпраці всіх зацікавлених сторін. Врахування цих аспектів допомагає забезпечити інформаційну безпеку та ефективно реагувати на інформаційні атаки.

ЛІТЕРАТУРА:

1. Crisis Communication. *United Nations : Office of counter-terrorism*. URL: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/unoct-crisis-comms-toolkit-web.pdf

2. Disinformation and Russia's war of aggression against Ukraine : threats and governance responses of 03 November 2022. URL: https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/

3. Information management and communication in emergencies and disasters: manual for disaster response teams / ed. S. Barrantes., M. RodrIguez, R. Pérez. Washington : Pan American Health Organization, 2009. 139 p.

4. Інформаційні війни: проблеми, загрози та протидія. Електронне фахове наукове видання «*Кібербезпека: освіта, наука, техніка*» / З. Бржевська та ін. 2019. Т. 3. № 3. С. 88–96.

5. Критичні комунікації та протидія дезінформації : навчальна програма. URL: https://pdp.nacs.gov.ua/courses/krytychni-komunikatsii-ta-protydiia-dezinformatsii

6. Руденко Т. Аналітична доповідь «Використання антикризових комунікацій органами державної влади у виборчий період: виклики та реагування». Київ : НІСД, 2018. 18 с. URL: https://niss.gov.ua/sites/default/files/2019-02/111Rudenko_Analitichna-zapiska_listopad_-2018_red2-02322.pdf.

7. Семенець-Орлова, І. А. (2015). Державне управління освітніми змінами: наукові категорії, методологія та актуальна проблематика досліджень на основі досвіду України та США. *Університетські наукові записки*. № 1. С. 302–311.

8. Толюпа С., Пархоменко І., Штаненко С. Модель системи протидії вторгненням в інформаційних системах. *Інфокомунікаційні технології та електронна інженерія.* 2021. № 1 (1). С. 39–50.

9. Управління інформаційною безпекою: конспект лекцій : навч. посіб. для студ. спец. 125 «Кібербезпека» / уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. Київ : КПІ ім. Ігоря Сікорського, 2021. 258 с.

10. Bukina N., Ostapchuk S., Sydorchuk N., Melnyk O., Semenets-Orlova I. Demonization of virtual reality in modern media culture. *Research Journal in Advanced Humanities*. 2023. № 4(3).

11. Radchenko O., Kovach V., Radchenko O., Kriukov O., Sydorchuk L., Sharov P., Semenets-Orlova I. (2021). Principles of natural capital preservation in the context of strategy of state environmental safety. In *E3S Web of Conferences.* Vol. 280. P. 09024. EDP Sciences.

12. Semenets-Orlova, I. (2016). Osvita dlya demokraty'chnogo gromadyanstva/osvita z prav lyudy'ny'yak zasib formuvannya kul'tury'gromadyans' kosti [Education for Democratic Citizenship and Human Rights Education as a means of forming of the culture of citizenship]. *Civic competences in vocational education of civil servants and local government officials.* P. 66–87.

13. Shmalenko, I., Yeftieni, N., & Semenets-Orlova, I. (2021, December). Impact of social media influencers on public policy and political discourse. In *International Conference on Social Science, Psychology and Legal Regulation (SPL 2021)* (pp. 88–93). Atlantis Press.