МУДРА Світлана В'ячеславівна,
завідувач кафедри мовної підготовки, кандидат педагогічних наук, доцент, Київський інститут Національної гвардії України
КРУТІКОВ Павло Дмитрович,
слухач магістратури 153 навчальної групи, Київський інститут Національної гвардії України

ПРОФЕСІЙНА МОВНА КОМУНІКАЦІЯ ЯК АСПЕКТ ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ІНФОРМАЦІЙНОЇ АГРЕСІЇ

У сучасному світі інформаційна агресія стає однією з ключових загроз безпеці, особливо в контексті охорони об'єктів критичної інфраструктури. Інформаційні атаки можуть призвести до серйозних наслідків, зокрема порушення роботи інфраструктурних об'єктів і завдання шкоди економіці та суспільству в цілому.

З огляду на значення критичної інфраструктури для нормального функціонування суспільства та економіки, необхідно розглядати питання забезпечення її безпеки в умовах постійного стрімкого розвитку технологій та зростаючих загроз. Інформаційна агресія стає все більшою загрозою для критичної інфраструктури, оскільки вона може бути використана для здійснення широкого спектру атак, від хакерських нападів до дезінформації та маніпуляції інформацією.

Таким чином, дослідження ролі професійної мовної комунікації у забезпеченні безпеки об'єктів критичної інфраструктури є актуальним і важливим з погляду подолання цих викликів і забезпечення стійкості суспільства.

Мета дослідження – виявити чинники ефективності професійної мовної комунікації в забезпеченні безпеки об'єктів критичної інфраструктури.

Мовна комунікація дозволяє правильно ідентифікувати, аналізувати та передавати інформацію про потенційні загрози, а також координувати дії підрозділів у кризових ситуаціях. Крім того, ефективна мовна комунікація з громадськістю та медіа допомагає уникнути паніки та забезпечити раціональну

реакцію на небезпеку[1, с. 14].

Для протидії інформаційній агресії під час охорони об’єктів критичної інфраструктури необхідно вживати комплексних заходів.

Чітко формулювати інструкції та рекомендації: мовна комунікація повинна бути простою та зрозумілою, щоб усі військовослужбовці могли легко розуміти і виконувати вказівки у надзвичайних ситуаціях.

Швидко передавати інформацію: важливо, щоб інформація про поточну ситуацію та необхідні заходи безпеки передавалася оперативно та точно між всіма групами через канали комунікації (телефоном, радіостанцією)

Організовувати збори та наради: проведення зборів і нарад для обговорення поточної ситуації, розроблення планів дій та вирішення проблем допомагає уніфікувати розуміння ситуації та виробити спільні стратегії.

Ефективно керувати підрозділом: використання мовних засобів для мотивування особового складу, підтримки та демонстрації лідерських якостей дозволяє зберегти спокій та ефективність у кризових ситуаціях.

Інформаційна агресія часто передбачає застосування дезінформації та маніпулювання з метою створення паніки або виклику недовіри до державних та комерційних установ[5, р 3, ст 36,]. Це може призвести до порушення громадського порядку та загрози національній безпеці.

Одночасно дезінформація, яка передається через різноманітні канали, зокрема соціальні медіа, сайти новин, телеграм-канали та інші джерела, може суттєво впливати на громадську думку.

Визначимо основні аспекти негативного впливу дезінформації на стабільність суспільства.

Порушення довіри. Поширення неправдивої інформації може призвести до загальної недовіри до урядових структур, правоохоронних органів та інших державних установ. Це може підірвати авторитет влади та спричинити кризу довіри до державних інституцій, що загрожує стабільності суспільства.

Паніка та хаос. Поширення неправдивої інформації може призвести до масової паніки серед населення. Наприклад, чутки про надзвичайні події або загрози

безпеці можуть викликати паніку, що призведе до хаосу та неврівноваженості в суспільстві.

Вплив на економіку. Дезінформація може мати негативний вплив на економічну ситуацію країни. Паніка та недовіра можуть призвести до зниження інвестицій, зростання витрат на зберігання та захист від можливих загроз, а також до втрати довіри до тієї чи іншої установи.

Для протидії інформаційній агресії під час охорони об’єктів критичної інфраструктури необхідно вживати комплексних заходів.

Можна виділити основні напрями такої протидії.

1. Зміцнення кіберзахисту систем:

- розроблення та впровадження сучасних технологічних рішень для захисту критичної інфраструктури від кібератак;

- удосконалення програмного забезпечення та апаратних засобів для виявлення та запобігання кіберзагрозам.

2. Посилення моніторингу та аналізу інформації:

- розвиток систем моніторингу та аналізу для вчасного виявлення потенційних загроз інформаційної безпеки;

- підвищення ефективності реагування на кіберінциденти шляхом швидкого реагування на виявлені загрози.

3. Розвиток відповідних правових інструментів:

- прийняття законодавства, яке визначає відповідальність за кіберзлочинність та інші форми інформаційної агресії;

- створення механізмів правового захисту для об’єктів критичної інфраструктури та їхніх користувачів в інформаційному полі.

4. Міжнародне співробітництво:

- установлення міжнародних стандартів щодо кібербезпеки та обміну інформацією про кіберзагрози;

- спільна робота з міжнародними партнерами з метою координації дій у виявленні та припиненні кібератак.

Отже, можемо стверджувати, що інформаційна агресія становить загрозу для

безпеки об’єктів критичної інфраструктури, але за допомогою ефективних заходів можливо зменшити її вплив та захистити суспільство від негативних наслідків таких атак. Для протидії інформаційній агресії під час охорони об’єктів критичної інфраструктури необхідно вживати комплексних заходів, і ефективність професійної мовної комунікації є одним із вагомих чинників такої протидії.

Список використаних джерел:

1. «ПРОФЕСІЙНА КОМУНІКАЦІЯ: МОВА І КУЛЬТУРА». Житомирський державний університет імені ІВАНА ФРАНКА Матеріали ІІІ Всеукраїнського науково-практичного вебінару 23 листопада 2016 року https://dspace.udpu.edu.ua/bitstream/6789/6117/1/Vebinar_Zhytomyr.pdf

2. ПРОФЕСІЙНА МОВНОКОМУНІКАТИВНА КОМПЕТЕНЦІЯ. Національний університет «Львівська політехніка» Колодій Н. В 2012. – 96 с

3. КОМУНІКАТИВНА БЕЗПЕКА КРИТИЧНИХ ОБ'ЄКТІВ: навчальний посібник. Лазарєв, В. О. Київ: КНТ, 2017.

4. Постанова К М У від 22 .07 2022 р. № 821 «Про затвердження Порядку проведення моніторингу рівня безпеки об’єктів критичної інфраструктури» https://zakon.rada.gov.ua/laws/show/821-2022-%D0%BF#Text

5. ІНФОРМАЦІЙНА БЕЗПЕКА ТА КІБЕРБЕЗПЕКА ДЕРЖАВИ Навчальні посібник. Видавництво: Ліра-К, Титова Н.М., Рідей Н. М., Настрадін В.П., Присяжнюк М. М., Мамченко С. М., Артюх С. В., Яворська Р. О.