Modern Economics. 2025. № 49(2025). С. 124-132. DOI: https://doi.org/10.31521/modecon.V49(2025)-17

ТЕРОРИСТИЧНІ ЗАГРОЗИ ОБ'ЄКТАМ ТЕЛЕРАДІОМОВЛЕННЯ ЯК ФАКТОР СОЦІАЛЬНОЇ ДЕСТАБІЛІЗАЦІЇ

Мельничук Д.В.
Миколаївський національний аграрний університет
kurepin@mnau.edu.ua

Стабільний та надійний інформаційний простір держави відіграє ключову роль у забезпеченні будь яких процесів, включаючи економіку й соціальні процеси суспільства. Інформаційна інфраструктура забезпечує постійний інформаційний потік: передачу, обробку та поширення інформації. Телерадіоканали комунікації формують мовлення для населення держави як на місцевому, так й на державному рівні. Також від них залежить поінформованість населення про стабільність суспільства, про надзвичайні ситуації та координацію дій при загрозах й небезпеках.

Висока залежність суспільства від інформаційних ресурсів підсилює ризики, пов'язані з навмисним ураженням інформаційної інфраструктури. Порушення чи знищення інфраструктури може призвести до масштабних наслідків, якими є дезорганізація управління, поширення паніки та дезінформація [1, с. 327].

Намір порушити стабільність інформаційного простору та вплинути на громадську свідомість зумовлює види терористичних загроз, зокрема різні форми збройних нападів. Блокування роботи телерадіоцентрів має свої характерні особливості. Вони поєднують фізичний вплив (знищення чи пошкодження обладнання) із інформаційними атаками, включаючи поширення дезінформації або маніпулятивного контенту. Таким чином досягається психологічний ефект, зокрема створення паніки, дезорієнтація населення, підрив довіри до офіційних джерел інформації.

Терористичні дії мають і стратегічний характер. Вони здатні викликати значні соціальні наслідки навіть за відносно обмежених фізичних пошкоджень [2, с. 261]. Для таких загроз характерними рисами є: раптовість, високий рівень організованості та використання сучасних засобів впливу, що ускладнює їх попередження та нейтралізацію. Сценарії збройних нападів зазвичай передбачають цілеспрямовані дії, спрямовані на порушення функціонування інформаційної інфраструктури та встановлення контролю за інформаційними потоками. Такі сценарії відбуваються із застосуванням сили або загроз, що дозволяє нападникам швидко дезорганізувати роботу персоналу та систем безпеки.

Ефективність безпеки та запобігання терористичним загрозам потребує комплексного підходу, який поєднує фізичний захист інфраструктури; постійний моніторинг об’єкта; підготовка персоналу; розробка чітких планів реагування тощо. Безпека значно підвищується завдяки впровадженню сучасних технічних рішень, зокрема систем відеоспостереження, сигналізації та автоматизованого контролю. Це дозволяє - своєчасно виявляти потенційні загрози, посилити охорону об'єктів, забезпечити контроль доступу, підготувати персонал до дій в умовах ризику, забезпечити координацію між службами та сприяти мінімізації можливих наслідків.

Отже, захист об'єктів телерадіомовлення від терористичних загроз можливий лише за умови комплексних безпекових заходів та належної підготовки персоналу.

Список використаних джерел

1. Курепін В. М., Курепін Д. В., Іваненко В. С. Цивільний захист: навчальний посібник для здобувачів другого (магістерського) рівня вищої освіти денної та заочної форм здобуття вищої освіти. Миколаїв : МНАУ, 2025. 491 с. URL:https://dspace.mnau.edu.ua/jspui/handle/123456789/20130.

2. Курепін В. М., Самойленко О. О., Бацуровська І. В. Кібербезпека цифрового освітнього середовища як складова системи безпеки праці та життєдіяльності. Суспільство та національні інтереси: журнал. 2025. № 11(19). С 255-268. https://dspace.mnau.edu.ua/jspui/handle/123456789/22584.

РОЛЬ МОНІТОРІНГУ, ВИЯВЛЕННЯ ВТОРГНЕНЬ ТА РЕАГУВАННЯ НА КІБЕРГІНЦИДЕНТИ

Мельничук Д.В.
Миколаївський національний аграрний університет
kypins@ukr.net

В умовах воєнного стану моніторинг та кіберзахист систем оповіщення про загрози для населення набуває критичного значення. Ці системи стають потенційною метою для кібератак, спрямованих на дестабілізацію суспільства. Потрібне цілодобове відстеження стану серверів, каналів зв'язку та програмного забезпечення, які забезпечують передачу сигналів тривоги.

При різкому збільшені мережевого трафіку система моніторингу може виявити ознаки DDoS-атаки на сервер, який відповідає за розсилку повідомлень про повітряну тривогу. Щоб не допустити зриву оповіщення населення автоматично активуються механізми обмеження трафіку або відбувається переключення на резервні канали.

Важливо захистити системи керування від спроб несанкціонованого доступу. Якщо обліковий запис оператора намагаються використати з нетипової геолокації або в незвичний час, система безпеки повинна заблокувати сесію та повідомити адміністратора про потенційний інцидент. Це дозволе запобігти ситуаціям, коли злодії могли б змінити налаштування системи або запустити фальшиві сигнали тривоги.

Елементом кіберзахисту є системи аналізу поведінки користувачів. Вони фіксують відхилення від звичних дій персоналу та сигналізують про можливу компрометацію доступу. Оперативне реагування на кіберінциденти відіграє окрему роль. У разі виявлення шкідливого програмного забезпечення серверні системи оповіщення негайно здійснюють ізоляцію враженого сегмента мережі. Управління переводиться на резервний центр, а відновлення працездатності відбуваються з резервних копій. В умовах воєнного стану, щоб не допустити перерв у передачі критичних повідомлень, такі дії виконуються за лічені хвилини.

Важливим є постійне тестування та удосконалення систем кіберзахисту. Проведення навчальних симуляцій атак дозволяє перевірити готовність персоналу та ефективність алгоритмів реагування. Також впроваджується практика дублювання каналів оповіщення. Інформація передається одночасно через мобільні застосунки, SMS та локальні системи гучномовців, це зменшує ризик повної втрати зв'язку навіть у разі успішної атаки на один із каналів.

При виявленні загроз у системах оповіщення алгоритми дій персоналу починаються з фіксації аномалії, яка може бути як технічною, так і кібернетичною. Дії мають бути чітко регламентованими, відпрацьованими та максимально автоматизованими, оскільки від швидкості та правильності реакції залежить безпека населення.