у сфері утвердження української національної та громадянської ідентичності.

У цілому, позитивно оцінюючи актуальність і необхідність запровадження базової військової підготовки в закладах вищої освіти, вважаємо, що механізм її реалізації повинен бути чітко продуманий та визначений на рівні нормативно-правових актів, які визначатимуть порядок її проведення, з урахуванням у тому числі виявлених нами проблемних аспектів її запровадження.

Список використаних джерел:

1. Проєкт Закону України «Про внесення змін до деяких законодавчих актів України щодо окремих питань проходження військової служби, мобілізації та військового обліку» (реєстр. № 10449 від 30.01.2024). URL : https://itd.rada.gov.ua/billInfo/ Bills/Card/43604. (дата звернення: 03.04.2024).

ГОРЕЛОВ Юрій,
кандидат технічних наук, доцент,
доцент кафедри кібербезпеки та DATA-технологій
Харківського національного
університету внутрішніх справ
(м. Харків, Україна)
ГАБОРЕЦЬ Ольга,
доктор філософії, доцент,
доцент кафедри оперативно-розшукової діяльності та
інформаційної безпеки Донецького державного
університету внутрішніх справ
(м. Кропивницький, Україна)

ІННОВАЦІЙНІ ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ГРОМАДЯН ПІД ЧАС ВОЄННОГО СТАНУ: РОЛЬ ТЕХНОЛОГІЙ ТА КОМУНІКАЦІЙ

У сучасному світі, повному нестабільності та геополітичних напружень, питання забезпечення безпеки громадян у часи воєнного стану є одним із наи більш актуальних та складних завдань. Відтак, необхідність розвитку та впровадження інновацiи них підходів стає нагальною вимогою для ефективного захисту населення.

Ця наукова робота присвячена дослідженню та аналізу ролі технологіи та комунікаціи у забезпеченні безпеки громадян під час воєнного стану. Особлива увага приділяється визначенню новаторських підходів, що дозволяють оптимізувати реакцію на кризові ситуаці та мінімізувати загрози для населення. Зазначении аспект є критичним у зв'язку зі стрімким розвитком технологіи та поширенням інформаціи них засобів, що забезпечують безпосередню зв'язаність та доступність інформаці . Це відкриває нові можливості для швидкого реагування на загрози та координаці діи у воєнних умовах.

Розуміння сучасних технологічних можливостеи та х впливу на забезпечення безпеки громадян у критичних ситуаціях охоплює аналіз широкого спектру інноваціи них технологіи , що включають не лише технічні розробки, а и алгоритмічні підходи та стратегі використання цих технологіи. На першии погляд, важливо

визначити, які саме технологічні інструменти доступні для використання у ситуаціях кризового характеру. Це можуть бути штучнии інтелект, аналіз великих даних, супутникова зи омка, дронова технологія, розробка спеціалізованих програмних продуктів тощо.

Подальше розуміння полягає у вивченні того, як ці технологі можна використовувати для підвищення рівня безпеки громадян. Наприклад, штучнии інтелект може бути використании для аналізу потоків даних зі спутників та інших джерел, для швидкого виявлення аномаліи , які можуть вказувати на потенціи ні загрози. Аналіз великих даних дозволяє виявляти патерни та тренди, що можуть вказувати на ризик для безпеки. Супутникова зи омка та дронова технологія дозволяють здіи снювати моніторинг територіи та динаміки подіи , що важливо для оперативного реагування на кризові ситуаці .

Також необхідно враховувати етичні та правові аспекти використання цих технологіи , а також х взаємодію з існуючими структурами та системами безпеки. Важливо забезпечити, щоб впровадження нових технологіи не порушувало приватність громадян та не створювало нові ризики або вразливості.

Визначення новаторських підходів у контексті забезпечення безпеки громадян у кризових ситуаціях передбачає комплекснии аналіз і розробку передових стратегіи , спрямованих на оптимізацію реакці на кризові ситуаці та мінімізацію х впливу на населення. Ці

підходи базуються на використанні передових наукових теоріи , концепціи та технологіи з метою розробки ефективних та інновациі них методів захисту населення в умовах надзвичаи них ситуациі . Наукове обґрунтування новаторських підходів включає аналіз актуальних досліджень та розробок у галузі безпеки та кризового управління. Цеи аналіз дозволяє виявити наи ефективніші методи та стратегі , що базуються на відомих принципах і теоріях у сферах психологі , соціологі , інженері та інших галузях.

Зокрема, науковии підхід передбачає використання теоріи кризового управління та ризик-орієнтованого підходу для розробки стратегіи прогнозування, попередження та реагування на кризові ситуаці . Також враховується інновациі нии потенціал сучасних технологіи , зокрема штучного інтелекту, аналізу великих даних, інтернету речеи та інших інструментів, які можуть значно підвищити ефективність заходів безпеки та реагування на кризові ситуаці .

Досягнення передово науки та технологіи дозволяють розробляти и впроваджувати інновациі ні підходи до забезпечення безпеки, що базуються на комплексному підході до аналізу та використанню наукових знань і технологіи . Такии підхід є ключовим для постіи ного вдосконалення систем захисту населення в умовах надзвичаи них ситуациі та мінімізаці загроз для громадсько безпеки. Використання передових технологіи

та ефективних систем комунікаціи може значно підвищити рівень безпеки в умовах воєнного конфлікту. Впровадження нових підходів, заснованих на інноваціи - них технологіях, дозволить швидше та ефективніше реагувати на кризові ситуаці та зменшити х наслідки для населення.

Отже, результати цього дослідження підтверджують необхідність та перспективність впровадження новаторських підходів у сфері забезпечення безпеки громадян у період воєнного стану. Вони мають великии потенціал для захисту населення та збереження життів у наи складніших ситуаціях.

ГРИЩЕНКО Денис,
підполковник поліції,
старший викладач кафедри
протидії кіберзлочинності Харківського
національного університету внутрішніх справ
(м. Харків, Україна)
МАЛЕНЮК Михайло,
курсант 3 курсу факультету № 4 Харківського
національного університету внутрішніх справ
(м. Харків, Україна)

ПРОБЛЕМАТИКА ПІДГОТОВКИ КАДРІВ ДЛЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

На сьогодні інциденти в кіберпросторі відбуваються у всіх секторах економіки та повсякденному житті. Кібербезпека нині нерозривно пов'язана з проявами