БЕЗПЕКА В ЦИФРОВОМУ ПРОСТОРІ В УМОВАХ ВОЄННОГО СТАНУ

Артур ВОЛОБОЄВ

У період стрімкого технологічного розвитку і високоінтегрованого віртуального середовища безпека в цифровому просторі стає ключовою складовою національної та міжнародної стабільності. З поширенням кіберзагроз та кібератак формується новий вимір – вимір цифрової вразливості та високотехнологічних загроз. У цьому контексті розуміння та вирішення питань кібербезпеки стають першочерговим завданням для забезпечення національної безпеки та захисту стратегічних інтересів держави в умовах можливих агресивних дій.

Сучасні конфлікти виявляються у вигляді гібридної війни, де кіберпростір стає важливим полем боротьби, а втручання в інформаційні системи – стратегічним інструментом ведення військових дій. Провідні світові держави розглядають кіберпростір як ключовий бойовий театр, що потребує інноваційних та надійних стратегій кіберзахисту, особливо в умовах воєнного стану.

Цифрові загрози під час воєнного конфлікту не обмежуються тільки аспектами військових операцій, а мають глибокий економічний, політичний та соціокультурний вплив. Розгортання кіберзброї вимагає від держав розробки комплексних стратегій, що поєднують технічні інновації, правові регулювання, етичні норми та організаційні кадрові заходи. З огляду на це, обговорення безпеки в цифровому просторі в умовах воєнного стану набуває наукового та стратегічного значення, адже вимагає розуміння інтердисциплінарного характеру викликів та пошук інтегрованих рішень для забезпечення національної та міжнародної стійкості в умовах важливих геополітичних та кібернетичних змін.

Актуальність теми безпеки в цифровому просторі в умовах воєнного стану визначається низкою ключових факторів. По-перше, швидкі темпи цифрової трансформації призводять до зростання кількості цифрових інфраструктур, що стають жертвою можливих кібератак під час воєнних конфліктів. По-друге, збільшення кількості кіберзагроз та розвиток кіберзброї, що може ефективно використовуватися у військових операціях, ілюструє тенденцію виникнення конфліктів, де кіберфронт стає важливим стратегічним фактором.

У світлі цих тенденцій слід розуміти, як сучасні держави можуть впоратися з викликами, що постають внаслідок цифрової залежності, коли інформаційні системи та мережі визначаються об'єктами кібернетичного вторгнення. Активізація кіберзагроз та їх використання в умовах воєнного стану може мати серйозні наслідки для національної безпеки, економіки, інфраструктури та соціального порядку.

Усвідомлюючи важливість виявів сьогодення, наукова та практична діяльність кафедри оперативно-розшукової діяльності та інформаційної безпеки Донецького державного університету внутрішніх справ спрямована на вивчення, аналіз та вирішення сучасних проблем, пов'язаних з кібербезпекою в умовах воєнного стану. Кафедра активно залучає здобувачів вищої освіти та професорсько-викладацький склад до наукових досліджень у галузі кібербезпеки та розробки практичних заходів з вирішення завдань оперативно-розшукової діяльності.

Однією з основних сфер діяльності науково-педагогічних працівників є розробка та вдосконалення методів кіберзахисту, зокрема в умовах ведення воєнних конфліктів. Дослідницькі роботи охоплюють аналіз сучасних тенденцій у сфері кібербезпеки, а також удосконалення методів виявлення та реагування на кібератаки.

Кафедра також забезпечує навчання курсантів та студентів основам інформаційної безпеки та кіберзахисту в рамках навчальних дисциплін як загального, так й практичного спрямування. Викладачі та студенти активно співпрацюють з представниками силових відомств та інших організацій, що займаються кібербезпекою, для обміну досвідом та розвитку спільних проєктів у сфері оперативно-розшукової діяльності та захисту інформації в умовах воєнного конфлікту.

Кафедра відіграє важливу роль у вивченні та практичному впровадженні заходів з кібербезпеки, сприяючи розвитку не лише наукового напряму, але й формуванню висококваліфікованих фахівців, готових ефективно впоратися із сучасними викликами в цифровому просторі.

Отже, загальний вектор роботи спрямований на ефективність забезпечення безпеки в цифровому просторі в умовах воєнного стану:

на налагоджування взаємодій та безперервного обміну з практичними працівниками, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки;

своєчасність та оперативність реакцій на отриману інформацію як від державних, так і міжнародних партнерів;

проведення систематичного, залежного від постійно змінюваної оперативної обстановки в цифровому просторі, аналізу ризиків та прогнозування змін структури та характеру підготовки, організації та вчинення кіберзлочинів;

визначення заходів і механізмів, спрямованих на недопущення витоку інформації, а також запобігання несанкціонованому доступу до неї сторонніх осіб;

системне і на постійні основі забезпечення навчання та підвищення кваліфікації професорсько-викладацького складу, здобувачів вищої освіти та практичних працівників, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, з урахуванням питань викори-

стання сучасних підходів, міжнародного досвіду та методів самостійного опрацювання первинних даних та іншої інформації.

Указане також визначає джерела для прийняття якісних управлінських рішень з дослідження та впровадження окресленої тематики задля зменшення та нейтралізації ризиків і загроз протиправної активності, що дозволить забезпечити безпеку держави й громадян в цифровому просторі.