# КІБЕРРИЗИКИ ПІД ЧАС ВОЄННИХ ДІЙ

**Кравцова Людмила Володимирівна**
*ORCID ID: 0000-0002-0152-635X*
канд. техн. наук, доцент,
доцент кафедри інноваційних технологій та технічних засобів судноводіння
*Херсонська державна морська академія, Україна*

**Камінська Наталія Геннадіївна**
*ORCID ID: 0000-0002-9975-7403*
викладач кафедри інноваційних технологій та технічних засобів судноводіння
*Херсонська державна морська академія, Україна*

Ворог прийшов на нашу землю. Він знищує наші міста, нашу культуру, наше надбання у всіх напрямках. Для нього немає нічого святого. В більшості з них немає мети, немає мотивації, крім тотального знищення нашої держави, ну якщо тільки добре підзаробити навіть пограбуванням українського населення. Він використовує для цього будь-які засоби, у тому числі кібератаки на інфраструктуру та на населення України.

Ворожі спеціалісти з інформаційних технологій перехоплюють розмови звичайних громадян, завдяки цьому відстежують важливу для них інформацію. Нам здається, що наша розмова з друзями чи родичами не несе ніякої корисної інформації для ворога або злочинця. Але це не так. Навіть маленький натяк на щось, що може бути використано злочинцями, може спричинити дуже негативні наслідки. Це стосується не тільки особистого захисту. Нажаль, на даний момент є приклади реального використання ворогом інформації з соціальних мереж. Так, бажання поділитися відзнятим вами відео може допомогти ворогові корегувати цілі обстрілу, розстановку техніки та безпосередньо військових. Вся ця інформація може бути передана за допомогою сучасних засобів зв'язку, а значить, безпосередньо пов'язана з кібернебезпекою в широкому сенсі цього слова.

Кібератаки з боку російських загарбників, спрямовані на знищення нашої країни, у той же час наносять великої шкоди глобальним структурам, як, наприклад, це трапилося з польською залізницею, з метою завадити переміщенню вимушених переселенців з України. Злочинцям байдуже, що це лише жінки та діти, які втекли з рідного міста, втративши все що мали.

На цю проблему звернув увагу Євросоюз, який хоче посилити заходи кібер- та інформаційної безпеки у своїх установах. Про це заявив член ЄК з бюджету та адміністративних питань Йоганнес Хан, передає Інтерфакс-Україна. За його словами, у сучасному взаємопов'язаному середовищі якийсь єдиний інцидент у галузі кібербезпеки може завдати великої шкоди цілій організації. В ЄК вказують на те, що контекст пандемії COVID-19 та наростаючі геополітичні виклики підтвердили необхідність загального підходу в ЄС до кібер- та інформаційної безпеки. Тож Єврокомісія запропонувала відповідні єдині регламенти.

Такий же точки зору притримується і Міжнародна морська організація (ІМО), яка розробила та прийняла ряд документів з кібербезпеки [1]. Ці документи зобов'язують адміністрацію забезпечити належний розгляд кіберризиків в системах управління безпекою. Морська галузь потребує фахівців, які б могли на належному рівні контролювати ситуацію на всіх об'єктах, на які може бути спрямована кібератака ворога. Тому керівництво Херсонської державної морської академії

прийняло рішення внести в навчальний план підготовки курсантів дисципліну «Кібербезпека на морських суднах», метою якої є всебічна інформованість здобувача освіти про міжнародні норми кібербезпеки на морському транспорті, джерела кібернебезпеки, сучасні загрози інформаційній безпеці, стійкість суднових систем та інфраструктури, управління кібербезпекою, бортові мережі та багато інших важливих питань, відповіді на які надає вивчення вказаного курсу. Створенню програми і контенту курсу передувала велика кількість обговорень всіх проблем як на випускаючих кафедрах з активною участю викладачів – діючих капітанів, суднових механіків та інших спеціалістів, так і на нарадах за участю керівництва академії.

Викладачі академії, які взяли на себе відповідальність за підготовку курсу, не зупинилися лише на зборі на структуризації інформації щодо кібербезпеки на морських суднах. Маючи великий досвід наукових досліджень, вони провели детальний аналіз джерел кібернебезпеки, пов'язаних з проблемою впливу людського фактору у цієї сфері. Було виявлено, що деякі людські якості, навмисно чи ні, можуть фатально вплинути на безпеку судна. На підставі результатів досліджень показників кібератак, здійснених саме завдяки впливу людського фактору, було побудовано математичну модель ймовірнісного опису розглянутого процесу, яка спирається на властивості так званих ланцюгів Маркова [2]. Результатом роботи є створення матриці ймовірностей появи кібератаки з боку того чи іншого джерела. Це надає можливість попередити деякі кібератаки, пов'язані з впливом людського фактору, тим самим збільшити рівень кібербезпеки суднових систем.

## Список використаних джерел:

1. Резолюція MSC.428(98) «Управління морськими кіберризиками в системах управління безпекою» http://rise.odessa.ua/texts/MSC428_98.php3
2. Турчин В.М., Турчин Є.В. Марковські ланцюги: Основні поняття, приклади, задачі: Навч. посіб. для студентів вищих навчальних закладів. — Дніпро: ЛізуновПрес, 2017. — 212 с.