НАТО на 2017 рік» від 8 квітня 2017 р. № 103/2017 [5], визначено: удосконалення системи військового управління та зв'язку; удосконалення систем матеріально-технічного та медичного забезпечення ЗСУ; підтримання у боєздатному стані, модернізація і оновлення озброєння та військової техніки; підвищення ефективності системи кадрового менеджменту; удосконалення системи військової освіти та підготовки професійних кадрів; удосконалення системи підготовки військ та забезпечення їх взаємосумісності; забезпечення соціального захисту військовослужбовців та членів їх сімей.

Отже, за результатами двадцятирічної співпраці між Україною та НАТО можна зробити висновок, що проведення реформування ЗСУ на основі стандартів НАТО – це справа не одного року. Запровадження стандартів НАТО в діяльність ЗСУ не повинно розглядатися як основна ціль реформування ЗСУ або як одна з обов'язкових вимог для вступу до Північноатлантичного альянсу, реалізація їх вимог є лише одним з обов'язкових кроків на шляху до створення в нашій державі сучасної, професійної армії, здатної забезпечити досягнення цілей Воєнної доктрини України.

1. Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України»: Указ Президента України від 24 вересня 2015 р. № 555/2015. *Офіційний вісник України*. 2015. № 78. Ст. 2592.

2. Мукосий С. О внедрении стандартов НАТО. URL: https://defence-ua.com/index.php/statti/296-sergej-mukosij-segodnya-ministerstvo-oborony-yavlyaetsya-lokomotivom-sredi-vsekh-organov-vlasti-po-vnedreniyu-standartov-nato

3. Романенко Є. О. Реформування Збройних Сил України за стандартами НАТО. *Публічне урядування*. 2016. № 3. С. 142–150.

4. У Збройних Силах України впроваджено стандарт НАТО щодо медичної евакуації. URL: http://www.milnavigator.com/uk/v-vooruzhennyx-silax-ukrainy-vnedren-standart-nato-po-medicinskoj-evakuacii-zamestitel-ministra-oborony-ukrainy/

5. Про затвердження Річної національної програми під егідою Комісії Україна-НАТО на 2017 рік: Указ Президента України від 8 квітня 2017 р. № 103/2017. *Офіційний вісник України.* 2017. № 32. Ст. 990.

Поливанюк Василь Дмитрович,
старший викладач кафедри
тактико-спеціальної підготовки
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, доцент,
полковник поліції

УКРАЇНА ТА НАТО: РОЗВИТОК МІЖНАРОДНОЇ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ

Інформація взагалі та знання зокрема є вирішальними факторами, які впливають на розвиток технології і технологічних ресурсів людства. Власне вони визначають кордони технологій та можливості в освоєнні природи і подальшого розвитку суспільства. Саме ключові революційні винаходи у галузі

інформатики відкривали нові можливості та надавали поштовху до розвитку великих технологічних революцій.

Бурхливий розвиток інформаційно-комунікаційних технологій в останні два десятиліття вплинув на міжнародні відносини. Ці технології стали застосовуватися не лише як засіб обміну та обробки інформації, але і як інструмент для заподіяння шкоди. В останні кілька років терміни з приставкою «кібер» отримали поширення в міжнародно-політичному дискурсі і знайшли своє відображення у стратегічних доктринах не лише окремих держав, але й міжнародних організацій, зокрема НАТО.

К. Гірз, представник США в Центрі кібероборони НАТО, зазначає, що термін «кібер» використовується стосовно до комп'ютерів, інформаційних мереж і цифрової інформації.

Ядром «проблемного поля» інформаційної безпеки є визначення того, якими є природа і деструктивний потенціал інформаційних загроз. П. Корніш з лондонського Королівського інституту закордонних справ наводить таку класифікацію інформаційних загроз: 1) діяльність хакерів-одинаків; 2) організована злочинність, яка діє в глобальних інтернет-мережах; 3) ідеологічний і політичний екстремізм; 4) інформаційна агресія, яку проводить держава.

Як підкреслюють вчені-криміналісти України, у вітчизняній криміналістичній науці все ще не існує чіткого визначення поняття комп'ютерного злочину, дискутуються різні точки зору по їх класифікації. Складність у формулюваннях цих понять існує як внаслідок неможливості виділення єдиного об'єкта злочинного посягання, так і множинності предметів злочинного посягання з точки зору їх кримінально-правового значення.

На наш погляд, під комп'ютерною злочинністю слід розуміти суспільно небезпечну діяльність чи бездіяльність, яка здійснюється з використанням сучасних інформаційних технологій і засобів комп'ютерної техніки з метою спричинити збитки майновим або суспільним інтересам держави і громадянам, а також правам особи.

Експерти з Центру кіберзахисту НАТО розглядають мілітаризацію Інтернету в якості одного з головних і найбільш небезпечних трендів розвитку світового кіберпростору, зазначаючи, що сучасні військові структури готові використовувати інформаційний простір як «паралельне поле битви» в конфліктах майбутнього. При цьому висловлюється впевненість у тому, що проведення кібератаки «в чистому вигляді» малоймовірне. Більш вірогідним є сценарій, при якому агресивні акції в кіберпросторі будуть використовуватися для посилення ефекту традиційних операцій із застосуванням звичайних наступальних озброєнь. Саме така формула – звичайні озброєння плюс кіберзброя – лежатиме в основі стандартних оперативних і стратегічних дій в майбутніх конфліктах.

Сприйняття кіберзагроз було відображено у Стратегічній концепції НАТО, прийнятій на саміті в Лісабоні в листопаді 2010 року. У даній концепції інформаційні атаки фігурують у ряді найбільш небезпечних викликів і загроз безпеці і процвітанню держав-членів Альянсу. В ієрархії викликів, представ-

леній в даній концепції, проблема загроз у сфері інформаційного простору знаходиться відразу після поширення зброї масового знищення і тероризму.

В цілому питання забезпечення кібербезпеки включають в себе об'ємний комплекс проблем, серед яких фігурують загрози, що розрізняються за своїми джерелами і мотивами. Важливим фактором є відсутність у міжнародно-правового консенсусу щодо того, що розуміти під термінами «кібервійна», «кібератака», «кібертероризм» або «критично важлива інформаційна інфраструктура».

Термін «кіберзлочинність» вперше з'явився в американській, а потім і в іншій зарубіжній пресі на початку 60-х років, коли були виявлені перші випадки злочинів, вчинених з використанням електронних обчислювальних машин. Це явище посилюється не тільки в локальному, національному, а й у глобальному масштабі.

Перші спеціальні закони по боротьбі з комп'ютерною злочинністю були прийняті в 1973 році у Швеції і в 1976 році у США на федеральному рівні. Склади злочинів у сфері інформаційних технологій (комп'ютерних злочинів) були сформовані в 1979 році на Конференції американської асоціації адвокатів у Далласі, до яких увійшли: використання або спроба використання комп'ютера, обчислювальної системи або мереж комп'ютерів з метою отримання грошей, власності або послуг шляхом прикриття фальшивими кодами або видання себе за іншу особу; умисна несанкціонована дія, що має за мету зміну, пошкодження, знищення або викрадення комп'ютера, обчислювальної системи, комп'ютерної мережі або систем математичного забезпечення, що містяться в них, програм або даних; умисне незаконне порушення зв'язку між комп'ютерами, обчислювальними системами або комп'ютерними мережами. Згодом у багатьох країнах світу затверджено законодавчі акти стосовно цієї категорії злочинів.

Вперше питання про забезпечення кібербезпеки організації з'явилися в політичному порядку денному НАТО на саміті у Празі в листопаді 2002 р., коли лідери країн Альянсу висловили готовність посилювати можливості з надання протидії інформаційним атакам.

Проблема забезпечення безпеки інформаційних технологій і систем НАТО і його членів має, окрім питань технічного забезпечення та стратегічного планування, ще й політичний вимір.

Сьогодні Україна знаходиться перед проблемою подальшого розвитку сучасних біо- та інформаційних технологій, телекомунікаційних систем, інформатизації суспільства. Майбутнє як національної, так і глобальної інформаційної безпеки буде залежати від того, якою мірою держави проявлять волю до конструктивної співпраці у вирішенні нагальних проблем інформаційної безпеки, оскільки Інтернет не визнає державних кордонів, то і зусилля щодо забезпечення його безпеки повинні бути міжнародними.