КОЗЬМІНИХ АЛЬОНА ВІТАЛІЇВНА

Національний університет «Одеська юридична академія»,
доцент кафедри політичних теорій, кандидат політичних наук, доцент

КІБЕРБЕЗПЕКА ТА КІБЕРАТАКИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Одним з головних інструментів політики, міжнародної політики зокрема, є – інформація. Спотворення інформації посилює напруженість, особливо в умовах гібридних війн та змінюють сприйняття фактів відповідно до уподобань акторів, які прагнуть вплинути. Варто відзначити, що досягнення в галузі цифрових медіа, скасування інформаційних меж, залишають країни відкритими та вразливими для втручання у їхній політичний та інформаційний простір з боку інших держав [2, p. 27]. Інформаційний простір впливає на економічні, політичні та культурні процеси, на розвиток військової справи та технології. З прискореним переходом на цифрові системи управління зросла загроза кібербезпеці, адже Україна завжди була серед стратегічних цілей зовнішньої політики Росії серед інших країн, тому прагнемо забезпечити кібербезпеку.

Кібербезпека в умовах гібридної війни набуває особливої важливості, оскільки сьогодні вже практично неможливо уявити собі жоден об'єкт технологічної інфраструктури, який не був би оснащений різними програмними комплексами, багато з яких мають вихід у мережу Інтернет, що несе серйозні ризики.

Кібератаки можуть бути використані як допоміжний засіб у рамках інформаційної війни, з метою злому закритих даних та їх опублікування або «вкидання» фейкової інформації, в т. ч. з посиланням на джерела, що вселяють довіру. Все це змушує по-новому дивитися на проблему кібербезпеки, особливо коли йдеться про небезпечні об'єкти чи системи забезпечення життєдіяльності.

Загрози в кіберпросторі є найбільш серйозними для національної безпеки України. Кібербезпека зараз ключова проблема в економічному, політичному, соціальному та військовому аспектах. Тим не менш, вона залишається найменш зрозумілою та найбільш недооціненою загрозою. Тому потрібно розуміти, що кіберпростір в даний час є найважливішим театром бойових дій. Боротьба за кібер-домінування – і відповідно здатність протистояти кібератакам – означає нову еру військових відносин, яка суттєво змінить природу та структуру збройних сил. Також слід відзначити, що кібербезпеки не можна досягти на рівні держави. Вона потребує інтеграції зусиль і приватного сектору, і підприємств, міжнародної координації та співпраці у безпрецедентних масштабах.

Більше того, кіберпростір є ідеальним полем для асиметричної війни. Окремих людей чи групи залучають дуже низька вартість і щодо низький рівень технічної підготовки, необхідний проведення атак на

важливі урядові, економічні, фінансові та військові об'єкти. У 2008 році, напередодні нападу Росії на Грузію із застосуванням звичайної зброї, серія кібератак вивела з ладу грузинські урядові, медійні та військові об'єкти, показавши «обличчя майбутніх війн» [1].

Російсько-українська війна з початку повномасштабного вторгнення продемонструвала, що кібератаки агресора співпадають з воєнними діями, тобто захопленням або руйнуванням об'єктів критичної інфраструктури. Відзначимо, що Росія використовувала хакерські кампанії для підтримки свого повномасштабного наступу на Україну, поєднуючи шкідливе програмне забезпечення з ракетами в кількох атаках, у тому числі на телевізійні станції та державні установи.

Вважаємо, що важливу роль у створенні ефективної системи кібербезпеки має підготовка відповідних фахівців у нашому випадку у військовій, політичній, промисловій сферах, адже однією з головних проблем забезпечення кібербезпеки в Україні є недостатній професіоналізм – навіть за наявності передових технологій країна досі відчуває брак відповідних спеціалістів. З огляду на ситуацію України важко протистояти кібератакам, які застосовує Росія. Так завдяки активній діяльності проєвропейських сил та за конструктивної підтримки зовнішніх гравців Україні вдається протистояти РФ.

На даний момент потрібно більше зосереджувати увагу на: підвищення захищеності критичної інформаційної інфраструктури та стійкості її функціонування, розвиток механізмів виявлення та попередження кіберзагроз та ліквідації наслідків їх прояву, підвищення захищеності громадян та територій від наслідків надзвичайних ситуацій, спричинених інформаційно-технічним чи військовим впливом на об'єкти критичної інформаційної інфраструктури. Певна річ, захист критичних галузей, які функціонують на базі широко розповсюджених інформаційних систем, наприклад телекомунікацій або охорони здоров'я, також має приділятися значна увага, але, на нашу думку, сучасні засоби забезпечення кібербезпеки при грамотному їх використанні здатні значно знизити ризики, що виходять від самих різних загроз: починаючи від звичайних шкідливих програм і до складних таргетованих атак. У промислових інформаційних системах ці методи просто непридатні через безліч причин.

Список використаних джерел:

1. Шрайер Ф., Викс Б., Винклер Т. Х. Кибербезопасность: дорога, которую предстоит пройти. *DCAF Horizon*. 2015. Working Paper No. 4.RU.
2. Melykh O., Korbut A. Entertainment media in the context of hybrid war in the post-Soviet countries: the case of Ukraine. *Economic Annals-XXI.* 2020. Vol. 182(3–4). P. 25–33. URL: http://ea21journal.world/index.php/ea-v182-03/

Ключові слова: інформація, кіберпростір, кібербезпека, кібератака, інформаційна інфраструктура.

Key words: information, cyberspace, cybersecurity, cyber attack, information infrastructure.