**Оксана ШЕЛОМОВСЬКА**
доцент кафедри соціології
Дніпровського державного
технічного університету
(м. Камянське Дніпропетровської обл.),
кандидат наук з державного
управління, доцент

## КІБЕРАРМІЯ: МІСЦЕ І РОЛЬ ГРОМАДСЬКОСТІ

Відповідно до чинного законодавства України кібербезпека цілком справедливо визначена складовою національної безпеки, а отже стратегічне управління нею здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України. В її складі функціонує Національний координаційний центр кібербезпеки, що здійснює координацію та контроль за діяльністю суб'єктів сектора безпеки і оборони, котрі забезпечують кібербезпеку [1]. Державна служба спеціального зв'язку та захисту інформації України є органом зі спеціальним статусом, що розробляє комплексну систему кіберзахисту стратегічних об'єктів і опікується компаніями, котрі проводять аудит стратегічних об'єктів. У своєму підпорядкуванні вона має Державний центр кіберзахисту, підрозділ якого CERT-UA являє собою урядову команду реагування на комп'ютерні надзвичайні події і здійснює моніторинг та виявлення потенційних кіберзагроз. Однак, як зрозуміло з вищесказаного, ця система побудована з метою захисту від кібератак, але повноважень проводити якісь активні дії не має. Такі повноваження мають бути у кібервійська.

У Стратегії кібербезпеки України від 2021 р. зазначається, що до завдань кібервійська належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, що зараховує виведення з ладу критично важливих об'єктів інфраструктури противника шляхом руйнування інформаційних систем, котрі управляють такими об'єктами. При цьому передбачається, що для подальшої розбудови національної системи кібербезпеки на засадах стримування, кіберстійкості, взаємодії, крім основних суб'єктів національної системи кібербезпеки, має бути залучено більш широке коло учасників, у тому числі суб'єктів господарювання, громадських об'єднань та окремих громадян України [3].

Вперше про необхідність створення кібервійська було згадано у нормативному полі в Указі Президента України № 446/2021 від 26.08.2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про невідкладні заходи з кібероборони держави»». Згідно з цим указом кібервійська мають бути невідклано створені у складі Міністерства

оборони України для захисту суверенітету держави, забезпечення її обороноздатності, запобігання збройному конфлікту та відсічі збройній агресії у кіберпросторі. Для цього потрібно було визначити обсяг матеріально-технічних та фінансових ресурсів, необхідних для створення та забезпечення належного функціонування кібервійськ та комплектування особового складу кібервійськ з урахуванням оптимального співвідношення [2]. Передбачалося, що більш детально повноваження і функції кібервійськ мають бути визначені в законопроєкті, котрий Кабінет Міністрів України мав розробити протягом двох місяців і внести на розгляд Верховної Ради України. У листопаді 2021 р. Міністерство оборони України повідомило, що підготувало такий проект, проте його подальша доля на сьогодні невідома.

Фактично створення українського кібервійська було викликано повномасштабним вторгненням, і Україна стала, напевно, однією з перших у світі країн із кіберармією. І відбулося це лише завдяки активній участі громадськості. 26 лютого 2022 р. Міністр цифрової трансформації М. Федоров оголосив своєрідну «повну мобілізацію» спеціалістів ІТ-сектора країни і створення дієвої кіберармії як групи фахівців, що спеціалізується на виконанні операцій у кіберпросторі. Зазвичай до її складу входять кібербійці різних напрямів, кібербезпекові експерти, кібераналітики. Кіберармії можуть виконувати різноманітні завдання, такі як захист від кібератак, проведення кіберспостереження та кібершпигунство, розробка та застосування кіберзброї, а також ведення кібероперацій у межах кібервійни.

У кіберпросторі проблематично не просто здійснити розмежування державних та недержавних акторів, комбатантів та некомбатантів. В українському варіанті кіберармія об’єднала у свої лави не лише працівників ІТ-сфери, а й багато активних пересічних громадян, які у перші місяці війни брали участь у атаках на російські цифрові ресурси. Для того, щоб стати кібербійцем, достатньо лише приєднатися до телеграм-каналу ІТ-армії і виконувати завдання, що там публікуються. Лише протягом кількох днів існування канал суттєво зріс, і на початку березня 2022 р. в ньому було вже понад 276 тисяч підписників (кібервоїнів). Хоча через рік після початку повномасштабного вторгнення кількість підпісників знизилася до 196 тис.

По суті українська кіберармія стала аналогом територіальної оборони в кіберпросторі, діяльність якої полягає в нанесенні ударів по цифровій інфраструктурі ворога. Основними завданнями «солдатів» кіберармії України є масовані DDoS-атаки, зломи сайтів та інформаційних ресурсів країни-агресора, зокрема основних джерел пропаганди; атаки на цифрові ресурси основних банків рф, паралізація роботи онлайн торгових майданчиків, зрив документообігу підприємств. Дійсно, українським кіберфахівцям вдалося досягнути значних успіхів, серед яких: зламані офіційні та стратегічні вебсайти РФ, поширення на цифровому телебаченні в рф правди про війну в Україні, блокування російських ресурсів, що поширювали неправду та пропаганду.

Проведеним нами соціологічним дослідженням було встановлено, що 88,5% опитаних респондентів добре обізнані про створення кіберармії України. Оцінки її діяльності дещо різняться, хоча й є здебільшого позитивними. Виявлено, що 33,8% оцінюють діяльність українського кібервійська однозначно позитивно, і 39,2% – швидше позитивно. Негативні оцінки є вкрай рідкими і зустрічаються лише у 2,7%. Обумовлено це, на нашу думку, недостатньою обізнаністю респондентів у цій сфері і специфічним характером діяльності кібервійська.

Створення і активна діяльність кіберармії України продемонстрували, що в умовах глобальної катастрофи багато ІТ-спеціалістів високого рівня є патріотами своєї країни і готові захищати її на своєму фронті без особистої матеріальної вигоди. Навіть пересічні громадяни, не маючи відповідної освіти та досвіду, активно долучаються до DDoS-атак проти ворога на волонтерських засадах. Отже, ефективна протидія загрозам національній безпеці у кіберпросторі можлива лише за умови акумулювання всього потенціалу держави і громадськості, і ефективна діяльність української ІТ-армії це наочно доводить.

**Список використаних джерел**

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про невідкладні заходи з кібероборони держави» : Указ Президента України від 26.08.2021 № 446/2021. URL : https://zakon.rada.gov.ua/laws/show/446/2021#Text.

3. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL : https://zakon.rada.gov.ua/laws/show/447/2021#Text.

**Володимир ГОРБЕНКО**
студент
***Науковий керівник:***
доцент кафедри соціології, к. н. з держ. упр., доц. **Оксана ШЕЛОМОВСЬКА**
*(Дніпровський державний технічний університет, м. Кам'янське Дніпропетровськохї обл.)*

## ЧЛЕНСТВО В МОЛОДІЖНИХ ГРОМАДСЬКИХ ОРГАНІЗАЦІЯХ: СОЦІОЛОГІЧНИЙ АСПЕКТ

Громадська організація являє собою одну з організаційно-правових форм громадського об'єднання, тобто добровільного об'єднання фізичних осіб для здійснення та захисту прав і свобод, задоволення суспільних,