

Пилипчук Я. В.,

доктор історичних наук,
старший науковий співробітник
відділу наукового інформаційно-аналітичного супроводу освіти
Державної науково-педагогічної бібліотеки України
ім. В. О. Сухомлинського,
м. Київ, Україна
ORCID ID: 0000-0002-9809-3166
pylypchuk.yaroslav@gmail.com

Розвиток кіберпсихології в умовах повномасштабної російсько-української війни: інформаційно-аналітичний супровід

У межах дослідження «Інформаційно-аналітичний супровід психологічної освіти у воєнний і повоєнний періоди» відділу наукового інформаційно-аналітичного супроводу освіти Державної науково-педагогічної бібліотеки України ім. В. О. Сухомлинського кіберпсихологія у контексті війни РФ проти України є складовою частиною психологічної науки на сучасному етапі, а її актуальність є беззаперечною. Цифровий простір України мають захищати кіберполіція та кібервійська, що провокує забезпечення інформаційно-аналітичного супроводу підготовки військових психологів у цьому контексті. Особливо важливим є запровадження дисципліни «Кіберпсихологія» в закладах вищої освіти. Виклики війни проти Росії змушують Україну оперативно реагувати на загрози для громадян України у Кіберпросторі.

Ключові слова: кіберпсихологія, кіберполіція, кібервійська, Україна, війна, кіберпростір, військова психологія, підготовка військових психологів.

Повномасштабна війна Росії проти України поставила перед населенням України нові виклики. Війна ведеться не тільки на полі бою, а й у кіберпросторі. Звичним стало використання безпілотників під час зіткнення на лінії вогню. Стали легендарними «Птахи Мадяра» під керівництвом Роберта

Броді. Безпілотники турецького виробництва Bayraktar зіграли велику роль у збройних зіткненнях 2022 року. Україна також контратакує Росію, завдаючи ударів по об'єктах російської військової та цивільної інфраструктури. Для протидії ворожим безпілотникам використовуються засоби РЕБ.

Вразливими є органи державної влади та державні установи, чії комп'ютери можуть бути вражені російськими хакерами. Ця проблема ускладнюється тим, що на більшості комп'ютерів стоїть неліцензійні комп'ютерні програми, які діставали з Інтернету. Можливі масовані DDOS атаки на сайти українських державних установ.

У контексті інформаційної війни необхідно згадати і про кіберпсихологію. Важливо наголосити на розумінні понять «кібербезпека» та «інформаційна гігієна». Українська держава має адекватно відповідати на загрози для неї в цифровому просторі.

Кібербезпека – це комплекс процесів, практичних порад і технологічних рішень, які допомагають захищати важливі системи й мережу від кібератак. Оскільки об'єм даних збільшується й усе більше користувачів працює і спілкується звідусіль, кіберзлочинці розробляють складні методи, щоб отримувати доступ до ресурсів, викрадати дані, саботувати роботу компаній або вимагати гроші. Щороку кількість атак збільшується, а зловмисники розробляють нові методи для уникнення виявлення їхніх злочинних дій. Ефективна програма з кібербезпеки включає фахівців, процеси й технологічні рішення, які разом зменшують ризик перерв у роботі компаній, фінансових втрат і підриву репутації внаслідок атак. Атака на комп'ютери працівників державних установ може дестабілізувати психологічний стан їх співробітників.

У багатьох університетах України є навчальні курси з дисципліни «Кібербезпека», «Кіберпсихологія»: міжнародна академія управління персоналом (м. Київ), Європейський університет (м. Київ), Вінницький національний технічний університет, Державний університет інтелектуальних технологій і зв'язку (м. Одеса), Дніпровський національний університет імені

Олеся Гончара, мала комп'ютерна академія «Крок», Донецький національний технологічний університет (м. Луцьк), Донецький національний університет імені Василя Стуса (м. Вінниця), Західноукраїнський національний університет (м. Тернопіль), Київський політехнічний університет імені Ігоря Сікорського, Київський національний економічний університет імені Вадима Гетьмана, Київський національний університет будівництва та архітектури, Київський національний університет імені Тараса Шевченка, Київський національний університет технологій і дизайну, Київський столичний університет імені Бориса Гринченка, Київський університет банківської справи. Коледж інженерії і управління (м. Київ), Луцький національний технічний університет, Львівський державний університет безпеки життєдіяльності, Львівський національний університет імені Івана Франка, Маріупольський державний університет (м. Київ), Національна академія служби безпеки України (м. Київ), Національний авіаційний університет (м. Київ), Харківський аерокосмічний університет імені Миколи Жуковського, Національний технічний університет «Дніпровська політехніка», Національний технічний університет «Харківський політехнічний інститут», Національний університет «Одеська політехніка», Національний університет «Одеська юридична академія», Національний університет «Чернігівська політехніка», Національний університет «Львівська політехніка», Національний університет кораблебудування імені Степана Макарова (м. Миколаїв), Одеський національний технологічний університет, Сумський державний університет, Тернопільський національний технічний університет імені Івана Пулюя, Ужгородський національний університет, Український державний університет науки і технологій (м. Дніпро), Університет митної справи і фінансів (м. Дніпро), Університет штучного інтелекту та цифровізації (м. Київ), Харківський навчально-науковий інститут «Університет банківської справи», Харківський національний університет внутрішніх справ, Харківський національний університет імені Василя Каразіна, Харківський національний університет радіоелектроніки, Херсонський національний

технологічний університет (переміщений заклад, м. Хмельницький), Хмельницький національний університет, Чернівецький університет імені Юрія Федьковича інтегрували дисципліну «Кібербезпека» до своїх навчальних програм. В межах Міністерства внутрішніх справ організований департамент кіберполіції, який здійснює діяльність в межах цифрового простору. Відповідно до законодавства України кіберполіція забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю.

27 липня вважається днем Кіберполіції України. Такий департамент був створений 27 липня 2009 року. Нова Кіберполіція була створена 13 жовтня 2015 р. Кіберполіція веде боротьбу з скімінгом, кеш-трапінгом, кардінгом, фішингом, онлайн-шахрайством, піратством, кардшарінгом, рефайлінгом. Від Кіберполіції залежить безпека громадян. Під час повномасштабної війни росії проти України важливим є дотримання інформаційної гігієни. Важливо верифікувати інформацію. У зв'язку з цим не треба довіряти інформації з боку російських ЗМІ, не зважати на платну рекламу в Фейсбуку, де часто розміщуються панічні та інші дописи, спроможні вести громадян в стан паніки, не використовувати інформацію з неперевіраних сайтів з маніпулятивними заголовками, перевіряти інформацію з соцмереж. З метою безпеки громадяни не мають викладати в соцмережах відео прильотів по цивільній та військовій інфраструктурі. Сучасна війна це ще й інформаційна війна, тому важливо викривати фейки, які поширюються в Інтернеті стосовно війни. Українська держава запустила з цією метою веб-сайт «StopFake». Існує громадська організація з подібною назвою. Зі своєї сторони сама держава має подавати правдиву інформацію про війну. Україна має вести боротьбу з анонімними телеграм-каналами, які поширюють неправдиву інформацію. Сама Кіберпсихологія є дуже молодого галуззю психології. Вона стоїть перед викликами кібербулінгу, віртуальної реальності та кібербезпекою. Кіберпсихологія здійснює онлайн-терапію, використовує новітні дані для досліджень психології громадян України, здійснює соціальну підтримку для чисельних онлайн-спільнот, сприяє електронній освіті та саморозвитку.

Виклики повномасштабної війни ставлять перед кіберпсихологією задачу ще й інформаційної безпеки громадян. Це особливо важливо перед загрозою російських кібератак на кіберпростір України. Зараз Україна знаходиться на стадії постіндустріального інформаційного суспільства. Вона має потурбуватись про викладання кіберпсихології як наукової психологічної дисципліни у закладах вищої освіти України.

Цифрові технології та соціальні мережі впливають на психічне здоров'я громадян. Кіберполіція має знешкоджувати «фабрики російських тролів» та блокувати російських ботів в цифровому просторі.

Кібервійська України були створені апаратом Рада національно безпеки і оборони у вересні 2021 р. Це рішення було ефективним і вчасним. Зараз Кібервійська України адекватно реагують на загрози з боку Росії.

Таким чином, робимо висновок, що цифровий простір України мають захищати кіберполіція та кібервійська. Особливо важливим є запровадження дисципліни «Кіберпсихологія» у закладах вищої освіти. Виклики війни проти Росії змушують Україну оперативно реагувати на загрози для громадян України у кіберпросторі.

Список використаних джерел

1. Кіберпсихологія : ефекти, ризики, прогнози. URL: <https://medium.com/avitar-blog/кіберпсихологія-ефекти-ризики-прогнози-dc053611f544> (дата звернення: 30.09.2024).
2. Постанова Кабінету Міністрів України від 13.10.2015 № 831 «Про утворення територіального органу Національної поліції»// Урядовий кур'єр від 21.10.2015 № 195/
3. Що таке кібербезпека? URL <https://www.microsoft.com/uk-ua/security/business/security-101/what-is-cybersecurity;>
<https://armyinform.com.ua/tag/kibervijska-ukrayiny/>
StopFake <https://www.stopfake.org/uk/golovna/>

DrSci (in History), Senior Researcher,
Department of Scientific Information and Analytical Support of Education
V. Sukhomlynskyi State Scientific and Educational Library of Ukraine
Kyiv, Ukraine
ORCID ID: 0000-0002-9809-3166
pylypchuk.yaroslav@gmail.com

CHALLENGES AND CURRENT STATE OF CYBERPSYCHOLOGY DURING THE FULL-SCALE WAR BETWEEN RUSSIA AND UKRAINE

Within the framework of the study "Informational and analytical support of psychological education in the war and postwar periods" of the department of scientific informational and analytical support of education of the State Scientific and Pedagogical Library of Ukraine named after V. O. Sukhomlynskyi cyberpsychology in the context of the Russian Federation's war against Ukraine is an integral part of psychological science at the current stage, and its relevance is undeniable. The digital space of Ukraine must be protected by cyber police and cyber troops, which provokes the provision of information and analytical support for the training of military psychologists in this context. The introduction of the discipline "Cyberpsychology" in institutions of higher education is especially important. Provocations of war against Russia force Ukraine to promptly respond to threats to Ukrainian citizens in Cyberspace.

Keywords: Cyberpsychology, Cyberpolice, Cybermilitary, Ukraine, war, Cyberspace.