системне використання психотехнологій у роботі з кадрами та професійної підготовки фахівців екстремального профілю діяльності дозволяє на якісно новому рівні розкрити та розвинути здібності працівників, підвищити їх професіоналізм, працездатність, зберегти здоров'я і життя у виконанні ними різноманітних службово-професійних завдань. Крім того, психотехнологічний кадровий менеджмент сприятиме мінімізації різних негативних явищ серед персоналу сектору безпеки та оборони, таких як плинність кадрів, порушення дисципліни, алкоголізм, психологічна дезадаптація тощо.

**Список використаних джерел:**

1. Барко В. І. Професійний відбір кадрів до органів внутрішніх справ (психологічний аспект): монографія Київ : Ніка-Центр, 2002. 344 с.

2. Лефтеров В. О. Психологічні тренінгові технології в органах внутрішніх справ: монографія: в 2-х т. Т. І: Методологія психотренінгу та його використання у професійно-психологічному розвитку персоналу, задіяного в екстремальних видах діяльності. Донецьк : ДЮІ, 2008. 242 с.

Гурський В. Є., Лефтеров В. О. Професійно-психологічний розвиток працівників спецпідрозділів поліції імітаційними засобами : монографія. Одеса: Видавничий дом «Гельветика», 2017. 164 с.

**ЛУНГОЛ Ольга,**
кандидат педагогічних наук, доцент,
доцент кафедри оперативно-розшукової
діяльності та інформаційної безпеки

факультету підготовки фахівців
для підрозділів кримінальної поліції
Донецького державного
університету внутрішніх справ
(м. Кропивницький, Україна)

## ВИКЛИКИ ТА ПЕРСПЕКТИВИ КІБЕРБЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ

Кібербезпека у сучасному світі стала одним із найважливіших аспектів забезпечення безпеки як національних, так і корпоративних інформаційних систем. Проте, разом із швидким розвитком технологій та поширенням цифрових сервісів, зростає і кількість та складність викликів, які стоять перед кібербезпекою.

Одним із основних викликів сьогодення у формуванні загального безпекового середовища нашої країни є постійно зростаюча кількість кібератак, які стають усе більш виразними та складними. Хакерські угрупування та кіберзлочинці вдосконалюють свої методи й стратегії для здійснення незаконних діянь у цифровому просторі. Крім того, з'являються нові технології, такі як інтернет речей (IoT), штучний інтелект (AI) та квантові обчислення, які вимагають нових підходів до забезпечення кібербезпеки.

Питання кібербезпеки є особливо актуальним в складних умовах сьогодення нашої країни. Кібербезпека є темою наукових досліджень значного кола вітчизняних науковців та ІТ-фахівців. Так К. Краус [1], Н. Кра-

ус [1] та О. Штепа [1] у своїх наукових роботах описуються можливі трансформаційні процеси кібербезпеки суб'єктів господарювання в умовах воєнного стану. Науковці зазначають факти, що є обов'язковими критеріями безпеки сучасного цифрового підприємництва: для забезпечення безпеки даних, необхідно зашифровувати їх як при зберіганні, так і при передачі; шифрування повинно здійснюватися на рівні користувача, і лише сам користувач повинен мати доступ до ключів шифрування; дані не повинні передаватися через відкриті канали електронної пошти, а компанія має забезпечувати контроль за сховищем зашифрованих даних та ключами доступу до них тощо.

Є. Смілянец [2], О. Білаш [2], А. Плахотний [2], О. Пелещак [3] та ін. описують у своїх дослідженнях різновиди кіберзагроз, які є актуальними на часі, а саме: кібершпигунство, кіберсаботаж та кібертероризм. О. Пелещак [3] зазначає, що найнебезпечнішим є потенціал кібердиверсій, які здійснюються на об'єктах критичної інформаційної інфраструктури або об'єктах, важливих для життєдіяльності держави. Небезпеку можуть становити віруси, призначенням яких є не збирання інформації, а її знищення або цілеспрямоване атакування певних вузлів управління, що може не тільки зупинити їх роботу, а й призвести до людських жертв. Частина науковців включають у кібердиверсії такі складові, як дезінформація та маніпуляція інформацією, кібершпигунство, кібератаки, соціальну інже-

нерію, кібертероризм, вірусні атаки, кіберблокування тощо. Це означає, що часто відбувається об'єднання різних форм кібернебезпек для досягнення злочинних цілей у цирфовому просторі. Особливо зріс із початку повномасштабного вторгнення об'єм неправдивої або спотвореної інформації у соціальних медіа, на вебсайтах, у месенджерах, з метою впливу на громадську думку, створення розбіжностей або зміни уявлень суспільства.

Проаналізувавши матеріали сайту Департаменту Кіберполіції України [4], можна стверджувати, що актуальними небезпеками є також отримання несанкціонованого доступу до конфіденційної інформації, такої як документи, електронні листи або файли, для використання їх у шантажі, дезінформації або інших злочинних цілях; злам інформаційних систем, мереж або комп'ютерів з метою завдання шкоди, крадіжки конфіденційної інформації, перешкоджання нормальному функціонуванню важливих об'єктів інфраструктури; використання маніпуляційних та психологічних методів для отримання доступу до конфіденційної інформації або підміни ідентифікаційних даних; використання кібератак для залякування або впливу на національну безпеку, громадський порядок або економіку; розповсюдження шкідливих програм або вірусів з метою завдання шкоди комп'ютерним системам або мережам. Незважаючи на виклики, перед кібербезпекою

стоять також значні перспективи. Впровадження новітніх технологій, таких як машинне навчання та аналіз великих даних допомагає виявляти та запобігати кібератакам з більшою ефективністю. Розробка міжнародних стандартів та співпраця між державами та корпораціями сприяють створенню більш безпечного цифрового середовища. Посилення заходів та стратегій із забезпечення безпеки інформаційних систем, мереж і даних, як у державних, так і у приватних організаціях нашої країни, такі, як використання брандмауерів, віртуальних приватних мереж (VPN) та інших технологій для захисту мережевих з'єднань та запобігання несанкціонованому доступу; використання спеціального програмного забезпечення для виявлення потенційних загроз та аномальних дій у мережі для оперативного реагування на них; шифрування конфіденційної інформації під час передачі та зберігання даних; встановлення багатофакторної аутентифікації та інших методів для перевірки ідентичності користувачів і забезпечення доступу лише авторизованим особам; регулярне встановлення оновлень і патчів для програмного забезпечення та операційних систем для закриття вразливостей й захисту від відомих загроз тощо. Не менш важливою в кібербезпеці на рівні нашої держави є активна освітня спрямованість в напрямі інформаційної та кібербезпеки.

Воєнний стан створює унікальні виклики для кібербезпеки нашої держави, оскільки кібератаки ви-

користовуються для завдання шкоди національній безпеці та інфраструктурі. Тому важливо досліджувати та посилювати заходи кібербезпеки для формування безпечного цифрового середовища. Умови воєнного стану вимагають розробки та впровадження ефективних стратегій відповіді на кібератаки. Даний процес включає не тільки технічні заходи захисту, але й організаційні та правові механізми для координації дій та реагування на інциденти. Завдяки динаміці кіберзагроз і технологічному прогресу, вдосконалення стратегій та методів кібербезпеки має бути постійним процесом для ефективного протистояння сучасним кіберзагрозам. Розвиток комплексного підходу до кібербезпеки є важливим завданням для забезпечення стійкості та безпеки в цифровому світі.

**Список використаних джерел:**

1. Краус К., Краус Н., Штепа О. Цифрова трансформація кібербезпеки на мікрорівні в умовах воєнного стану. *Innovation and Sustainability*. 2022. № 3. С. 26-37.

2. Смілянец Є., Білаш О., Плахотний А. Щодо кібербезпеки в умовах воєнного стану : матер. І Міжнар. наук. конф. «Інноваційна наука: пошук відповідей на виклики сучасності», 22.12. 2023. Одеса, Україна. С. 166-170.

3. Пелещак О. Р. Деякі аспекти кримінально-правової характеристики кібердиверсій. *Соціально-правові студії.* Вип. 3(9). 2020. С. 26-33.

4. Сайт Департаменту Кіберполіції України. URL: https:// cyberpolice. gov.ua.