

## ДЕТЕКТИВ І КІБЕРРОЗВІДКА: ВИКЛИКИ ВОЄННОГО СТАНУ

*Дерев'янка Т.*

*здобувачка вищої освіти першого (бакалаврського) рівня  
2-го курсу спеціальності 081 – Право  
Міжнародний гуманітарний університет  
Науковий керівник: Слатвінська В. М.  
експерт комп'ютерно-технічних експертиз,  
викладач кафедри кримінального права, процесу та криміналістики  
Міжнародний гуманітарний університет  
м. Одеса, Україна*

У сучасних умовах кібербезпека стає однією з головних проблем державної безпеки, і роль детектива у кіберрозвідці набуває все більшого значення, особливо в умовах воєнного стану.

У воєнний час детективні агенти та кіберрозвідувачі стикаються з безліччю викликів, які потребують негайної та точної реакції. Одним із головних завдань таких фахівців є забезпечення національної безпеки та захисту від зовнішніх загроз.

Особливо в контексті військових операцій, на думку Горінова П. В. Драпушко Р. Г.: «Кіберпростір є новим каналом. Він призначений для створення і поширення різноманітної інформації, яка стала новим двигуном економічного зростання, новою платформою для соціального управління, новим способом міжнародного співробітництва і цілою новою сферою національного суверенітету» [1, с. 267].

Детективи займаються розслідуванням злочинів, які можуть бути пов'язані з шпигунством, тероризмом та іншими формами злочинності, що ставлять під загрозу державну безпеку. Вони використовують свої професійні знання та досвід, щоб знайти й ідентифікувати злочинців, які діють на користь ворожих держав або груп.

У свою чергу, кіберрозвідувачі займаються виявленням та запобіганням кібератак та кібершпигунства. Вони мають у своєму розпорядженні передові технології та програмне забезпечення, що дозволяє виявляти та аналізувати потенційні кіберзагрози та кібератаки.

У воєнний час детективи та кіберрозвідувачі стикаються з більш складними викликами. Наприклад, вони можуть бути залучені до збору інформації про можливі напади на об'єкти критичної інфраструктури, або до виявлення та ліквідації кібератак на важливі об'єкти. Також у воєнний час збільшується ризик зламу державних систем та

інформаційних мереж, що може призвести до серйозних наслідків для національної безпеки. Тому, детективи та кіберрозвідувачі повинні бути готові до оперативних дій.

У воєнний час детективи, які займаються кіберрозвідкою, мають виконувати складні завдання, пов'язані з захистом державної безпеки та запобіганням кіберзароз.

Одним із головних завдань детективів у воєнний час є виявлення та ідентифікація можливих кіберзароз для держави. Вони мають досліджувати Інтернет-ресурси, соціальні мережі та інші канали комунікації з метою виявлення підозрілих активностей, які можуть ставити під загрозу національну безпеку.

Детективи використовують передові технології та програмне забезпечення для збору та аналізу інформації з Інтернету, щоб виявити потенційні кібератаки та кібершпигунство.

У воєнний час детективи повинні бути готові до оперативних дій, таких як виявлення та ліквідація кібератак на об'єкти критичної інфраструктури, а також до запобігання зламу державних інформаційних систем.

Детективи також мають бути готові до співпраці з іншими військовими підрозділами, які займаються кібербезпекою, з метою координації дій та ефективного вирішення завдань, пов'язаних з захистом держави.

У воєнний час детективи, які займаються кіберрозвідкою, мають бути готові до швидкої реакції на кіберзагрози та до виконання завдань у складних умовах військового конфлікту.

Таким чином, місце детектива в кіберрозвідці у воєнний час є дуже важливим, оскільки він виконує завдання, які допомагають забезпечити безпеку держави в кіберпросторі та запобігти можливим загрозам.

### **Література:**

1. Горінов П. В. Драпушко Р. Г. Сучасні виклики адміністративно-правових засад кібербезпеки України в умовах воєнного стану. *Юридичний науковий електронний журнал*. 2023. № 1. С. 267–270. DOI: <https://doi.org/10.32782/2524-0374/2023-1/63>