У надзвичайних ситуаціях військового характеру населенню потрібно дотримуватися інструкцій цивільної оборони, слідувати вказівкам військових та рятувальників, реагувати на сигнали оповіщення. Важливо допомагати одне одному, бути готовими до евакуації або тимчасового переселення, надавати допомогу потерпілим. У таких умовах необхідно співпрацювати та підтримувати зв'язок з іншими людьми для забезпечення загальної безпеки та виживання.

**Список використаних джерел**

1. Бака М. М., Квашньов Ю. О. Захист Вітчизни 10-11 кл. Порядок оповіщення населення, евакуація населення. Київ : Вид-во «Вежа», 2006. С. 270–274.

2. Лелека В. М., Бахтін А. М. Захист Вітчизни 10 кл. Надзвичайні ситуації воєнного характеру. Рівні надзвичайних ситуацій. Харків : Вид-во «Ранок», 2018. С. 120–122.

3. Фука М. М., Герасимів І. М., Пашко К. О. Захист України 10 кл. Дії в умовах особливого періоду, під час артилерійського обстрілу, у разі виявлення особливого предмета. Київ : Вид-во «Астон», 2018. 288 с.

## КІБЕРБЕЗПЕКА В УКРАЇНІ В УМОВАХ ВОЄННОГО СТАНУ

***Кропивка О. Г.***
*консультант начальника Управління по взаємодії з питань антитерористичної діяльності УСБУ в Полтавській області, полковник, доктор філософії*

Від початку широкомасштабного вторгнення росії в Україну кібербезпека стала одним із ключових фронтів цієї війни. Російські хакери безперервно здійснюють атаки на інфраструктуру України, намагаючись знищувати важливі об'єкти, викрадати дані та спричиняти хаос. У таких умовах, особливо за дії воєнного стану, Україна, як і багато інших держав, стикається з необхідністю суттєвого зміцнення своїх кіберзахисних спроможностей. Воєнний стан підвищує ризики кібератак та інших форм кіберзагроз, що можуть мати

серйозні наслідки для національної безпеки. Тому посилення кіберзахисту є нагальним завданням держави.

Одним із головних викликів у сфері кібербезпеки в умовах воєнного стану є зростання кількості кібератак з боку країни-агресора. Агресія росії проти України, зокрема окупація територій та підтримка бойових дій, супроводжується активною кібервійною. Хакерські угруповання, пов'язані з російськими військовими структурами та спецслужбами, здійснюють атаки на інформаційні системи України, провокують матеріальні збитки, проводять шпигунську діяльність і намагаються дестабілізувати суспільство.

За даними українських служб кібербезпеки, атаки здійснюються різними методами: поширенням шкідливих програм, атаками на критично важливі системи та інфраструктуру, втручанням у телекомунікаційні мережі, кібершпигунством і кібервимаганням. Крім того, експерти відзначають зростання кількості атак соціальної інженерії, коли зловмисники використовують довіру людей або дезінформацію для отримання несанкціонованого доступу до даних. Такі атаки є складнішими та важчими для виявлення, що ускладнює забезпечення ефективного захисту.

У зв'язку з цим захист критично важливих інформаційних систем і мереж стає пріоритетним завданням українських інституцій, що працюють у сфері кібербезпеки. Важливо не лише вдосконалювати технічні засоби захисту та моніторингу, а й підвищувати рівень обізнаності громадян щодо кіберзагроз. Кожному українцю важливо знати основні види загроз та способи захисту [1].

До основних кіберзагроз належать:

– атаки на критичну інфраструктуру (електростанції, системи водопостачання, транспортні мережі), що можуть спричинити серйозні зброї, економічні втрати та загрожувати життю людей;

– крадіжка даних – особистих, комерційних або державних; викрадену інформацію можуть використовувати для шантажу, вимагання чи підриву довіри до уряду;

– дезінформація та пропаганда, що поширюють неправдиві відомості, розпалюють ненависть і спричиняють соціальну нестабільність;

– фішинг і кібершахрайство, які спрямовані на викрадення особистих або фінансових даних чи поширення шкідливого програмного забезпечення.

Україна вже здійснила низку кроків для посилення кіберзахисту в умовах війни, однак необхідні подальші зусилля та інвестиції. Науковці та експерти рекомендують такі базові заходи безпеки:

– використовувати надійні та унікальні паролі;

– увімкнути двофакторну автентифікацію;

– регулярно оновлювати програмне забезпечення;

– встановлювати антивірусні рішення та брандмауери;

– бути обережними з підозрілими посиланнями та вкладеннями;

– регулярно створювати резервні копії важливих даних [2].

Отже, у контексті воєнного стану кібербезпека стає важливим елементом національної оборони України. Зростання кількості атак з боку противника, зокрема тих, що підтримуються Росією, створює серйозні загрози для національної безпеки та стабільності. Ефективний кіберзахист вимагає розвитку технічних засобів, підвищення цифрової грамотності населення та активної міжнародної співпраці. Лише об’єднавши зусилля держави, приватного сектору та міжнародних партнерів, Україна зможе забезпечити належний рівень кіберзахисту у період військового конфлікту [3].

**Список використаних джерел:**

1. Кібербезпека під час війни: базові заходи з кіберзахисту для українських організацій. URL: https://www.kmu.gov.ua/news/kiberbezpeka-pid-142 chas-viiny-bazovi-zakhody-z-kiberzakhystu-dlia-ukrainskykh-orhanizatsii

2. Кібербезпека під час вій ни: як надій но захйстйтй ваші прйстрої і дані на нйх. URL: https://koda.gov.ua/kiberbezpeka-pid-chas-vijny-yaknadijno-zahystyty-vashi-prystroyi-i-dani-na-nyh/.

3. Кібербезпека. URL: https://moz.gov.ua/kiberbezpeka.