ЗМІСТ

# Методичні рекомендації з використання соціальних мереж у Збройних Силах України

# Анотація

Методичні рекомендації з використання соціальних мереж у Збройних Силах України (далі — Рекомендації) розроблено Головним оперативним управлінням Генерального штабу Збройних Сил України та погоджено із заінтересованими органами військового управління та структурними підрозділами Генерального штабу Збройних Сил України.

Ці Рекомендації розроблені з метою надання порад та пропозицій щодо висвітлення інформації про діяльність Збройних Сил України та правил поведінки військовослужбовців у соціальних мережах.

ГОЛОВНЕ ОПЕРАТИВНЕ УПРАВЛІННЯ
ГЕНЕРАЛЬНОГО ШТАБУ ЗБРОЙНИХ СИЛ УКРАЇНИ



# МЕТОДИЧНІ РЕКОМЕНДАЦІЇ З ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ У ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Видавництво
«Центр учбової літератури»
Київ – 2023

УДК [316.77:004.738.5] (477)
М 54

**М 54** **Методичні рекомендації соціальних мереж у Збройних Силах України.** — Київ: «Центр учбової літератури», 2023. — 28 с.

**ISBN 978-611-01-2879-7**

Методичні рекомендації з використання соціальних мереж у Збройних Силах України (далі — Рекомендації) розроблено Головним оперативним управлінням Генерального штабу Збройних Сил України та погоджено із заінтересованими органами військового управління та структурними підрозділами Генерального штабу Збройних Сил України.

Ці Рекомендації розроблені з метою надання порад та пропозицій щодо висвітлення інформації про діяльність Збройних Сил України та правил поведінки військовослужбовців у соціальних мережах.

ISBN 978-611-01-2879-7

**ЗМІСТ**


| | | |
|---|---|---|
| | ВСТУП | 4 |
| | ПОСИЛАННЯ НА ВІЙСЬКОВІ ПУБЛІКАЦІЇ | 5 |
| | ОСНОВНІ ТЕРМІНИ ТА ВИЗНАЧЕННЯ | 6-7 |
| | ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ | 8 |
| 1 | ОГЛЯД СОЦІАЛЬНИХ МЕРЕЖ ТА МЕСЕНДЖЕРІВ | 9-12 |
| 2 | БЕЗПЕКА І РИЗИКИ В СОЦІАЛЬНИХ МЕРЕЖАХ | 13 |
| 2.1 | Небезпечні фактори під час роботи в Інтернеті | 13-14 |
| 2.2 | Приклади службової і конфіденційної інформації та можливі наслідки її поширення в соціальних мережах (медіа) | 15-16 |
| 3 | ПОРЯДОК СТВОРЕННЯ ОФІЦІЙНИХ СТОРІНОК ОРГАНІВ ВІЙСЬКОВОГО УПРАВЛІННЯ, ВІЙСЬКОВИХ ЧАСТИН ТА ПІДРОЗДІЛІВ ЗБРОЙНИХ СИЛ УКРАЇНИ У СОЦІАЛЬНИХ МЕРЕЖАХ ТА ВИМОГИ ДО НИХ | 17 |
| 3.1 | Порядок створення офіційного акаунту та його верифікація | 17-18 |
| 3.2 | Вимоги до інформації, яка поширюється на офіційних сторінках | 18-20 |
| 3.3 | Символіка Збройних Сил України | 20 |
| 4 | ПРАВИЛА ПОВЕДІНКИ В СОЦІАЛЬНИХ МЕРЕЖАХ | 21-23 |
| 5 | РЕКОМЕНДАЦІЇ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ ТА МЕСЕНДЖЕРАХ | 24-26 |
| 6 | ЗАКЛЮЧНА ЧАСТИНА | 27 |

# ВСТУП

Сучасні виклики зумовлені застосуванням Російською Федерацією технологій гібридної війни та перенесенням театру воєнних дій у площину інформаційного простору, перетворили його на одну з ключових арен протиборства.

Аналіз способів ведення останніх збройних конфліктів свідчить, що у військовій справі настав новий етап розвитку, коли ефективність сучасних засобів ураження все більше визначається не стільки вогневою міццю, скільки ступенем інформаційної безпеки. У змісті військових дій все більше зростає значимість інформаційного протиборства і перевага у ступені інформованості стає неодмінною умовою перемоги у війні.

На сьогодні соціальні мережі є зручним та ефективним засобом комунікації. Вони надають величезну свободу висловлювань в інформаційному просторі, який є відкритим та доступним для всіх. При ефективному їх використанні вони стають потужним інструментом для підняття іміджу та репутації Збройних Сил України, підтримання зв'язків з громадськістю, спілкування та обміну досвідом тощо.

Крім того, соціальні мережі можуть ефективно використовуватись у ході реабілітації військовослужбовців, для підвищення та підтримання на високому рівні їх морально-бойового духу та популяризації військової служби серед населення.

Водночас відкритий та глобальний характер соціальних мереж та медіа створює передумови до збору й аналізу іноземними розвідками конфіденційної інформації про діяльність Збройних Сил України, персональних даних військовослужбовців та членів їх родин, а також використання противником соціальних мереж для вербування особового складу та здобуття необхідної йому інформації.

Керівництво Збройних Сил України не забороняє військовослужбовцям та працівникам Збройних Сил України використання соціальних мереж. Однак з метою забезпечення їх захисту та безпеки важливо, щоб вони були обізнані про можливі загрози, які впливають як на їх службову діяльність, так і на приватне життя.

Положення цієї публікації викладені з метою надати допомогу військовослужбовцям та працівникам Збройних Сил України, членам їх родин та близьким у правильному використанні соціальних мереж, медіа-порталів та месенджерів, поширенні інформації про діяльність Збройних Сил України та обмеженні доступу до їх персональних даних.

# ПОСИЛАННЯ НА ВІЙСЬКОВІ ПУБЛІКАЦІЇ

| Позначка військової публікації | Повне найменування військової публікації |
|---|---|
| | Закон України "Про основні засади забезпечення кібербезпеки України", із змінами, Верховна Рада України, Київ, 2020 |
| | Закон України "Про телекомунікації", із змінами, Верховна Рада України, Київ, 2020 |
| | Закон України "Про інформацію", із змінами, Верховна Рада України, Київ, 2016 |
| ВКП 18-00(01).01 | Доктрина публічного спілкування, Київ, 2020 |
| | Пам'ятка щодо забезпечення інформаційної безпеки при роботі в мережі інтернет, Департамент контр-розвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України, Київ, 2019 |
| | Рекомендації для персоналу Міністерства оборони України та Генерального штабу Збройних Сил України щодо поводження в соціальних мережах, Управління інформаційних технологій, Київ, 2014 |
| ВП 1-185(49)03.01 | Порадник "Медіаграмотність. Практичні поради військовослужбовцям Збройних Сил України", Київ, 2021 |
| | U.S. Marine Corps Social Media Handbook, Headquarters Marine Corps Communication Directorate Production and Engagement, 2021 |
| | Using Social Media in the British Army, The British Army's Social Media Policy, Digital Army, Version 5, July 2020 |
| | Family Guidance For the Internet and Social Media. OPSEC, PII and Identity Management, United States Fleet Forces, February 2019 |
| | U.S. Navy Social Media Handbook for Navy leaders, communicators, Sailors, families, ombudsmen and civilians, March 2019 |
| | Identity Awareness, Protection, and Management Guide. A Guide for Online Privacy and Security Comprised of the Complete Collection of Department of Defense Smart Cards Seventh Edition, US Department of Defense, September 2018 |
| | Guide du bon usage des réseaux sociaux, À destination de tous les militaires et civils du ministère de la Défense et de leur entourage, 2016 |
| | U.S. Army Social Media Handbook, Army Office of the Chief of Public Affairs, Online and Social Media Division,1500 Pentagon, Washington, DC, January 2011 |
| | The U.S.M.C. Social Media Principles marine Corps, Insider Threat Working Group, the Marine Corps Production Directorate, Defense Media Activity, the Marine Corps Division of Public Affairs |

## ОСНОВНІ ТЕРМІНИ ТА ВИЗНАЧЕННЯ

**IP адреса** (Internet Protocol Address) – це ідентифікатор (унікальний числовий номер) мережевого рівня, який використовується для адресації комп'ютерів чи пристроїв у мережах, які побудовані з використанням протоколу TCP/IP.

**Акаунт** (обліковий запис) – сукупність інформації про користувача, засобів та його прав відносно багатокористувацької системи. Обліковий запис, як правило, містить відомості, необхідні для ідентифікації користувача при підключенні до системи, інформацію для авторизації і обліку. Це ім'я користувача та пароль.

**Вебсайт** (або сайт) – сукупність вебсторінок та вмісту, доступних у Інтернеті, які об'єднані як за змістом, так і за навігацією під єдиним доменним ім'ям. Сайтом також називають вузол Інтернету (комп'ютер), за яким закріплена унікальна IP-адреса, що ідентифікує його в мережі.

**Відеоконференція** – телекомунікаційна технологія, що забезпечує одночасну двосторонню передачу, обробку, перетворення та представлення інтерактивної інформації на відстані в режимі реального часу *(Skype, Viber, Zoom).*

**Загрози інформаційній безпеці** – сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства і держави в інформаційній сфері.

**Захист інформації** - сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

**Інформація** – це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

**Інформаційна безпека –** здатність забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації.

**Інформаційна загроза** – наміри, дії або явища, які шляхом інформаційного впливу на соціальні об'єкти, інформаційну інфраструктуру та інформаційні ресурси можуть ускладнити (унеможливити) реалізацію національних інтересів держави (функцій її структурних органів).

**Інформаційний ресурс –** документи або масиви документів, які зберігаються в інформаційних системах.

**Інформаційна система** – це сукупність обладнання, методів та процедур, і, в разі необхідності, персоналу, організованого для виконання функцій накопичення, обробки, зберігання та передавання даних.

**Інформаційний простір** – це інформаційне середовище, в якому відбуваються інформаційні процеси та інформаційні відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації, інформаційних продуктів та інформаційних ресурсів.

**Інформаційне середовище** – це частина інформаційного простору, що характеризується мінімальною територією поширення та обмеженою кількістю суб'єктів інформаційної діяльності, обумовлюється своєрідним інформаційним мікрокліматом, що включає сукупність способів, прийомів, заходів та умов безпосереднього здійснення інформаційної діяльності.

**Кіберзагроза -** наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, негативно впливають на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів.

**Кібербезпека** - захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

**Кіберзахист** - сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем.

**Кіберпростір** - середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних.

**Кібероборона -** сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії.

**Комунікація** – процес передачі інформації (фактів, ідей, поглядів, емоцій тощо) вербальним, письмовим, друкованим, аудіовізуальним, електронним та іншим способом між суб'єктами або від суб'єкта до об'єкта інформаційно-комунікаційної діяльності та в зворотному напрямку.

**Медіа-блог** – це вебсайт, головний зміст якого записи, зображення чи мультимедіа, які регулярно публікуються.

**Медіахостинг** (медіа-портал) – послуга надавання дискового простору, підключення до мережі та інших ресурсів для розміщення медіа (фото, відео) інформації на сервері, що постійно перебуває в Інтернеті *(YouTube, Vimeo).*

**Месенджери** – це програми (платформи), що дозволяють створювати обмін повідомленнями між користувачами в режимі реального часу (он-лайн) *(Viber, Telegram, WhatsApp, Signal, Facebook Messenger).*

**Проксі-сервер** – сервер (комп'ютерна система або програма) в комп'ютерних мережах, що дозволяє клієнтам виконувати непрямі (через посередництво проксі-сервера) запити до мережевих сервісів.

**Соціальні медіа –** он-лайн технології, завдяки яким користувачі контенту через свої дописи стають його співавторами і можуть співпрацювати, спілкуватися, ділитися інформацією або брати участь у будь-якій іншій соціальній активності із усіма іншими користувачами сервісу *(TikTok, Likee).*

**Соціальна мережа** – це сервіс (вебдодаток), який використовується користувачами для підтримки соціальних зв'язків в Інтернеті. Важливим елементом мережі є контент (зміст, інформація), який створюється її користувачами *(Facebook, Instagram, Twitter, MySpace).*

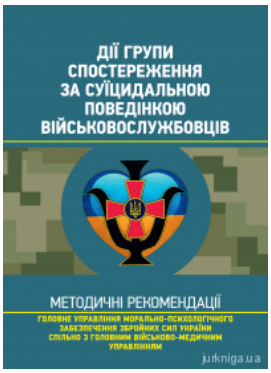
**Фішинг** – вид шахрайства, метою якого є здобування у довірливих або неуважних користувачів соціальних мереж власних (інших користувачів) персональних даних або відомостей.

# ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ

| Скорочення та умовні позначення | Повне словосполучення та поняття, що скорочується |
|---|---|
| ЗМІ | Засоби масової інформації |
| НАТО (NATO) | Організація Північноатлантичного договору (en: North Atlantic Treaty Organization) |
| ОІД | Об’єкт інформаційної діяльності |
| ПЕОМ | Персональна електронно-обчислювальна машина |
| РНБО | Рада національної безпеки і оборони |

# Книги, які можуть вас зацікавити


Алгоритм дії командира військової частини при виявленні та направленні на лікування військовослужбовців з алкогольною залежністю




Дії групи спостереження за суїцидальною поведінкою військовослужбовців


Превентивні психофізіологічні заходи з попередження розвитку дезадаптації у військовослужбовців (невротичних та психічних розладів, пресуїцидальних...


Профілактика відхильної поведінки у військовослужбовців


Пам'ятка психологу для психологічного супроводження військовослужбовців в екстремальних умовах


Психологічна робота з військовослужбовцями -учасниками бойових дій на етапі відновлення

Перейти до галузі права
**Військове право**