Тема .Військово- або безпеково-орієнтована фахова компетентність.

План лекції:

1. Військово- або безпеково - орієнтована фахова компетентність;
2. Національна безпека;
3. Державна пропаганда;
4. Протидія ворожій пропаганді;
5. Забезпечення життєдіяльності суспільства і громадян;

Рекомендована література:

Нормативно-правова база України

- Закон України «Про основи національного спротиву» — базовий документ, що визначає завдання ТРО, Руху опору та підготовки населення.
- Закон України «Про національну безпеку України» — визначає архітектуру сектору безпеки, цивільний контроль та засади СтратКому.
- Закон України «Про правовий режим воєнного стану» — регламентує повноваження військових адміністрацій та обмеження/обов'язки громадян.
- Закон України «Про національну безпеку України» ВВР 2018. №31, ст241
- Стратегія воєнної безпеки України (діюча редакція) — засади всеохоплюючої оборони.

Додаткова література:

Зовнішня політика та національна безпека : навч. посіб. / Г. П. Ситник, Д. В. Неліпа, М. Г. Орел (за ред. Г. П. Ситника, 2022).

Національна безпека: порядок денний для України / В. П. Горбулін, О. Ф. Бєлов, О. В. Литвиненко

Берещак, В. (2023). Комунікаційна стратегія в бізнесі. Як досягти максимуму в спілкуванні з аудиторією. Yakaboo Publishing. YAKABOO+1 2. Б обало, О. Ю. (2015). Комунікативні стратегії: навч. посіб. Львівська політехніка. mybook.biz.ua+1

Falkheimer, J., & Heide, M. (2022). Strategic Communication: An Introduction to Theory and Global Practice (2nd ed.). Routledge. Google Книги+1

Botan, C. H. (Ed.). (2018). The Handbook of Strategic Communication. Wiley. wiley.com 5. Holtzhausen, D., Fullerton, J. A., Lewis, B. K., & Shipka, D. (2021). Principles of Strategic Communication. Routledge. Scrib

Текст лекції

Військово- або безпеково - орієнтована фахова компетентність – це здатність особи ефективно виконувати професійні завдання в кризових умовах, що безпосередньо стосуються національної безпеки, оборони, охорони правопорядку, забезпечення життєдіяльності суспільства і громадян, використовуючи здобуту освітню і професійну кваліфікацію.

Застосування фахових знань у контексті національного спротиву — це залучення цивільних професійних навичок (компетенцій) для посилення обороноздатності країни, захисту її суверенітету та забезпечення життєдіяльності суспільства в умовах військової загрози чи окупації.

Сьогодні національний спротив в Україні є всеохоплюючою системою, де кожен громадянин може бути ефективним на своєму місці, конвертуючи свій професіоналізм у спільну перемогу.

Галузі застосування фахових знань

Залежно від вашої професії, фахові знання інтегруються у різні напрямки спротиву:

1. Інженерія, ІТ та технології

- **Розробка та модернізація ОВТ:** Створення та прошивка БПЛА, розробка систем РЕБ/РЕР, програмування платформ штучного інтелекту для розпізнавання цілей.
- **Кібероборона та кібератака:** Захист критичної інфраструктури від хакерських атак, блокування ворожих пропагандистських ресурсів, збір даних.
- **Зв'язок:** Налаштування захищених каналів комунікації та супутникового зв'язку (Starlink тощо) для військових і цивільних потреб.

2. Медицина та охорона здоров'я

- **Тактична медицина:** Навчання військовослужбовців та цивільних домедичній допомозі (TCCC/ASM).
- **Польова хірургія та реабілітація:** Робота у шпиталях, лікування поранених, фізична та психологічна реабілітація ветеранів.
- **Фармацевтика:** Організація логістики медикаментів та виготовлення дефіцитних ліків.

3. Юриспруденція та право

- **Фіксація воєнних злочинів:** Збір доказів руйнувань, катувань та порушень прав людини для міжнародних судів (Гаага).
- **Правовий супровід:** Юридична допомога військовослужбовцям, членам їхніх родин, ВПО та волонтерським організаціям.

4. Комунікації, маркетинг та медіа

- **Інформаційна протидія (ІПсО):** Боротьба з дезінформацією, спростування фейків, ведення роз'яснювальної роботи серед населення.
- **OSINT (розвідка на основі відкритих джерел):** Пошук геолокацій ворожої техніки, ідентифікація військових злочинців за соцмережами.
- **Фандрейзинг:** Створення креативних кампаній для збору коштів на потреби Сил оборони.

5. Логістика, будівництво та економіка

- **Управління ланцюгами постачання:** Оптимізація доставки військової та гуманітарної допомоги з-за кордону безпосередньо на передову.
- **Фортифікація та відновлення:** Проєктування та будівництво оборонних споруд, бліндажів, швидкий ремонт пошкоджених об'єктів критичної інфраструктури.

Рівні інтеграції фахівця у спротив

Ви можете застосувати свої знання через різні офіційні та неофіційні структури:

1. **Сили територіальної оборони (ТРО) ЗСУ** — проходження служби за контрактом або в резерві, де цивільні навички (наприклад, водіння, ремонт, адміністрування) стають військовими посадами.
2. **Рух опору** — виконання специфічних завдань на тимчасово окупованих територіях (інформаційний спротив, саботаж, передача розвідданих).
3. **Підготовка населення** — участь як інструктор (з топографії, такмеду, виживання) у програмах підготовки громадян до національного спротиву.
4. **Волонтерський рух** — професійна безкоштовна допомога (Pro Bono) фондам, армії чи громадам.

Національна безпека — це стан захищеності життєво важливих інтересів людини, суспільства і держави від внутрішніх та зовнішніх загроз. Вона є фундаментальною основою, на якій будується система національного спротиву.

У сучасному світі поняття національної безпеки вийшло далеко за межі суто військового захисту кордонів. Сьогодні це комплексна система, що охоплює всі сфери життєдіяльності країни.

Ключові сфери (види) національної безпеки

Застосування фахових знань громадян є критично важливим у кожній із цих сфер:

- **Військова безпека:** Здатність держави захистити себе від збройної агресії. Сюди інтегруються військові професіонали, інженери ВПК, інструктори з тактичної та вогневої підготовки.
- **Інформаційна та кібербезпека:** Захист цифрового та ментального простору. Фахівці з IT, кібербезпеки та комунікацій (медіа, OSINT) протидіють хакерським атакам, захищають критичну інфраструктуру та борються з ворожими ІПсО.
- **Економічна та енергетична безпека:** Стійкість фінансової системи, безперебійне виробництво та забезпечення ресурсами. Економісти, логісти, енергетики та аудитори забезпечують стабільність тилу та постачання армії.
- **Екологічна та техногенна безпека:** Захист від катастроф, ліквідація наслідків обстрілів промислових чи атомних об'єктів. Тут задіяні екологи, рятувальники (ДСНС), інженери та хіміки.
- **Гуманітарна та демографічна безпека:** Збереження культурної ідентичності, здоров'я нації та соціальний захист. Медики, психологи, юристи та освітяни дбають про людський капітал, адаптацію ВПО та реабілітацію ветеранів.

Взаємозв'язок національної безпеки та національного спротиву

Національний спротив є одним із головних інструментів забезпечення національної безпеки в умовах воєнної загрози.

Критерій порівняння	Національна безпека	Національний спротив

Масштаб	Загальна стратегічна мета держави.	Практичний інструмент досягнення цієї мети.
Суб'єкти	Державні інститути, спецслужби, ЗСУ, правоохоронні органи.	**Загальнонародний рух**: ЗСУ (ТРО), партизанські рухи, волонтери, цивільні фахівці.
Головне завдання	Прогнозування, запобігання та нейтралізація загроз у всіх сферах.	**Створення умов для суцільної оборони та неприйнятних втрат для агресора.**

Кібербезпека в контексті національного спротиву є одним із найкритичніших інструментів захисту держави, оскільки сучасна війна ведеться не лише на полі бою, а й у цифровому просторі. В умовах повномасштабної агресії **кіберпростір став повноцінним п'ятим театром воєнних дій**, де залучення цивільних ІТ-фахівців та кіберекспертів забезпечує стратегічну перевагу над ворогом.
Застосування фахових знань із кібербезпеки у національному спротиві поділяється на два ключові напрямки: **активна оборона** (захист власної інфраструктури) та **кібератака** (порушення логістики та управління ворога).

Основні напрямки застосування фахових знань у кіберспротиві
1. Захист критичної інфраструктури (Defensive Cyber)

-
- **Аудит та моніторинг вразливостей:** Постійний аналіз захищеності державних реєстрів, систем енергопостачання, зв'язку та банківського сектору.
- **Реагування на інциденти (Incident Response):** Оперативне блокування та ліквідація наслідків ворожих кібератак (наприклад, атак із використанням програм-стерників даних / wipers).
- **Налаштування резервного копіювання:** Побудова відмовостійких архітектур із хмарним дублюванням інформації для збереження даних у разі фізичного знищення серверів.

2. Кібернаступ та розвідка (Offensive Cyber & OSINT)

-
- **Блокування ворожих ресурсів:** Проведення скоординованих DDoS-атак на урядові сайти, пропагандистські медіа та логістичні системи РФ за допомогою інструментів ІТ-армії.
- **OSINT-розвідка:** Пошук закритих даних, геолокація військових об'єктів ворога за відкритими джерелами та злив баз даних російських військовослужбовців для ідентифікації воєнних злочинців.
- **Злам систем управління:** Порушення роботи електронного документообігу, залізничних та транспортних систем ворога для уповільнення його логістики.
-

3. Кібергігієна та протидія ІПсО

- **Навчання населення:** Створення інструкцій та проведення тренінгів із базової цифрової безпеки (двофакторна автентифікація, виявлення фішингу, безпека месенджерів).
- **Боротьба з дезінформацією:** Автоматизований пошук і блокування ботоферм, каналів поширення ворожих фейків та панічних настроїв у соцмережах.

Порівняння ролей фахівців у цивільному житті та кіберспротиві

Професія в мирний час	Роль / Завдання у національному спротиві
SOC-аналітик (Security Operations Center)	Цілодобовий моніторинг мереж для виявлення та відбиття цільових APT-атак ворожих спецслужб.
Пентестер (Етичний хакер)	Пошук вразливостей у ворожих інформаційних системах для їх подальшого виведення з ладу.
Розробник (Software Engineer)	Написання софту для автоматизації збору розвідданих, аналізу ворожого трафіку або координації DDoS-атак.
Системний адміністратор	Швидке відновлення працездатності мереж та зв'язку в деокупованих або прифронтових регіонах.

Як цивільний фахівець може офіційно долучитися?

1. **Кібервійська ЗСУ / Кіберпол:** Проходження служби або офіційна співпраця зі спеціалізованими державними підрозділами.
2. **ІТ-Армія України:** Добровільне онлайн-об'єднання ІТ-фахівців та волонтерів з усього світу, які координують атаки проти цифрової інфраструктури агресора.
3. **Громадські OSINT-спільноти:** Волонтерська участь у проектах з розслідування та верифікації військових даних (наприклад, Molfar або InformNapalm).

Захист інформації у контексті національного спротиву є критично важливим елементом загальної системи національної безпеки. Якщо кібербезпека більше фокусується на захисті технічного та цифрового простору (мереж, серверів, програм), то захист інформації — це ширше поняття, яке включає **захист самого змісту даних, їх конфіденційності, цілісності та доступності**, незалежно від форми їхнього представлення (цифрова, паперова, усна чи ментальна).

В умовах війни інформація стає повноцінною зброєю. Втрата або витік даних може коштувати життів, тоді як надійна ізоляція державних та військових

таємниць забезпечує стратегічну перевагу.

Напрямки застосування фахових знань із захисту інформації
Цивільні фахівці з технічного захисту інформації (ТЗІ), криптографії, стеганографії та безпеки документообігу застосовують свої знання у кількох ключових напрямках:

1. Технічний та інженерний захист

- **Захист від витоку по технічних каналах:** Блокування можливих каналів зняття інформації (акустичних, віброакустичних, електромагнітних випромінювань) у приміщеннях, де проводяться засідання штабів чи військових адміністрацій.
- **Радіоелектронний захист (РЕЗ):** Налаштування засобів шифрування радіозв'язку для ТРО та ЗСУ, щоб унеможливити перехоплення переговорів ворогом (скремблювання, ППРЧ).
- **Створення захищених периметрів:** Розгортання локальних мереж з обмеженим доступом у польових умовах.

2. Криптографічний захист та шифрування

- **Впровадження стійких алгоритмів:** Використання та розробка програмного забезпечення для наскрізного (end-to-end) шифрування чутливих даних, повідомлень та логістичних маршрутів.
- **Керування ключами доступу:** Організація безпечного розподілу, генерації та знищення цифрових ключів і сертифікатів для військових та волонтерів, щоб у разі потрапляння пристрою до рук ворога дані залишилися закритими.

3. Інформаційна безпека та менеджмент (ISO/IEC 27001)

- **Розробка суворих протоколів доступу:** Впровадження принципу "найменших привілеїв" (Zero Trust), коли кожен учасник спротиву має доступ лише до тієї інформації, яка безпосередньо потрібна для виконання його завдання.
- **Безпека волонтерських баз даних:** Захист списків донорів, отримувачів допомоги, закупленого спорядження від координації та зливу ворожим спецслужбам.

4. Протидія витокам інформації (DLP — Data Loss Prevention)

- **Контроль інформаційних потоків:** Запобігання випадковому чи навмисному передаванню критичних даних цивільними особами (наприклад, фотографування прильотів, переміщення техніки ЗСУ, публікація наказів у мережі).

Зміна парадигми захисту інформації для цивільних громадян
В умовах національного спротиву кожен громадянин стає суб'єктом захисту інформації. Фахівці цієї сфери активно залучаються до навчання населення базовим правилам інформаційної безпеки:

- **Режим "Тиша":** Повна заборона на розголошення в публічному просторі (соцмережах, месенджерах) інформації про розташування військових частин, ППО, результати обстрілів та плани командування.
- **Цифрова гігієна:** Правила очищення телефонів та носіїв інформації при перетині блокпостів або перебуванні на прифронтових/окупованих

територіях (видалення чутливих чатів, фото, контактів).

- **Перевірка джерел (Фактчекінг):** Захист власного ментального простору від маніпуляцій, чуток та ворожих фейків через верифікацію офіційних каналів комунікації.

Державна пропаганда у контексті національної безпеки та спротиву є інструментом стратегічних комунікацій держави. Вона спрямована на мобілізацію суспільства, підтримку високого морально-психологічного стану населення та армії, а також на формування позитивного іміджу країни на міжнародній арені.

Під час війни грань між класичною пропагандою та **державною інформаційною політикою** стає дуже тонкою, оскільки головною метою стає виживання нації та протидія деструктивному інформаційно-психологічному впливу ворога (ІПсО)

Ключові вектори державної пропаганди у націоспротиві

Застосування фахових знань (у сфері маркетингу, психології, журналістики, соціології) дозволяє будувати державну інформаційну політику за трьома основними напрямками:

1. Внутрішній контур (Консолідація суспільства)

- **Мобілізація духу:** Популяризація військової служби, волонтерства та національного спротиву. Формування образів героїв сучасности.
- **Протидія паніці:** Оперативне, але дозоване інформування про хід бойових дій. Роз'яснення дій уряду та військового командування для зниження тривожності.
- **Контрпропаганда:** Руйнування міфів та наративів, які ворог намагається впровадити в український медіапростір (наприклад, наративи про "зраду", "відсутність допомоги" тощо).

2. Зовнішній контур (Робота з міжнародними партнерами)

- **Адвокація допомоги:** Постійне нагадування світовій спільноті про масштаби агресії для забезпечення безперебійного постачання зброї, фінансової та гуманітарної допомоги.
- **Дипломатичний тиск:** Демонстрація воєнних злочинів агресора для посилення міжнародних санкцій.
- **Формування суб'єктності:** Популяризація національної культури, історії та цінностей як невіддільної частини цивілізованого світу.

3. Контур на окуповані території та вороже населення

- **Інформаційне утримання:** Підтримка зв'язку з громадянами в окупації, донесення правдивої інформації та надання інструкцій щодо безпеки чи саботажу дій окупантів.
- **Деморалізація ворога:** Донесення інформації про реальні втрати окупаційних військ, розвінчування міфів їхнього командування для зниження мотивації воювати.

Інструменти спротиву: Пропаганда агресора vs. Контрпропаганда України

Захист інформаційного простору вимагає чіткого розуміння різниці між

методами нападу та захисту:

Ознака	Тоталітарна пропаганда ворога	Державні інфокомунікації України
Базис	✕ **Вигадки та фейки**. Створення альтернативної реальності, викривлення фактів.	**Реальні факти**. Акцент на документально підтверджених подіях (злочини РФ, успіхи ЗСУ).
Мета	✕ **Деструктивна**. Посіяти хаос, розкол суспільства, зневіру та страх.	**Конструктивна**. Об'єднання громадян, підтримка армії, збереження державності.
Цінності	✕ Культ війни, ненависть до інших народів, дегуманізація.	Захист свободи, суверенітету, прав людини та європейського вибору.

Роль цивільних фахівців у державній інфополітиці

Фахівці гуманітарного та креативного секторів є головними рушіями цього напрямку спротиву:

- **Журналісти та редактори:** Створення якісного контенту для єдиного інформаційного марафону, верифікація даних перед публікацією.
- **Психологи та лінгвісти:** Аналіз ворожого контенту, виявлення маніпулятивних маркерів, розробка психологічно стійких текстів та закликів.
- **Графічні дизайнери та криейтори:** Створення вірусних патріотичних плакатів, мемів (які є потужною зброєю в інтернет-війні), відеороликів для закордонної аудиторії.
- **SMM-спеціалісти та таргетологи:** Просування проукраїнських наративів у західних соцмережах, блокування каналів поширення російської дезінформації.

Протидія ворожій пропаганді у контексті національного спротиву — це система заходів, спрямована на захист ментального та інформаційного простору держави від деструктивного впливу агресора. В умовах сучасної гібридної війни інформація використовується як зброя масового ураження, метою якої є розкол суспільства, деморалізація армії, посіяння паніки та підрив довіри до військово-політичного керівництва країни.

Застосування фахових знань у цій сфері дозволяє перейти від пасивного захисту до активної контрпропаганди та упередження інформаційних атак.

Ключові напрямки протидії ворожим ІПсО

Цивільні фахівці з комунікацій, аналітики, психології та ІТ застосовують свої компетенції у кількох стратегічних напрямках:

1. Моніторинг та аналітика (OSINT та Data Science)

- **Виявлення інформаційних операцій:** Раннє виявлення координованих інформаційних кампаній ворога за допомогою автоматизованого аналізу

соцмереж (Telegram, TikTok, X).
- **Картіювання ботоферм:** Ідентифікація мереж штучних акаунтів, які масово поширюють панічні або антидержавні коментарі.
- **Аналіз наративів:** Розуміння ключових тез ворога (наприклад, «усе пропало», «нас зрадили», «допомоги не буде») для підготовки точкових контраргументів.

2. Фактчекінг та деконструкція фейків
- **Верифікація медіаконтенту:** Перевірка фото та відео на предмет використання штучного інтелекту (Deepfakes), фотомонтажу або застарілих кадрів з інших конфліктів.
- **Офіційне спростування:** Оперативне донесення правдивої інформації через авторитетні платформи та лідерів думок до того, як фейк встигне укорінитися у свідомості людей.
- **Викриття маніпулятивних технік:** Пояснення аудиторії, *як саме* ворог намагається маніпулювати емоціями (страхом, гнівом, жалем).

3. Формування медіаграмотності (Цивільний захист)
- **Навчання критичному мисленню:** Розробка курсів, тренінгів та пам'яток для населення щодо перевірки джерел інформації.
- **Інформаційна гігієна:** Популяризація правил «не поширюй неперевірене», «читай далі заголовка», «довіряй лише офіційним джерелам».

4. Технічне блокування та кібер-протидія
- **Скарги на ворожі ресурси:** Координація дій волонтерів для масового подання скарг (репортів) на пропагандистські канали, які порушують правила платформ.
- **Злам та викриття джерел:** Фізичне припинення роботи серверів або злив даних адміністраторів ворожих ботоферм та пропагандистських ресурсів.

Суб'єкти протидії пропаганді в Україні

Ефективна протидія є результатом синергії державних органів та громадянського суспільства:
- **Державний рівень:** Центр протидії дезінформації (при РНБО) та Центр стратегічних комунікацій та інформаційної безпеки (при Мінкультури).

  Вони аналізують загрози на стратегічному рівні та видають офіційні аналітичні звіти.
- **Громадський сектор:** Волонтерські проекти (наприклад, *StopFake*, *По той бік новин*, *Детектор медіа*), які займаються щоденним розбором фейків на молекули.
- **Національний спротив:** Кожен громадянин, який дотримується режиму інформаційної тиші та не стає ретранслятором чуток, здійснює особистий внесок у безпеку держави.

Основи стратегічних комунікацій (СтратКом) — це узгоджене й синхронізоване використання всіх комунікаційних спроможностей держави (дипломатії, інформполітики, військових зв'язків та кібер-засобів) для досягнення стратегічних цілей національної безпеки та спротиву. На відміну від звичайного інформування чи точкової протидії фейкам, СтратКом діє

системно, проактивно та грає «у довгу».
У контексті національного спротиву стратегічні комунікації є каркасом, який перетворює моніторинг, аналітику та фактчекінг на потужну єдину систему захисту й наступу

Наріжні камені (Основи) стратегічної комунікації
Ефективний СтратКом будується на чотирьох базових принципах:

1. **Єдність голосу (Unity of Voice):** Усі державні інститути, військове командування та офіційні спікери мають транслювати узгоджені й такі, що не суперечать один одному, наративи. Це унеможливлює спроби ворога зіграти на внутрішніх розбіжностях.

1. **Синхронізація дій та слів (Words and Deeds):** Комунікація не існує окремо від реальності. Кожна заява має підкріплюватися реальними діями на полі бою, в економіці чи політиці (і навпаки — успішні дії мають бути правильно та вчасно прокомуніковані).

2. . **Розуміння та сегментація аудиторії:** Повідомлення для внутрішнього споживача (цивільних, військових), міжнародних партнерів та населення ворога не можуть бути однаковими. Вони адаптуються під тригери, цінності та страхи конкретної цільової групи.

3. **Проактивність (Формування порядку денного):** СтратКом не просто реагує на загрози (як-от фактчекінг після виходу фейку), а формує власний інформаційний контекст. Держава має першою повідомляти важливі новини, задаючи тон та інтерпретацію подій.

4. **Проактивність (Формування порядку денного):** СтратКом не просто реагує на загрози (як-от фактчекінг після виходу фейку), а формує власний інформаційний контекст. Держава має першою повідомляти важливі новини, задаючи тон та інтерпретацію подій.

Як СтратКом об'єднує аналітику, моніторинг та фактчекінг?
Виділені вами напрямки протидії ІПсО є інструментами, які СтратКом інтегрує у глобальну оборонну стратегію:

- **Моніторинг та аналітика (OSINT, Data Science)** є «очима та вухами» СтратКому. Вони допомагають виявити, куди саме ворог спрямовує свій удар (наприклад, б'є по темі мобілізації чи відключень світла).
- **Фактчекінг та деконструкція** — це «тактична зброя». Вони нейтралізують конкретну загрозу «тут і зараз».
- **Стратегічна комунікація** — це «генеральний штаб». Отримавши дані від аналітиків про нову ворожу кампанію, СтратКом не просто спростовує фейк, а створює комплексний довгостроковий наратив (наприклад, запускає масштабну інформаційну кампанію про важливість єдності, готує серію роз'яснювальних інтерв'ю з експертами та координує роботу з міжнародними партнерами).

Порівняння рівнів інформаційного спротиву

Рівень	Що робить?	Приклад дії

Тактичний (Фактчекінг)	Реагує на наслідки.	Спростування конкретного змонтованого відео про «прорив фронту».
Оперативний (Протидія ІПсО)	Виявляє та блокує мережі ворога.	Ліквідація мережі Telegram-каналів або ботоферм, які це відео розганяли.
Стратегічний (СтратКом)	Формує стійкість та порядок денний.	Завчасне системне навчання суспільства медіаграмотності + побудова абсолютної довіри до офіційних зведень Генштабу.

Основи лідерства у контексті національного спротиву та стратегічних комунікацій — це здатність особистості чи інституції об'єднувати людей, вести їх за собою та приймати критичні рішення в умовах високої невизначеності, стресу та інформаційного тиску.
В умовах гібридної війни лідерство перестає бути суто військовим чи політичним поняттям. **Національний спротив тримається на мережевому лідерстві**, де керівником і рушійною силою змін стає кожен фахівець на своєму місці — від командира взводу ТРО та координатора волонтерського хабу до керівника ІТ-команди чи аналітика СтратКому.

Ключові складові лідерства в умовах спротиву
Сучасна концепція лідерства під час кризи (Crisis Leadership) базується на чотирьох фундаментальних принципах:

1. **Стійкість та адаптивність (Resilience):** Здатність зберігати тверезе мислення під час критичних збоїв (обстріли, блекаути, кібератаки, втрата зв'язку) та миттєво адаптувати стратегію до нових реалій.
2. **Співпереживання та емоційний інтелект (Empathy):** Розуміння психологічного стану своєї команди чи аудиторії. Лідер у націоспротиві не просто віддає накази, а підтримує моральний дух, бореться з вигоранням підлеглих та панікою.
3. **Децентралізація та довіра (Mission Command):** В умовах динамічної війни неможливо контролювати кожен крок. Ефективний лідер делегує повноваження, виховує «лідерів на місцях» та довіряє професіоналізму своєї команди, окреслюючи лише фінальну мету.
4. **Комунікаційна прозорість (Чесність):** Лідер є головним джерелом правди. Він чітко комунікує як успіхи, так і виклики чи втрати. Саме на чесності будується абсолютна довіра, яка є основою стратегічної комунікації.

Інтеграція лідерства у систему СтратКому та захисту інформації
Лідерські якості визначають, наскільки ефективно працюватимуть усі

попередньо розглянуті нами інструменти:

- **Лідерство в аналітиці та OSINT:** Це здатність взяти на себе відповідальність за верифікацію критично важливих даних, коли від твого висновку залежить ухвалення військового чи політичного рішення.
- **Лідерство у захисті інформації:** Це жорстке та безкомпромісне впровадження протоколів безпеки (наприклад, режиму «Тиша») у своїй команді чи організації, навіть якщо це створює тимчасові незручності для персоналу.
- **Лідерство у СтратКомі:** Це вміння першим вийти в інформаційне поле під час кризи (наприклад, після важкого прильоту чи ворожої кібератаки), перехопити ініціативу у ворога, заспокоїти населення та чітко скоординувати подальші дії громадськості.

Модель лідерства: Тоталітарна вертикаль vs. Мережевий спротив

Критерій	Лідерство ворога (Тоталітарна модель)	Лідерство України (Мережева модель)
Ухвалення рішень	Сувора ієрархія. Страх виявити ініціативу. Очікування наказів «згори».	**Ініціатива знизу**. Швидкі рішення на рівні громад, волонтерів, дрібних підрозділів.
Комунікація	✕ Приховування втрат, вигадування міфічних перемог, залякування.	Взаємодія з суспільством як із партнером. Пояснення логіки дій.
Джерело сили	✕ Примус, адмінресурс, страх перед покаранням.	Спільна цінність (свобода, виживання нації), авторитет та взаємовиручка.

Процедура формування і прийняття управлінських рішень в умовах національного спротиву є критично важливим процесом, від якого залежить життєздатність держави, ефективність оборони та безпека громадян. У кризових умовах та при високому рівні невизначеності традиційні бюрократичні моделі трансформуються у гнучкі, динамічні, але суворо структуровані алгоритми.
Лідер у системі спротиву (чи то військовий командир, чи то керівник ІТ-департаменту кібербезпеки) спирається на чітку послідовність етапів, де аналітика, захист інформації та СтратКом виступають ключовими елементами.

Етапи процедури прийняття управлінських рішень у кризових умовах
1. Виявлення та діагностика проблеми (Аналітика та Моніторинг)

- **Збір первинних даних:** Використання засобів OSINT, розвідки, кібермоніторингу або систем захисту інформації для фіксації загрози (наприклад, підготовка ворогом потужної кібератаки або масштабної ІПсО).

- **Оцінка масштабів та критичності:** Визначення ступеня загрози для національної безпеки, інфраструктури чи конкретного підрозділу.

2. Формування альтернативних варіантів дій (Розробка сценаріїв)

- Лідер разом із командою експертів розробляє кілька варіантів реагування (наприклад: *Варіант А* — повна ізоляція мережі; *Варіант Б* — перехід на резервні закордонні сервери; *Варіант В* — контратака у кіберпросторі).
- На цьому етапі суворо дотримуються правила **захисту інформації**, щоб варіанти рішень не стали відомі ворогу завчасно.

3. Оцінка альтернатив та прийняття рішення (Лідерський вибір)

- Прораховуються ризики, ресурси та можливі наслідки для кожного сценарію.
- **Прийняття рішення:** Лідер бере на себе персональну відповідальність і обирає фінальний план дій. В умовах спротиву часто застосовується принцип децентралізованого управління (*Mission Command*), коли вище керівництво визначає *що* треба зробити (мету), а лідери на місцях вирішують, *як* саме.

4. Комунікація та запуск рішення в дію (СтратКом і Логістика)

- **Внутрішня комунікація:** Чітке доведення наказів до виконавців через захищені канали зв'язку.
- **Зовнішня комунікація (СтратКом):** Якщо рішення впливає на цивільне населення (наприклад, введення комендантської години чи обмежень у мережі), СтратКом оперативно пояснює логіку цього кроку, щоб упередити паніку та ворожу контрпропаганду.

5. Контроль виконання та зворотний зв'язок (Моніторинг результатів)

- Постійний аналіз того, як виконується рішення. Якщо ситуація на фронті чи в кіберпросторі динамічно змінюється, рішення миттєво коригується

Особливості прийняття рішень: Мирний час vs. Національний спротив

Характеристика	Прийняття рішень у мирний час	Прийняття рішень під час спротиву (Кризове)
Час на розробку	Тривалий (тижні, місяці), багато етапів узгоджень.	**Мінімальний** (хвилини, години). Рішення приймаються в реальному часі.
Інформаційна база	Повна, перевірена, стабільна аналітика.	**Дефіцит або надлишок спотвореної інформації** (дезінформація ворога).
Рівень ризику	Фінансовий, репутаційний (помірний).	✕ **Критичний** (загроза життю людей, втрата територій чи систем управління).

Стиль керівництва	Демократичний, колегіальний.	**Директивний (авторитарний) під час бойових дій**, але з високою автономією виконавців на місцях.

Роль попередніх елементів у процесі прийняття рішень

- **Кібербезпека та Захист інформації** гарантують, що процес обговорення та саме рішення не будуть перехоплені ворогом.
- **Протидія пропаганді** очищує інформаційне поле, щоб лідер приймав рішення на основі тверезих фактів, а не під впливом штучно створеної ворогом паніки.
- **Стратегічна комунікація** забезпечує правильне сприйняття рішення суспільством та міжнародними партнерами.
- **Лідерство** є тією силою, яка перетворює сухий алгоритм прийняття рішень на реальні, сміливі та ефективні дії команди.

Дії державних органов та населення в умовах воєнного стану в Україні регламентуються Законом України «Про правовий режим воєнного стану» та відповідними нормативно-правовими актами. Воєнний стан передбачає повну перебудову системи управління країною на військові рейки та максимальну мобілізацію цивільного населення для забезпечення національної безпеки й спротиву.

Дії та повноваження державних органів

З моменту введення воєнного стану державна влада переходить на надзвичайний режим роботи, де ключову роль відіграють **Військові адміністрації** (обласні, районні, міські), які створюються на базі відповідних держадміністрацій або за рішенням Президента.

1. Обмеження конституційних прав (виключно в межах закону)

- **Запровадження комендантської години:** Встановлення заборони на перебування на вулицях у визначений час без спеціальних перепусток.
- **Встановлення особливого режиму в'їзду/виїзду:** Обмеження свободи пересування громадян, перевірка документів, огляд речей, службових приміщень та житла громадян.
- **Трудова повинність:** Залучення працездатних осіб до суспільно корисних робіт (будівництво фортифікацій, ліквідація наслідків обстрілів).

2. Організація оборони та економіки тилу

- **Примусове відчуження майна:** Вилучення майна (транспорту, будівель) для потреб оборони за умови подальшої повної компенсації його вартості.
- **Контроль за роботою підприємств:** Військові адміністрації мають право змінювати режим роботи підприємств усіх форм власності для виробництва оборонної продукції.
- **Регулювання інформаційного простору:** Контроль за роботою ЗМІ, друкарень, інтернет-провайдерів з метою захисту державної таємниці та протидії ворожій пропаганді. Повна заборона на публікацію переміщення техніки ЗСУ та роботи ППО.

3. Забезпечення життєдіяльності та евакуація

- **Організація евакуації:** Проведення обов'язкової або примусової евакуації населення, матеріальних і культурних цінностей із зон активних бойових дій.
- **Стабілізація критичної інфраструктури:** Забезпечення роботи медичних закладів, пунктів незламності, водо-, тепло- та енергопостачання в умовах постійних атак.

Дії та правила поведінки цивільного населення

В умовах воєнного стану кожен громадянин стає учасником національного спротиву. Цивільне населення має чітко розділяти свої обов'язки на дві категорії: **особиста безпека** та **сприяння обороні**.

1. Обов'язкові правила безпеки для кожного

- **Реагування на сигнали тривоги:** Негайне переміщення в укриття (сховища, паркінги, метро) або дотримання правила «двох стін» у будинку при оголошенні повітряної чи артилерійської тривоги.
- **Дотримання комендантської години:** Перебування вдома у визначені години. Маскування світла в оселях (світломаскування) за потреби.
- **Носіння документів:** Обов'язкова наявність при собі документів, що посвідчують особу (паспорт, Дія), для безперешкодного проходження перевірок на блокпостах.

2. Інформаційна гігієна та безпека (Ключовий елемент спротиву)

- **Режим «Тиша»:** Сувора заборона на зйомку та поширення в соцмережах кадрів роботи ППО, місць прильотів ракет, пересування українських військових колон чи локацій блокпостів.
- **Фактчекінг:** Довіра виключно офіційним джерелам інформації (Генштаб ЗСУ, Офіс Президента, ОВА). Негайне припинення ретрансляції чуток та анонімних повідомлень у месенджерах.

3. Практичний внесок у національний спротив

- **Донорство та волонтерство:** Регулярна здача крові для поранених, фінансова підтримка перевірених благодійних фондів, допомога внутрішньо переміщеним особам (ВПО).
- **Кіберспротив:** Участь в ІТ-армії, надсилання даних про переміщення ворога або підозрілих осіб через офіційні чат-боти (наприклад, чат-бот *єВорог*).
- **Цивільна підготовка:** Проходження курсів тактичної медицини, домедичної допомоги, поводження зі зброєю та мінної безпеки.