**Змістовий модуль 1. Теоретичні основи кризового менеджменту у сфері національної безпеки**

**Тема 1. Вступ до кризового менеджменту у сфері національної** безпеки (ЗК 1. ЗК 6. ЗК 7. ЗК 10. СК 1. СК 4. СК 5. СК 7. СК 13. СК 16. ПРН 3. ПРН 4. ПРН 6. ПРН 8. ПРН 9. ПРН 10. ПРН 13. ПРН 14. ПРН)

1. Поняття кризового менеджменту та його значення для національної безпеки.

2. Основні принципи та етапи кризового управління.

3. Ключові суб'єкти кризового менеджменту у сфері безпеки.

4. Типологія криз: внутрішні та зовнішні, природні та техногенні.

5. Вплив кризових ситуацій на різні аспекти національної безпеки.

6. Міжнародний досвід кризового менеджменту та його застосування.

**1. Поняття кризового менеджменту та його значення для національної безпеки**

**Кризовий менеджмент** — це система управлінських рішень і дій, спрямованих на запобігання, локалізацію, подолання та мінімізацію негативних наслідків кризових ситуацій, які загрожують життєво важливим інтересам держави, суспільства або окремих його інституцій.

У сфері **національної безпеки** кризовий менеджмент охоплює як планування, так і реалізацію заходів у разі надзвичайних подій — як природного, так і антропогенного, техногенного чи соціально-політичного характеру. Його значення полягає у:

* захисті критичної інфраструктури;
* збереженні політичної стабільності;
* мінімізації людських та економічних втрат;
* забезпеченні функціонування органів державної влади та сектору безпеки.

**Кризовий менеджмент** у сучасному розумінні є міждисциплінарною галуззю, яка поєднує елементи стратегічного управління, безпекових досліджень, адміністративного права, психології масової поведінки та логістики. Він формується як сукупність управлінських рішень, технологій, ресурсів та координаційних процедур, що активуються на всіх рівнях державного і місцевого управління в умовах загрози або настання надзвичайної ситуації.

Ключова мета кризового менеджменту — **відновити контроль над ситуацією, стабілізувати систему та мінімізувати втрати**. У сфері **національної безпеки** цей процес набуває системного характеру та охоплює:

* **Превентивну фазу** (виявлення та оцінка ризиків, формування сценаріїв реагування);
* **Активну фазу** (оперативне реагування, забезпечення стабільності, координація ресурсів);
* **Посткризову фазу** (відновлення систем життєдіяльності, аналіз ефективності дій, адаптація стратегій).

**Значення кризового менеджменту для національної безпеки:**

1. **Захист критичної інфраструктури.**
Кризовий менеджмент забезпечує своєчасне реагування на загрози об'єктам стратегічного значення — енергосистемам, транспортним вузлам, системам водопостачання, зв'язку тощо. У період війни чи терористичних загроз ці об'єкти є першочерговими мішенями, і їх захист — це питання не лише економіки, а й виживання держави.
2. **Збереження політичної стабільності.**
Кризи — це випробування для легітимності влади. Ефективні дії державних інституцій у критичні моменти зміцнюють довіру громадян, знижують ризик паніки, протестів чи внутрішніх деструктивних процесів. Недієздатність влади в кризі, навпаки, породжує соціальну дестабілізацію та політичні загрози.
3. **Мінімізація людських та економічних втрат.**
Кожна хвилина затримки у реагуванні на катастрофу призводить до додаткових жертв, втрат майна та поглиблення соціально-економічної кризи. Кризовий менеджмент дозволяє оптимізувати розподіл ресурсів, евакуацію, медичне забезпечення, психологічну підтримку тощо.
4. **Забезпечення безперервності державного управління.**
Навіть у надзвичайних умовах державна система має залишатися функціональною: органи влади повинні зберігати керованість, ухвалювати рішення, інформувати громадськість, координувати дії з міжнародними партнерами. Ефективний кризовий менеджмент передбачає наявність резервних планів, цифрових інструментів управління та процедур швидкої мобілізації.

Кризовий менеджмент — це фундаментальна складова національної безпеки, яка дозволяє не лише реагувати на загрози, а й підвищувати стійкість держави до майбутніх викликів. Його ефективність визначає здатність держави зберігати суверенітет, функціональність та соціальну згуртованість у будь-яких обставинах.

**2. Основні принципи та етапи кризового управління**

**Принципи:**

* **Превентивність** — перевага запобігання над реагуванням.
* **Оперативність** — швидкість прийняття та реалізації рішень.
* **Системність** — інтеграція всіх рівнів управління (місцевого, регіонального, національного).
* **Координація** — взаємодія між державними органами, бізнесом, міжнародними партнерами.
* **Прозорість і відповідальність** — довіра суспільства до управлінських рішень.

**Етапи кризового управління:**

1. **Ідентифікація ризиків** — виявлення потенційних загроз.
2. **Планування** — розробка сценаріїв, алгоритмів дій та розподіл ресурсів.
3. **Моніторинг і попередження** — спостереження за розвитком ситуації.
4. **Реагування** — дії під час кризи (евакуація, локалізація, забезпечення безпеки).
5. **Відновлення** — відбудова інфраструктури, повернення до нормального функціонування.
6. **Аналіз та оцінка** — вивчення ефективності дій і внесення корективів у стратегії.

***Принципи кризового управління***

***Превентивність***

Цей принцип передбачає, що найефективніший спосіб подолати кризу — не допустити її виникнення або мінімізувати ймовірність її ескалації. Передбачає розробку систем раннього попередження, регулярний аналіз загроз, розробку превентивних стратегій, навчань і симуляцій. Наприклад, до введення воєнного стану держава має заздалегідь активізувати оборонні та мобілізаційні ресурси.

***Оперативність***

У кризових ситуаціях кожна хвилина має вирішальне значення. Оперативність означає здатність приймати обґрунтовані рішення та негайно їх реалізовувати в умовах високої невизначеності. Це стосується як евакуації населення, так і мобілізації допомоги. Високий рівень оперативності базується на підготовлених протоколах, тренованих командах та наявності резервних планів.

***Системність***

Криза впливає на багато сфер одночасно: охорону здоров’я, транспорт, енергетику, комунікації, управління. Тому реакція має бути міжсекторальною, об'єднувати ресурси та зусилля різних органів влади, громадянського суспільства, приватного сектору. Системний підхід гарантує узгодженість дій на всіх рівнях: від місцевого до національного.

***Координація***

Кризове управління потребує злагодженої співпраці між усіма учасниками процесу — органами державної влади, силовими структурами, міжнародними партнерами, громадськими організаціями та ЗМІ. Координація дає змогу уникати дублювання зусиль, конфліктів повноважень та інформаційного вакууму. Наприклад, у надзвичайній ситуації на атомній електростанції необхідна взаємодія МВС, ДСНС, МОЗ, місцевих адміністрацій та МАГАТЕ.

***Прозорість і відповідальність***

Кризи супроводжуються підвищеною напругою в суспільстві. Успіх управлінських рішень значною мірою залежить від рівня довіри громадян. Прозорість передбачає відкриту комунікацію, надання достовірної інформації, обґрунтування рішень. Відповідальність — це чіткий розподіл повноважень і обов’язків, а також забезпечення контролю за виконанням рішень.

***Етапи кризового управління***

***Ідентифікація ризиків***

На цьому етапі здійснюється аналіз потенційних загроз — як зовнішніх (військові, терористичні атаки), так і внутрішніх (соціальні протести, епідемії). Використовуються інструменти стратегічного аналізу, прогнозування, систем моніторингу. Ціль — визначити можливі сценарії розвитку подій та оцінити їхню ймовірність і масштаб впливу.

***Планування***

Передбачає створення конкретних планів реагування на кожен з можливих сценаріїв. Розробляються алгоритми дій, розподіляються повноваження, ресурси та відповідальні структури. Включає підготовку персоналу, матеріально-технічне забезпечення, юридичні механізми. Приклад — «План евакуації» для зони потенційного затоплення або бойових дій.

***Моніторинг і попередження***

На цьому етапі впроваджуються системи раннього попередження (наприклад, датчики, супутниковий моніторинг, інформаційні системи) та комунікаційні канали. Постійно відстежується динаміка обстановки. За потреби оновлюються плани реагування. Такі системи мають критичне значення для реагування на стихійні лиха, кібератаки чи військові загрози.

***Реагування***

Це активна фаза дій безпосередньо під час кризи. Може включати евакуацію, надання першої медичної допомоги, введення надзвичайного стану, перекриття транспортних артерій, ліквідацію осередків загрози тощо. На цьому етапі критично важливо зберігати контроль, дотримуватись чітко розроблених протоколів та забезпечувати координацію між службами.

***Відновлення***

Після завершення гострої фази необхідно відновити функціонування основних інфраструктур, повернути населення до нормального ритму життя, забезпечити житло, медичне обслуговування, транспорт. Також триває процес психологічної, економічної та адміністративної реабілітації. Приклад — програми відбудови зруйнованих громад після бойових дій або стихійного лиха.

***Аналіз та оцінка***

Після завершення кризи проводиться всебічний аналіз ефективності прийнятих рішень, виявлення слабких місць, системних помилок і коригування нормативної та організаційної бази. Результати цього етапу стають основою для вдосконалення стратегій реагування та підвищення готовності до нових загроз.

Принципи та етапи кризового управління є взаємозалежними елементами єдиної системи. Від ефективності реалізації кожного з них залежить здатність держави швидко адаптуватись до викликів, зберегти стабільність та забезпечити безпеку громадян. У сучасному світі кризовий менеджмент має ґрунтуватися на гнучкості, проактивності та міжсекторальній взаємодії.

**3. Ключові суб'єкти кризового менеджменту у сфері безпеки**

* **Президент України** — головнокомандувач, координує дії у надзвичайних ситуаціях.
* **Рада національної безпеки і оборони (РНБО)** — стратегічне планування, міжвідомча координація.
* **Кабінет Міністрів України** — організація дій урядових структур.
* **Служба безпеки України (СБУ)** — протидія диверсіям, тероризму, зовнішнім загрозам.
* **Державна служба з надзвичайних ситуацій (ДСНС)** — реагування на техногенні та природні катастрофи.
* **Міністерство оборони, Нацполіція, Нацгвардія, органи місцевого самоврядування, НУО** — підтримка в операціях безпеки, евакуації, інформуванні населення.

У системі національної безпеки кризовий менеджмент реалізується завдяки чіткій взаємодії між державними органами, силовими структурами, органами місцевого самоврядування, а також суб’єктами громадянського суспільства. Кожен із них має чітко визначені повноваження, зону відповідальності та функціональні обов’язки. Їх скоординована робота дозволяє ефективно реагувати на загрози, забезпечувати життєздатність держави в умовах кризи та мінімізувати негативні наслідки.

**Президент України**

Президент як глава держави і Верховний Головнокомандувач Збройних Сил України має ключову роль у формуванні та реалізації політики національної безпеки. У кризових ситуаціях Президент:

* оголошує надзвичайний або воєнний стан (за погодженням із Верховною Радою);
* здійснює загальне стратегічне керівництво у сфері безпеки та оборони;
* координує діяльність органів виконавчої влади та військового командування;
* очолює Раду національної безпеки і оборони.

У період масштабної кризи саме Президент є центром політичної відповідальності за ухвалення рішень на найвищому рівні.

**Рада національної безпеки і оборони України (РНБО)**

РНБО — консультативно-дорадчий орган при Президентові, який розробляє та узгоджує стратегії безпеки, координує дії силових і спеціалізованих структур.

У сфері кризового менеджменту РНБО:

* визначає пріоритети державної політики з безпеки;
* ініціює та координує міжвідомчі заходи в умовах надзвичайної ситуації;
* затверджує рішення щодо мобілізації, санкцій, обмежень тощо.

Прикладом є діяльність РНБО під час повномасштабного вторгнення РФ у 2022 році, коли орган забезпечував комплексне управління національною безпекою.

**Кабінет Міністрів України**

КМУ забезпечує виконання політичних рішень у практичній площині, зокрема через підпорядковані міністерства та центральні органи виконавчої влади. У кризовому управлінні Кабмін:

* координує оперативні дії виконавчої влади;
* затверджує плани реагування, мобілізаційні програми, евакуаційні заходи;
* виділяє ресурси з резервного фонду державного бюджету;
* організовує міжнародну допомогу через МЗС, Міноборони, МОЗ тощо.

**Служба безпеки України (СБУ)**

Основний суб’єкт у боротьбі з гібридними, терористичними та інформаційними загрозами. СБУ виконує такі функції в умовах кризи:

* виявляє та запобігає диверсіям, шпигунству, саботажу;
* протидіє кіберзагрозам і терористичним атакам;
* координує дії з охорони державної таємниці;
* бере участь у спеціальних операціях і контррозвідувальній роботі.

СБУ також забезпечує аналітичне супроводження рішень вищого керівництва держави.

**Державна служба України з надзвичайних ситуацій (ДСНС)**

Центральний орган виконавчої влади, відповідальний за реагування на природні, техногенні, екологічні катастрофи. Основні завдання ДСНС:

* організація аварійно-рятувальних та евакуаційних робіт;
* забезпечення цивільного захисту населення;
* попередження та гасіння пожеж, ліквідація наслідків аварій;
* створення систем раннього попередження та навчання населення правилам безпеки.

У тісній співпраці з місцевими адміністраціями ДСНС реалізує заходи з відновлення критичної інфраструктури після кризи.

**Міністерство оборони, Збройні Сили України (ЗСУ)**

У воєнних та прикордонних кризах саме ЗСУ виступають основним гарантом територіальної цілісності та захисту населення. МО координує:

* мобілізацію людських і матеріальних ресурсів;
* участь армії у ліквідації наслідків надзвичайних ситуацій (саперні роботи, охорона об’єктів);
* оперативне реагування на зовнішні загрози.

**Національна поліція та Національна гвардія України**

Забезпечують правопорядок, охорону громадської безпеки, контроль за дотриманням режиму надзвичайного стану. Їх роль включає:

* патрулювання, охорону громадського порядку;
* участь у евакуації;
* боротьбу з мародерством, панікою, дезінформацією.

**Органи місцевого самоврядування (ОМС)**

Грають вирішальну роль у практичному забезпеченні безпеки населення на територіальному рівні:

* координують розміщення евакуйованих осіб;
* організовують локальні служби підтримки;
* забезпечують доступ до медичних, освітніх та соціальних послуг;
* взаємодіють із волонтерами та благодійними фондами.

**Недержавні організації (НУО), волонтери, приватний сектор**

Сектор громадянського суспільства стає надзвичайно активним у кризових умовах:

* забезпечення гуманітарної допомоги, евакуаційного транспорту;
* аналітична та інформаційна підтримка (OSINT, розслідування, карти безпеки);
* технічна допомога (дрони, радіозв’язок, медичні засоби).

Система кризового менеджменту в Україні є багаторівневою і міжвідомчою. Її ефективність залежить від здатності усіх суб'єктів — державних, муніципальних та громадських — діяти скоординовано, оперативно і прозоро. Кожен учасник має свою унікальну функцію, але лише за умови інтеграції їхніх зусиль можна гарантувати реальну безпеку в умовах кризи.

**4. Типологія криз: внутрішні та зовнішні, природні та техногенні**

**За джерелом походження:**

* **Внутрішні** — політичні, соціальні кризи, громадські заворушення, терористичні акти.
* **Зовнішні** — військова агресія, гібридні атаки, зовнішній тиск (санкції, енергетичний шантаж).

**За природою:**

* **Природні** — повені, землетруси, епідемії (приклад: COVID-19).
* **Техногенні** — аварії на АЕС, транспортні катастрофи, витоки небезпечних речовин.

**Змішані форми** — сучасні гібридні кризи поєднують кілька факторів (наприклад, війна РФ проти України має одночасно військовий, інформаційний, енергетичний та гуманітарний виміри).

Типологізація криз є фундаментально важливою для побудови ефективної системи кризового менеджменту. Залежно від джерел виникнення, природи впливу та масштабу, кризи мають різну динаміку розвитку, вимагають специфічних управлінських рішень та залучення різних інституцій.

**За джерелом походження**

1. **Внутрішні кризи**
Це такі ситуації, що виникають у межах країни внаслідок внутрішніх політичних, соціальних, економічних чи адміністративних суперечностей. Вони загрожують стабільності державної влади, правопорядку та довірі до інституцій.

**Основні типи внутрішніх криз:**

* **Політичні кризи** — урядові конфлікти, дестабілізація влади, втручання у виборчі процеси.
* **Соціальні кризи** — масові протести, страйки, міжетнічні або міжконфесійні конфлікти.
* **Терористичні загрози** — атаки на об’єкти критичної інфраструктури, масові теракти в публічних місцях.
* **Кризи правопорядку** — сплески злочинності, насильства, вуличні заворушення.

**Приклад:** події на Майдані в 2013–2014 роках є прикладом політичної та соціальної кризи, що призвела до зміни уряду та радикального переосмислення безпекової політики.

1. **Зовнішні кризи**
Виникають внаслідок дій або політик інших держав, міжнародних акторів або глобальних процесів, що безпосередньо загрожують національним інтересам.

**Ключові форми зовнішніх криз:**

* **Військова агресія** — збройне вторгнення, ракетні обстріли, блокади.
* **Гібридні атаки** — кібератаки, інформаційні кампанії, втручання у вибори.
* **Зовнішньоекономічний тиск** — санкції, маніпуляції з цінами на енергоносії, торговельні війни.
* **Міграційні хвилі**, спровоковані штучно або через конфлікти.

**Приклад:** повномасштабне вторгнення Росії в Україну у 2022 році є класичним прикладом зовнішньої військової та гібридної кризи, яка спричинила значні соціально-економічні та гуманітарні наслідки.

**За природою (характером походження)**

1. **Природні кризи**
Це надзвичайні ситуації, що виникають внаслідок дії природних факторів. Вони зазвичай мають раптовий характер і значний масштаб впливу.

**Типи природних криз:**

* Повені, паводки
* Землетруси, зсуви
* Урагани, смерчі
* Епідемії та пандемії (COVID-19, H1N1)

**Приклад:** пандемія COVID-19 у 2020–2022 роках стала глобальною кризою, яка призвела до масштабних людських жертв, економічного спаду та трансформації систем охорони здоров’я.

1. **Техногенні кризи**
Виникають внаслідок людської діяльності, зокрема через аварії, помилки проєктування, порушення правил експлуатації або навмисні дії.

**Типи техногенних криз:**

* Аварії на промислових об’єктах (АЕС, заводи)
* Катастрофи на транспорті (залізничні, авіаційні, морські)
* Витоки хімічних або біологічно небезпечних речовин
* Пожежі на інфраструктурних об’єктах

**Приклад:** вибух на Чорнобильській АЕС у 1986 році є одним із наймасштабніших техногенних інцидентів в історії людства, що мав транскордонні наслідки.

**Змішані (комбіновані, гібридні) кризи**

У сучасному світі дедалі частіше виникають **змішані кризи**, які поєднують елементи кількох типів і вимагають багаторівневої реакції. Гібридність полягає в одночасній дії воєнних, політичних, інформаційних, гуманітарних та енергетичних компонентів.

**Характеристики:**

* Високий рівень невизначеності;
* Використання сучасних технологій (кібератаки, маніпуляції у ЗМІ);
* Комплексний вплив на всі сектори безпеки.

**Приклад:**
Російська агресія проти України є класичним прикладом гібридної кризи, яка включає:

* **військову складову** (окупація територій, бойові дії);
* **інформаційну** (дезінформація, психологічний тиск);
* **енергетичну** (атаки на ТЕС, ГЕС, газову інфраструктуру);
* **гуманітарну** (вимушене переміщення мільйонів громадян);
* **екологічну** (підрив Каховської ГЕС, замінування лісів).

Системна класифікація криз є необхідною передумовою для вибору адекватної стратегії реагування. Внутрішні та зовнішні, природні й техногенні загрози вимагають різних управлінських підходів, інструментів і суб’єктів реалізації. Розуміння складної природи сучасних криз дозволяє розробляти адаптивні, скоординовані та ефективні механізми кризового менеджменту на національному рівні.

**5. Вплив кризових ситуацій на різні аспекти національної безпеки**

Кризи мають багатовимірний вплив:

* **Політична безпека** — загроза стабільності влади, спроби дестабілізації.
* **Економічна безпека** — порушення логістики, інфляція, втрата ВВП.
* **Соціальна безпека** — зростання безробіття, недовіра до держави.
* **Інформаційна безпека** — поширення фейків, дезінформація, кібератаки.
* **Екологічна безпека** — руйнівні наслідки для довкілля (наприклад, після підриву Каховської ГЕС).
* **Гуманітарна безпека** — переміщення населення, кризи біженців, вразливість громадян.

Кризові ситуації мають комплексний характер і впливають не лише на безпосередні сфери загрози, а й на всю систему національної безпеки. Вони викликають каскадні ефекти, які взаємопов’язані між собою, охоплюючи політичну, економічну, соціальну, інформаційну, екологічну та гуманітарну безпеку. Оцінка такого впливу є важливою умовою для ефективного планування кризового реагування.

 ***Політична безпека***

Кризи можуть дестабілізувати політичну систему, послабити легітимність влади та створити умови для політичної радикалізації, спроб державного перевороту або втрати керованості державними процесами.

**Прояви:**

* Падіння рівня довіри до уряду;
* Загострення протистояння між політичними силами;
* Використання кризи опозицією для зміни влади;
* Зовнішній тиск через дипломатичні чи гібридні інструменти.

**Приклад:** соціальні протести у Франції через пенсійну реформу або політична криза в Шрі-Ланці у 2022 р., викликана економічною нестабільністю.

 ***Економічна безпека***

Кризи часто паралізують ключові сектори економіки, призводять до втрати інвестицій, зниження виробництва, порушення ланцюгів постачання та падіння державних доходів.

**Прояви:**

* Інфляція, девальвація національної валюти;
* Відтік капіталу, скорочення іноземних інвестицій;
* Зниження ВВП і платоспроможності населення;
* Енергетичні кризи, залежність від імпорту.

**Приклад:** внаслідок повномасштабного вторгнення РФ, ВВП України у 2022 р. знизився на понад 29,1%, що стало найбільшим падінням за роки незалежності.

 ***Соціальна безпека***

Соціальна безпека страждає від зростання нерівності, безробіття, погіршення доступу до освіти, медицини та соціального захисту. Кризи підривають громадську згуртованість і сприяють соціальній фрагментації.

**Прояви:**

* Масове безробіття та еміграція трудових ресурсів;
* Зниження рівня соціального капіталу;
* Поширення протестних настроїв;
* Соціальна ізоляція та зростання злочинності.

**Приклад:** під час пандемії COVID-19 було зафіксовано різке зростання соціальної вразливості вразливих груп, зокрема людей похилого віку, людей з інвалідністю та тимчасово безробітних.

 ***Інформаційна безпека***

Кризи — благодатне середовище для інформаційної дезорієнтації, поширення фейків, пропаганди та кібератак. Інформаційний простір стає інструментом впливу, паніки або мобілізації.

**Прояви:**

* Кіберзлочинність, атаки на державні ресурси;
* Масові кампанії дезінформації;
* Маніпуляції в соціальних мережах;
* Недовіра до офіційних джерел інформації.

**Приклад:** під час агресії РФ проти України спостерігалося масштабне поширення фейкових повідомлень про втрати, капітуляцію, штучні «референдуми» тощо.

 ***Екологічна безпека***

Деякі кризи створюють довготривалу загрозу довкіллю та здоров’ю населення. Йдеться про екологічні катастрофи, знищення природних ресурсів, отруєння води, ґрунтів, повітря.

**Прояви:**

* Забруднення екосистем небезпечними речовинами;
* Знищення лісів, заповідників, водойм;
* Радіаційна або хімічна небезпека;
* Порушення балансу екосистем.

**Приклад:** підрив Каховської ГЕС у 2023 р. спричинив затоплення десятків населених пунктів, знищення сільськогосподарських угідь, масову загибель риби та птахів, а також загрозу техногенного забруднення.

 ***Гуманітарна безпека***

Цей вимір охоплює захист життя, здоров’я та гідності людини в умовах надзвичайних ситуацій. Кризові обставини можуть порушити базові права людини й створити масштабні гуманітарні катастрофи.

**Прояви:**

* Вимушене переміщення населення;
* Поява біженців і внутрішньо переміщених осіб (ВПО);
* Недоступність медичної, психологічної та продовольчої допомоги;
* Посилення вразливості дітей, жінок, осіб з інвалідністю.

**Приклад:** війна в Україні спричинила понад 6 млн ВПО, мільйони людей залишилися без доступу до медичних послуг, житла та роботи, особливо в зоні бойових дій.

Кризи мають системний вплив на всі компоненти національної безпеки, формуючи мультиплікативні загрози. Ефективна стратегія управління кризами повинна враховувати міжсекторальні взаємозв’язки та бути орієнтованою не лише на фізичне усунення загрози, а й на збереження соціальної цілісності, довіри та стабільного розвитку держави.

**6. Міжнародний досвід кризового менеджменту та його застосування**

**США:**

* Агентство FEMA (Federal Emergency Management Agency) забезпечує координацію національного реагування на надзвичайні ситуації.
* Сильна система раннього попередження та взаємодії між штатами.

**ЄС:**

* Механізм цивільного захисту ЄС забезпечує підтримку країн-членів у разі катастроф.
* Система CBRN-реагування (хімічна, біологічна, радіологічна, ядерна безпека).

**Ізраїль:**

* Постійна готовність до воєнних і терористичних загроз, високий рівень залучення цивільного населення, розвинені протоколи укриття, оповіщення та евакуації.

**Застосування для України:**

* Врахування міжнародного досвіду може посилити координацію на всіх рівнях, сприяти цифровізації управління, розвитку резервних систем та оновлення законодавчої бази.

Міжнародна практика управління кризами демонструє широкий спектр підходів, інституційних моделей та технологічних інструментів, які можна адаптувати до українських умов. Вивчення таких моделей дозволяє не лише покращити внутрішні механізми реагування, а й інтегрувати українську систему безпеки до європейських і глобальних структур реагування.

**США — модель централізованого реагування через FEMA**

**Federal Emergency Management Agency (FEMA)** є основним державним органом, відповідальним за реагування на надзвичайні ситуації у США. Агентство діє у структурі Міністерства внутрішньої безпеки та забезпечує міжштатну координацію у разі катастроф природного, техногенного чи соціального характеру.

**Ключові елементи:**

* **Національна система реагування (NIMS):** стандартизований підхід до управління кризами, який забезпечує взаємосумісність усіх служб (пожежних, медичних, поліції, армії).
* **Система раннього попередження:** поєднання супутникового моніторингу, штучного інтелекту, комунікаційних платформ для оповіщення громадськості.
* **Фінансова допомога населенню:** FEMA надає гранти, житло, відновлювальні фонди постраждалим.

**Значення для України:** впровадження єдиної цифрової платформи з координації дій, розробка уніфікованих процедур та навчання місцевих органів за моделлю NIMS можуть посилити готовність держави до масштабних криз.

**Європейський Союз — система солідарного реагування**

**Механізм цивільного захисту ЄС** (EU Civil Protection Mechanism) дозволяє країнам-членам та державам-партнерам (у тому числі Україні) швидко реагувати на надзвичайні події за принципом солідарності.

**Основні елементи:**

* **Резерви rescEU:** стратегічні запаси медичних засобів, обладнання, польових госпіталів, авіації для гасіння пожеж.
* **Координаційний центр (ERCC):** діє 24/7, збирає інформацію, координує міжнародну допомогу, направляє експертів.
* **CBRN-готовність:** спеціалізовані групи реагування на хімічні, біологічні, радіологічні та ядерні загрози (CBRN), з чіткими протоколами безпеки.

**Значення для України:** розширення участі у Механізмі цивільного захисту, інституційна інтеграція до CBRN-структур ЄС, формування національного резерву за прикладом rescEU є стратегічними напрямами євроінтеграції в сфері безпеки.

**Ізраїль — приклад тотальної мобілізації суспільства**

Ізраїль має унікальний досвід управління безпековими кризами, що поєднує технологічну оснащеність, централізоване управління та активну участь громадян у системі національної безпеки.

**Особливості:**

* **Система укриттів та оповіщення:** кожен населений пункт має інтегровану систему сигналізації, а будівництво нових житлових об’єктів передбачає обов’язкове бомбосховище.
* **Оперативна служба «Пікуд а-Ореф»** відповідає за цивільну оборону, навчає населення діям у кризі, забезпечує розподіл засобів захисту.
* **Залучення добровольців:** система резервістів та волонтерів у разі війни або теракту швидко активується для підтримки основних служб.

**Значення для України:** розвиток територіальної оборони, підвищення ролі громадян у системі національного спротиву, стандарти укриттів, масове навчання населення діям у надзвичайних ситуаціях є критично важливими в умовах постійних загроз.

**Застосування міжнародного досвіду в Україні**

Урахування моделей США, ЄС та Ізраїлю дозволяє сформувати в Україні **гібридну систему кризового управління**, яка поєднує:

* **Централізоване стратегічне керівництво** (на зразок FEMA);
* **Міжрегіональну та міждержавну координацію** (через участь у механізмах ЄС);
* **Інклюзивну безпекову культуру та готовність населення** (за ізраїльським зразком).

**Пріоритетні напрями адаптації:**

* Створення єдиного кризового центру національного рівня з цифровими інструментами управління;
* Впровадження національної системи раннього попередження;
* Розробка законодавства щодо цивільного захисту, укриттів, резервних ресурсів;
* Навчання персоналу за міжнародними стандартами;
* Формування довгострокових міжнародних партнерств у сфері безпеки.

Міжнародний досвід показує, що успішне управління кризами потребує не лише ресурсів, а й інституційної зрілості, високої мобільності системи управління та довіри суспільства. Інтеграція кращих практик у національний контекст дозволить Україні зміцнити свою безпекову архітектуру та сформувати сталу модель кризової стійкості.

**Тема 2. Класифікація та ідентифікація загроз національній безпеці (**ЗК 1. ЗК 6. ЗК 7. ЗК 10. СК 1. СК 4. СК 5. СК 7. СК 13. СК 16. ПРН 3. ПРН 4. ПРН 6. ПРН 8. ПРН 9. ПРН 10. ПРН 13. ПРН 14 )

1. Поняття загроз національній безпеці та їх основні види.
2. Методики ідентифікації та оцінки загроз.
3. Розподіл загроз за рівнем впливу та ступенем небезпеки.
4. Вплив технологічних змін на формування нових загроз.
5. Огляд найбільш актуальних загроз для національної безпеки (кіберзагрози, тероризм, економічні кризи).
6. Інструменти для моніторингу та раннього попередження загроз.

**1. Поняття загроз національній безпеці та їх основні види**

**Загроза національній безпеці** — це сукупність умов і факторів, що створюють реальну або потенційну небезпеку для життєво важливих інтересів держави, суспільства та громадян, порушують або унеможливлюють нормальне функціонування системи безпеки.

**Основні види загроз:**

* **Політичні:** спроби дестабілізації влади, підрив державного суверенітету, втручання у вибори.
* **Військові:** збройна агресія, терористичні акти, військово-технічний тиск.
* **Економічні:** енергетична залежність, фінансові кризи, санкції, зовнішній борг.
* **Соціальні:** масові заворушення, протестна активність, міграційна напруга.
* **Інформаційні:** кіберзагрози, дезінформація, маніпуляція свідомістю громадян.
* **Екологічні:** техногенні катастрофи, забруднення довкілля, кліматичні зміни.

*Начало формы*

***Поняття загроз національній безпеці***

**Загроза національній безпеці** — це сукупність реальних або потенційних обставин, дій, процесів чи явищ, які створюють небезпеку для життєво важливих інтересів держави, суспільства та окремих громадян, підривають суверенітет, територіальну цілісність, стабільність політичної системи, економічну та соціальну стабільність, екологічну рівновагу й основоположні права людини.

Національна безпека охоплює всі сфери життєдіяльності держави, а загрози, які постають перед нею, відображають динаміку змін у політичному, економічному, соціальному, інформаційному та природному середовищах.

***Основні види загроз національній безпеці***

1. **Політичні загрози**
Це загрози, що стосуються функціонування політичних інститутів, системи державного управління, легітимності влади, міжнародної суб'єктності держави.

**Прояви:**

* Підрив державного суверенітету (наприклад, через зовнішній вплив або спроби створення сепаратистських утворень);
* Втручання у внутрішню політику з боку іноземних акторів;
* Криза легітимності інституцій влади (масові протести, делегітимація виборів).

Приклад**:** підтримка Росією проросійських політичних сил в Україні з метою зміни геополітичного вектору розвитку держави.

***Військові загрози***Охоплюють ризики, пов’язані із застосуванням або загрозою застосування збройної сили проти держави, її союзників, або внутрішніх військових конфліктів.

**Прояви:**

* Пряма військова агресія (як у випадку повномасштабного вторгнення РФ в Україну);
* Терористичні акти, діяльність незаконних воєнізованих формувань;
* Нарощування озброєнь та військовий тиск з боку інших держав;
* Використання найманців, гібридних технологій ведення війни.

**Важливо:** військові загрози часто супроводжуються політичними, економічними й інформаційними компонентами, утворюючи комплексні (гібридні) виклики.

***Економічні загрози***Це порушення стабільності функціонування національної економіки, критичних ринків і фінансової системи, що призводять до втрати державного контролю над економічними процесами.

**Прояви:**

* Енергетична залежність від монопольних постачальників (наприклад, від російського газу);
* Фінансові кризи, відтік капіталу, девальвація валюти;
* Зовнішній борговий тиск;
* Санкції, обмеження міжнародної торгівлі.

**Наслідки:** зниження рівня добробуту населення, соціальна напруга, зменшення можливостей фінансування сектору безпеки.

***Соціальні загрози***Охоплюють ризики, що порушують соціальну стабільність, викликають масові заворушення, протести, кризу довіри до державних інституцій.

**Прояви:**

* Високе безробіття, нерівність доходів, зниження соціальних стандартів;
* Масова міграція, внутрішнє переміщення через конфлікти або економічні труднощі;
* Етнічна, релігійна або мовна напруга;
* Протести та страйки, радикалізація молоді.

Приклад**:** у 2022–2023 роках понад 6 млн внутрішньо переміщених осіб в Україні створили нові виклики для систем охорони здоров’я, житлової політики та соціального захисту.

***Інформаційні загрози***Пов’язані з маніпулюванням масовою свідомістю, кіберзлочинністю, підривом інформаційної безпеки та зниженням довіри до офіційних джерел.

**Прояви:**

* Поширення фейків, дезінформаційних кампаній;
* Кіберзлочини проти державних органів, ЗМІ, інфраструктури;
* Хакерські атаки, злам державних реєстрів;
* Підривна діяльність через соціальні мережі.

Приклад**:** російські інформаційні кампанії, спрямовані на дестабілізацію України, створення паніки, делегітимізацію ЗСУ, поширення фейкових новин.

***Екологічні загрози***Це процеси, які загрожують навколишньому середовищу, здоров’ю населення та екологічній рівновазі. Вони можуть бути як природного, так і техногенного походження.

**Прояви:**

* Викиди отруйних речовин, аварії на промислових об’єктах;
* Забруднення повітря, води, ґрунтів;
* Знищення природних ресурсів;
* Наслідки кліматичних змін (посухи, паводки, пожежі).

Приклад**:** підрив Каховської ГЕС у 2023 році спричинив масштабну екологічну катастрофу — затоплення територій, загибель фауни, знищення агросектору на півдні України.

Загрози національній безпеці мають поліструктурний характер і вимагають системного моніторингу, оцінки та координації зусиль на всіх рівнях державного управління. Ефективне виявлення, класифікація та запобігання цим загрозам є ключовим завданням як для органів безпеки, так і для всієї системи публічного управління.

1. **Методики ідентифікації та оцінки загроз**

Ефективне управління загрозами потребує їх своєчасної ідентифікації та кількісно-якісної оцінки. Найбільш поширені методики:

* **SWOT-аналіз** (Strengths, Weaknesses, Opportunities, Threats): дозволяє виявити сильні та слабкі сторони держави у контексті наявних загроз.
* **PEST-аналіз** (Political, Economic, Social, Technological): визначає зовнішні фактори, що впливають на безпекове середовище.
* **Оцінка ризиків**: розрахунок ймовірності реалізації загрози та рівня її наслідків.
* **Метод експертного оцінювання:** залучення спеціалістів для комплексної інтерпретації багатофакторних ризиків.
* **Моніторинг відкритих джерел (OSINT):** збирання інформації з медіа, соціальних мереж, аналітичних платформ.

Своєчасне виявлення, класифікація та оцінка загроз є критично важливими складовими системи національної безпеки. З огляду на зростання кількості багатофакторних, гібридних і транснаціональних викликів, державам необхідно використовувати системні та багаторівневі підходи до аналізу загроз. Нижче подано розгорнутий опис основних сучасних методик, які використовуються в сфері стратегічної безпеки.

 ***SWOT-аналіз* (Strengths, Weaknesses, Opportunities, Threats)**

Цей метод дозволяє здійснити комплексну оцінку безпекової ситуації шляхом виокремлення чотирьох ключових блоків:

* **S (Strengths)** – сильні сторони держави у сфері безпеки (наприклад, боєздатні ЗСУ, підтримка міжнародних партнерів);
* **W (Weaknesses)** – внутрішні слабкі місця (корупція в органах влади, фрагментація інституцій);
* **O (Opportunities)** – потенційні можливості для посилення безпеки (наприклад, вступ до безпекових альянсів, інновації у сфері оборони);
* **T (Threats)** – зовнішні або внутрішні загрози (військова агресія, кіберзлочинність, економічна залежність).

SWOT-аналіз дозволяє не тільки структурувати загрози, а й пов’язати їх з потенціалом реагування держави.

 ***PEST-аналіз* (Political, Economic, Social, Technological)**

Цей інструмент орієнтований на оцінку впливу **зовнішніх факторів** на національну безпеку. Він є важливим на етапі стратегічного планування:

* **P (Political):** міжнародна політична кон’юнктура, геополітичне становище, зовнішні загрози, внутрішня стабільність;
* **E (Economic):** фінансові ризики, санкції, залежність від імпорту, енергетична безпека;
* **S (Social):** демографічні процеси, міграція, соціальна нерівність, протестна активність;
* **T (Technological):** рівень розвитку інфраструктури, цифрова безпека, штучний інтелект.

**PEST-аналіз (Political, Economic, Social, Technological)** — це стратегічний інструмент оцінки впливу зовнішнього середовища на стан національної безпеки. Його використання дозволяє систематизувати зовнішні загрози, виявити довготривалі тенденції, розробити сценарії розвитку подій та адаптувати політику безпеки до умов, що змінюються.

**P — Political (політичні фактори)**

**Сутність:** охоплює політичну стабільність, ефективність державних інституцій, міжнародні відносини, участь у безпекових альянсах, ризики втручання ззовні.

**Загрози та виклики:**

* Геополітична напруженість (наприклад, агресивна політика РФ у Східній Європі);
* Втручання у виборчі процеси, спроби дестабілізації з боку третіх країн;
* Зниження впливу міжнародних інституцій (ООН, ОБСЄ), криза системи колективної безпеки;
* Внутрішньополітичні кризи, зниження довіри до державних інститутів.

**Приклад:** вихід Великої Британії з ЄС (Brexit) створив політичну нестабільність у Європі, вплинув на перерозподіл сил у сфері європейської безпеки.

**E — Economic (економічні фактори)**

**Сутність:** стосується макроекономічної стабільності, енергетичної незалежності, фінансових ризиків, доступу до світових ринків і технологій.

**Загрози та виклики:**

* Зовнішня заборгованість і залежність від кредитів МВФ;
* Енергетична залежність від імпорту (газ, вугілля, нафта);
* Інфляція, девальвація національної валюти, тиск на соціальні видатки;
* Ризик втрати інвесторів через воєнні або політичні загрози.

**Приклад:** у 2022 р. після повномасштабного вторгнення РФ ВВП України знизився майже на 30%, що призвело до критичного зменшення доходів державного бюджету і підвищення зовнішньої фінансової залежності.

**S — Social (соціальні фактори)**

**Сутність:** охоплює демографічні тенденції, рівень соціальної напруги, нерівність, міжетнічні та міжконфесійні відносини, загальний рівень довіри до держави.

**Загрози та виклики:**

* Високий рівень безробіття, особливо серед молоді;
* Зростання кількості внутрішньо переміщених осіб (ВПО);
* Етнокультурні конфлікти, протестна активність;
* Зниження рівня соціальної згуртованості, відчуження громадян від держави.

**Приклад:** унаслідок війни в Україні понад 6 мільйонів осіб стали ВПО, що призвело до напруженості у сферах житлової політики, охорони здоров’я, освіти та соціального захисту.

**T — Technological (технологічні фактори)**

**Сутність:** стосується рівня розвитку ІТ-інфраструктури, інноваційної спроможності, кібербезпеки, контролю за технологіями подвійного призначення.

**Загрози та виклики:**

* Кіберзагрози: атаки на держсистеми, банки, енергетичну інфраструктуру;
* Вразливість до зовнішнього технологічного шантажу (обмеження доступу до обладнання, програмного забезпечення);
* Використання технологій для дестабілізації (deepfake, big data в інформаційній війні);
* Технічне відставання від розвинених країн.

**Приклад:** кібератака на урядові ресурси України у 2017 році (вірус Petya) вивела з ладу державні сервіси, банківські системи та транспортну інфраструктуру.

Висновок:

PEST-аналіз є ефективним інструментом стратегічного аналізу в системі національної безпеки, оскільки дозволяє:

* виявляти зовнішні тренди, які можуть трансформуватись у загрози;
* оцінювати здатність держави до адаптації;
* забезпечувати інтегроване бачення викликів на перетині політики, економіки, суспільства і технологій.

Його регулярне застосування в процесі формування політик безпеки сприяє підвищенню стійкості держави до довгострокових кризових явищ.

 ***Оцінка ризиків* (risk assessment)**

Методика оцінки ризиків базується на **розрахунку ймовірності реалізації загрози (Probability)** та **оцінці масштабів її наслідків (Impact)**. Часто використовується матриця ризиків (Risk Matrix), яка поділяє загрози за категоріями:

* Високий ризик (висока ймовірність + високий вплив);
* Помірний ризик (середній рівень впливу або ймовірності);
* Низький ризик (малоймовірні або незначні за масштабами загрози).

Цей підхід дозволяє визначити пріоритети для стратегічного планування і розподілу ресурсів безпеки.

 ***Метод експертного оцінювання***

Використовується для глибокого аналізу **комплексних або слабо формалізованих загроз**, зокрема у сфері геополітики, гібридних конфліктів, стратегічного прогнозування. Передбачає:

* Залучення вузькопрофільних фахівців з безпеки, права, міжнародних відносин, технологій;
* Створення експертних груп або аналітичних центрів;
* Розробку сценаріїв розвитку подій (Scenario Planning);
* Узагальнення якісних оцінок у вигляді рейтингу загроз, рекомендацій тощо.

Метод підвищує гнучкість прийняття рішень, особливо у ситуаціях високої невизначеності.

 ***Моніторинг відкритих джерел* (OSINT — Open Source Intelligence)**

OSINT — це збирання, аналіз та інтерпретація інформації з відкритих, легально доступних джерел. Основні канали:

* **ЗМІ та офіційні сайти державних органів;**
* **Соціальні мережі (Twitter/X, Telegram, Facebook, YouTube);**
* **Аналітичні центри, дослідницькі звіти (наприклад, RAND, IISS, CSIS);**
* **Бази даних, супутникові знімки, веб-трекери (FlightRadar, MarineTraffic);**
* **Форуми, даркнет, інструменти OSINT-аналітики (Maltego, Shodan, DataMiner).**

Перевага OSINT — швидкість отримання інформації, можливість виявляти загрози у режимі реального часу. У поєднанні з аналітичною обробкою цей метод є невід’ємною складовою сучасної системи попередження загроз.

Комплексне застосування методик ідентифікації та оцінки загроз дозволяє державі:

* здійснювати стратегічний моніторинг динаміки загроз;
* формувати адекватну та адаптивну систему реагування;
* інтегрувати експертний, технологічний і аналітичний потенціал у сферу національної безпеки.

Сучасний підхід до оцінки загроз передбачає поєднання кількісних інструментів з якісним експертним аналізом, що забезпечує високий рівень обґрунтованості управлінських рішень.

**3. Розподіл загроз за рівнем впливу та ступенем небезпеки**

Ідентифіковані загрози класифікуються відповідно до таких критеріїв:

* **За рівнем впливу:**
	+ *Глобальні* (наприклад, пандемії, світові війни, глобальні фінансові кризи);
	+ *Регіональні* (конфлікти в межах певного геополітичного простору, міждержавна напруга);
	+ *Національні* (внутрішні кризи, локальні катастрофи, внутрішній тероризм).
* **За ступенем небезпеки:**
	+ *Критичні* (реалізація загрози призводить до системного колапсу);
	+ *Суттєві* (загроза порушує окремі сфери життєдіяльності, але є контрольованою);
	+ *Локальні* (впливають на обмежену територію або певну галузь).

Такий розподіл дозволяє встановити пріоритетність заходів безпеки та розподіл ресурсів.

Класифікація загроз за **рівнем впливу** та **ступенем небезпеки** є важливим інструментом у стратегічному плануванні національної безпеки. Такий підхід дозволяє не лише систематизувати загрози, але й визначити пріоритети для оперативного реагування, мобілізації ресурсів та координації міжвідомчих дій.

***Розподіл за рівнем впливу***

 ***Глобальні загрози***

Це загрози, що охоплюють більшість країн світу або мають транснаціональний характер, впливаючи на світовий порядок, економіку, екологію чи систему міжнародної безпеки.

**Приклади:**

* Пандемії (COVID-19);
* Глобальні фінансові кризи (2008, 2020);
* Загроза ядерного конфлікту;
* Глобальне потепління та зміна клімату;
* Світові війни або наддержавні конфлікти.

**Наслідки:** дестабілізація міжнародних організацій (ООН, ВООЗ), порушення глобальних ланцюгів постачання, масова міграція, порушення екологічного балансу.

 ***Регіональні загрози***

Це загрози, що виникають у межах певного географічного або політичного регіону та охоплюють кілька суміжних країн. Вони часто пов’язані з конфліктами, геополітичним суперництвом або інтеграційними процесами.

**Приклади:**

* Військове протистояння на Балканах;
* Збройні конфлікти в Південному Кавказі;
* Напруженість у Східній Європі (включно з агресією РФ проти України);
* Конфлікти навколо ресурсів (вода, енергоносії).

**Наслідки:** зростання регіональної нестабільності, загроза енергетичній безпеці, гуманітарні кризи, посилення потоку біженців.

 ***Національні загрози***

Ці загрози стосуються виключно внутрішньої безпеки країни та реалізуються на її території. Вони можуть бути як природного, так і антропогенного походження.

**Приклади:**

* Політична криза, державний переворот;
* Внутрішній тероризм або сепаратизм;
* Протестна активність, соціальні заворушення;
* Надзвичайні ситуації (техногенні аварії, природні катастрофи).

**Наслідки:** підрив легітимності влади, параліч функцій управління, дестабілізація суспільства, зростання недовіри до інституцій.

 **Розподіл за ступенем небезпеки**

 ***Критичні загрози***

Це загрози, реалізація яких може призвести до системного колапсу: зруйнування державності, втрати суверенітету, непоправної шкоди для населення, економіки чи довкілля.

**Приклади:**

* Зовнішнє військове вторгнення;
* Застосування зброї масового ураження;
* Велика техногенна катастрофа (типу Чорнобиля);
* Кібератаки на об’єкти критичної інфраструктури.

**Особливість:** потребують негайного реагування на найвищому рівні, задіяння всіх національних ресурсів, часто — введення надзвичайного або воєнного стану.

 ***Суттєві загрози***

Такі загрози мають значний, але локалізований або контрольований вплив на одну чи кілька сфер життєдіяльності держави.

**Приклади:**

* Зростання рівня злочинності в окремих регіонах;
* Фінансова дестабілізація або інфляційна криза;
* Тимчасове порушення енергопостачання;
* Міграційна напруга.

**Особливість:** можуть бути ефективно подолані через координацію органів влади, за умови наявності адекватних механізмів управління.

 ***Локальні загрози***

Ці загрози мають обмежений вплив — географічний або функціональний — і не становлять системної небезпеки для держави в цілому.

**Приклади:**

* Повінь у межах однієї громади;
* Локальна аварія на підприємстві;
* Конфлікт на рівні місцевого самоврядування;
* Хакерська атака на окрему ІТ-систему.

**Особливість:** здебільшого розв’язуються силами місцевої влади або обмежених ресурсів, але можуть ескалувати за несприятливих умов.

**Практичне значення класифікації**

 **Управлінські переваги:**

* Дає змогу **ранжувати загрози** та встановлювати пріоритети.
* Сприяє **оптимальному розподілу ресурсів** (людських, фінансових, організаційних).
* Полегшує **розробку сценарного планування** на випадок ескалації ситуації.
* Забезпечує основу для **розробки нормативно-правових документів** у сфері безпеки.

Класифікація загроз за рівнем впливу та ступенем небезпеки є ключовим інструментом стратегічного аналізу в системі національної безпеки. Вона дозволяє приймати зважені управлінські рішення, адаптувати політику безпеки до контексту та підвищити готовність держави до реагування на кризові ситуації.

**4. Вплив технологічних змін на формування нових загроз**

Технологічний прогрес — двосічне явище: з одного боку, сприяє розвитку держави, з іншого — створює нові вектори загроз.

**Сучасні виклики:**

* **Кіберзагрози:** атаки на державні системи, об’єкти інфраструктури, банківський сектор.
* **Штучний інтелект:** можливість використання в інформаційній війні, автономні системи озброєнь.
* **Біотехнології:** загроза біотероризму, модифіковані віруси.
* **Дрони та автономні системи:** використання в терористичних цілях, порушення приватності.
* **Цифрова залежність:** уразливість до порушень роботи зв’язку, інтернет-інфраструктури.

Усе це вимагає постійного оновлення системи національної безпеки відповідно до темпів технологічних змін.

Технологічний прогрес є рушієм розвитку економіки, безпеки, медицини та управління, але водночас відкриває нові простори для ризиків і небезпек. В умовах динамічного розвитку цифрових, біо- та військових технологій класичні уявлення про загрози національній безпеці суттєво трансформуються. Технології стали не лише об’єктом, а й інструментом потенційної деструкції державності, економіки й суспільства.

 ***Кіберзагрози***

**Сутність:** атаки на інформаційні системи, бази даних, критичну інфраструктуру, електронні реєстри, комунікаційні мережі.

**Типові форми:**

* DDoS-атаки (перевантаження систем);
* Фішинг, шкідливе ПЗ, віруси (як-от Petya, NotPetya, WannaCry);
* Злам державних порталів, знищення архівів;
* Виведення з ладу систем управління енергетикою чи транспортом.

**Приклад:** атака на Державну казначейську службу України у 2023 році заблокувала фінансові розрахунки бюджетних установ, що паралізувало соціальні виплати.

 ***Штучний інтелект (AI)***

**Сутність:** AI здатен аналізувати великі обсяги даних, імітувати людську поведінку, автономно приймати рішення. Це відкриває як можливості, так і загрози.

**Загрози:**

* **Deepfake** — створення фальшивих відео із залученням політиків чи військових з метою дестабілізації;
* **AI в інформаційній війні** — автоматизоване поширення дезінформації;
* **Автономні озброєння** — безконтрольне застосування сили без участі людини;
* **AI у хакерських атаках** — системи, які самостійно адаптуються для подолання кіберзахисту.

**Приклад:** у 2022–2023 роках РФ активно використовувала штучний інтелект для імітації відеозвернень українських лідерів із закликами до капітуляції.

 ***Біотехнології***

**Сутність:** використання біологічних знань і технологій для створення або модифікації організмів з потенційно небезпечними властивостями.

**Загрози:**

* Створення штучних вірусів з високим рівнем патогенності;
* Утечі з лабораторій або навмисне застосування біологічної зброї;
* Порушення етичних і правових норм у генній інженерії.

**Приклад:** поява COVID-19 загострила дискусії щодо безпеки біолабораторій та необхідності міжнародного контролю за біотехнологіями.

 ***Дрони та автономні системи***

**Сутність:** безпілотні літальні апарати (БПЛА), наземні або морські дрони, які можуть виконувати як розвідувальні, так і бойові функції.

**Загрози:**

* Використання у терористичних атаках (мінування, підрив інфраструктури);
* Порушення приватності (спостереження за громадянами, політичними діячами);
* Складність ідентифікації джерела атаки;
* Використання у протиправній діяльності (контрабанда, шпигунство).

**Приклад:** атаки дронів на енергетичні об’єкти Києва і Одеси у 2023 році демонструють ефективність автономної зброї навіть у руках недержавних акторів.

 ***Цифрова залежність***

**Сутність:** технологічна інтеграція суспільства створює умови, в яких критичні функції держави, бізнесу та громадянської інфраструктури залежать від стабільності цифрових мереж.

**Загрози:**

* Вразливість до збою зв’язку (мобільного, супутникового, інтернету);
* Порушення роботи систем електронного урядування;
* Маніпуляції з цифровими реєстрами (кадастр, пенсії, субсидії);
* Поширення цифрової диктатури в авторитарних державах через моніторинг і контроль.

**Приклад:** під час активних бойових дій у Херсонській області у 2022 році припинення зв’язку унеможливило координацію евакуації цивільних.

Технологічні зміни створюють **нову архітектуру ризиків**, яка потребує:

* Постійного оновлення законодавства у сфері цифрової, кібер- та біологічної безпеки;
* Розвитку національних інституцій моніторингу та реагування;
* Формування цифрової грамотності населення;
* Міжнародного співробітництва у сфері контролю за новими технологіями.

Таким чином, **адаптація системи національної безпеки до темпів технологічного розвитку** є критичним завданням сучасної держави. Україна, як держава, що одночасно веде війну й інтегрується в західний безпековий простір, повинна стати прикладом проактивної та інноваційної безпекової політики.

**5. Огляд найбільш актуальних загроз для національної безпеки**

Станом на 2020-ті роки серед найбільш актуальних загроз для України та світу:

* **Кіберзагрози:** атаки на державні реєстри, критичну інфраструктуру, банківську систему (приклад — атака вірусу Petya у 2017 році).
* **Тероризм:** зокрема — гібридні форми, поєднані з інформаційними атаками.
* **Економічні кризи:** викликані пандеміями, війнами, енергетичною нестабільністю.
* **Військова агресія:** прикладом є вторгнення РФ в Україну.
* **Масова дезінформація:** підрив довіри до держави, розпалювання паніки, вплив на виборчі процеси.
* **Кліматичні загрози:** лісові пожежі, посухи, підтоплення — особливо актуальні у контексті глобального потепління.

У контексті 2020-х років загрози національній безпеці значно ускладнилися через інтеграцію традиційних і нетрадиційних чинників, що діють у гібридній, асиметричній та багатоаспектній формі. Україна, як держава, що протистоїть збройній агресії Російської Федерації, водночас перебуває під впливом глобальних загроз — від кіберзлочинності до змін клімату. Нижче подано детальний огляд найбільш актуальних загроз.

**Кіберзагрози** є однією з найдинамічніших і технологічно складних форм небезпеки. Атаки спрямовані проти державних реєстрів, систем енергопостачання, банківської інфраструктури та об’єктів критичної інфраструктури. Атака вірусу NotPetya у 2017 році стала показовою: злам інформаційних систем вивів з ладу урядові сервіси, логістичні платформи, приватні підприємства. Такі інциденти ілюструють потенціал кіберпростору як театру бойових дій. Окрім технічного вектору, кіберзагрози інтегруються в інформаційні операції, підтримуючи кампанії дезінформації.

**Тероризм**, особливо у своїх гібридних проявах, залишається постійною загрозою, яка підриває стабільність демократичних інституцій. У сучасних умовах це не лише вибухи чи захоплення заручників, а й цілеспрямовані деструктивні акти на об’єкти інфраструктури, енергетики, зв’язку, а також інспіровані ззовні соціальні протести. Особливе місце займає кібертероризм, а також спроби залучення вразливих верств населення до радикальних угруповань через інтернет.

**Економічні кризи** створюють як прямі, так і опосередковані загрози національній безпеці. Війна в Україні, пандемія COVID-19, енергетичні шоки через геополітичну нестабільність спричиняють макроекономічні дисбаланси, скорочення ВВП, дефіцит бюджету, інфляцію та падіння інвестиційної привабливості. Економічна дестабілізація також провокує соціальну напругу, посилення протестних настроїв і зниження довіри до державної політики.

**Військова агресія**, в умовах вторгнення Російської Федерації, є центральним фактором дестабілізації не лише України, а й європейського безпекового порядку. Війна охоплює широкий спектр — від конвенційного застосування сили до гібридних форм: інформаційних атак, економічного тиску, енергетичного шантажу, порушення норм міжнародного права. Агресія РФ призвела до руйнування інфраструктури, гуманітарних криз, екологічних катастроф і мільйонів внутрішньо переміщених осіб.

**Масова дезінформація** є надзвичайно небезпечною формою впливу, спрямованою на делегітимацію держави, послаблення суспільної єдності та створення паралельного інформаційного поля. Поширення фейкових новин, використання технологій deepfake, ботоферм і маніпуляцій у соціальних мережах сприяють втраті довіри до офіційних інституцій, викривленню сприйняття війни, посиленню паніки та фрустрації.

**Кліматичні загрози** також набувають безпекового виміру. Посухи, підтоплення, лісові пожежі, ерозія ґрунтів — усе це не лише загрожує екологічному балансу, а й безпосередньо впливає на енергетичну та продовольчу безпеку, стимулює внутрішню міграцію та зміну структури зайнятості. Особливу небезпеку становить вплив бойових дій на довкілля: забруднення ґрунтів, руйнування дамб, пожежі на нафтобазах та хімічних заводах.

Таким чином, сучасні загрози носять комплексний, мультидисциплінарний і міжгалузевий характер. Їх ефективне нейтралізування вимагає міжвідомчої координації, інтегрованих стратегій безпеки, інституційної стійкості й активної участі громадянського суспільства.

**6. Інструменти для моніторингу та раннього попередження загроз**

Для своєчасного виявлення загроз використовуються як національні, так і міжнародні системи:

* **Національні центри реагування на кіберінциденти (CERT-UA)**;
* **Інформаційні системи моніторингу надзвичайних ситуацій (ДСНС, МОЗ)**;
* **Супутниковий моніторинг та геоінформаційні системи (GIS)**;
* **OSINT-аналітика:** інструменти відкритого збору даних (Bellingcat, DataMiner);
* **Мережі раннього сповіщення (наприклад, система оповіщення НАТО, EU CBRN monitoring).**

Важливими також є міжвідомча співпраця, інформування громадян, регулярні симуляції (навчання) і міжнародні партнерства.

Сучасна система національної безпеки повинна бути не лише реактивною, а й проактивною. Це означає наявність **ефективних механізмів моніторингу, аналізу та прогнозування загроз** ще до їхньої реалізації. Для цього використовуються як державні, так і міжнародні технологічні та аналітичні інструменти, що поєднують людський фактор, штучний інтелект, супутникові дані, алгоритми великих даних і відкриту інформацію.

**Національні центри реагування на кіберінциденти (CERT-UA)**

**CERT-UA (Computer Emergency Response Team of Ukraine)** — основна державна структура, яка забезпечує моніторинг кіберпростору, фіксацію інцидентів, оперативне реагування на атаки та надання рекомендацій для органів влади та критичної інфраструктури.

**Функції:**

* Виявлення кіберзагроз у режимі 24/7;
* Поширення попереджень і рекомендацій (alerts, bulletins);
* Технічний аудит державних ІТ-систем;
* Співпраця з партнерами — наприклад, ENISA, US-CERT, кіберпідрозділами НАТО.

**Приклад:** у лютому 2022 року CERT-UA і Держспецзв’язку оперативно виявили та знешкодили новий варіант вірусу-вайпера HermeticWiper, яким РФ атакувала державні ІТ-ресурси України.

**Інформаційні системи моніторингу надзвичайних ситуацій (ДСНС, МОЗ)**

**ДСНС України** має систему оперативного спостереження та раннього оповіщення про природні й техногенні загрози (наприклад, повені, пожежі, хімічні викиди).

**МОЗ України** — координатор у сфері епідеміологічного моніторингу (наприклад, через Центр громадського здоров’я).

**Функції:**

* Збір та візуалізація даних із регіонів;
* Використання автоматизованих систем (АС «Оповіщення-2000», Система “Розвідка пожеж”);
* Інтеграція з системами цивільного захисту, медичних установ, лабораторій.

**Приклад:** під час поширення COVID-19 МОЗ здійснював моніторинг захворюваності через інтегровану систему “Епіднагляд”, зокрема для прогнозування нових спалахів.

**Супутниковий моніторинг та геоінформаційні системи (GIS)**

Супутникові технології та геоінформаційні системи дозволяють виявляти ознаки надзвичайних подій, військових пересувань, змін у ландшафті та забруднення навколишнього середовища.

**Функції:**

* Виявлення військової активності (рух техніки, створення укріплень);
* Моніторинг природних катастроф (затоплення, пожежі, посухи);
* Картографування загроз у реальному часі.

**Інструменти:** Google Earth, Sentinel Hub (EU), Planet Labs, Copernicus EMS (ЄС), ArcGIS (Esri).

**Приклад:** після підриву Каховської ГЕС у червні 2023 року супутникові знімки (NASA, Planet) дозволили оперативно оцінити масштаби затоплення, що стало основою для гуманітарного реагування.

**OSINT-аналітика (відкриті джерела даних)**

**OSINT (Open Source Intelligence)** — це метод збирання і обробки інформації з відкритих джерел, який відіграє ключову роль у моніторингу загроз, особливо в інформаційній сфері.

**Інструменти:**

* **Bellingcat** — використання супутникових фото, соціальних мереж та відкритих реєстрів для викриття дезінформації, ідентифікації військових підрозділів;
* **DataMiner, Maltego** — інструменти для візуалізації зв’язків, аналізу соціальних мереж;
* **Shodan, Censys** — пошук уразливостей в інтернет-пристроях;
* **Telegram-OSINT** — моніторинг бойових дій, обстрілів, настроїв.

**Приклад:** волонтерські ініціативи в Україні (як-от DeepState, InformNapalm) здійснюють картографування бойових дій, виявлення фейків та поширення правдивої інформації.

**Міжнародні системи раннього попередження**

**NATO Alert System** — платформа для обміну інформацією між країнами-членами та партнерами щодо загроз безпеці, включаючи кіберінциденти, переміщення зброї, теракти.

**EU CBRN Monitoring** — система ЄС для моніторингу хімічних, біологічних, радіологічних і ядерних загроз. Україна має доступ до консультацій і технічної допомоги через інструменти цивільного захисту ЄС.

**Приклад:** під час війни в Україні Європейський центр реагування ERCC координував доставку обладнання (CBRN-захист, медичні комплекти) для лікарень і служб цивільного захисту.

**Додаткові елементи ефективного реагування**

* **Міжвідомча співпраця:** координація між СБУ, Міноборони, МВС, ДСНС, МОЗ, Держспецзв’язком, а також місцевими органами влади.
* **Сценарні навчання та симуляції:** регулярні тренування (у т. ч. з міжнародними партнерами — США, Польщею, Литвою) дозволяють тестувати готовність до криз.
* **Громадське інформування:** запуск мобільних додатків («Повітряна тривога», «Дія»), SMS-оповіщення, телемарафони.
* **Міжнародні партнерства:** проєкти НАТО Trust Fund, USAID Cybersecurity for Critical Infrastructure, Європейський механізм цивільного захисту.

Система моніторингу та раннього попередження є невід’ємною частиною національної безпеки. Вона базується на інтеграції технічних платформ, відкритих даних, інституційної координації та участі громадянського суспільства. Україна має всі передумови для розбудови потужної системи превентивного реагування, яка здатна нейтралізувати загрози ще на етапі їх зародження.

**Тема 3. Система національного кризового менеджменту та її структура (**ЗК 1. . ЗК 6. ЗК 7. . ЗК 10. СК 1. СК 4. СК 5. СК 7. СК 13. СК 16. ПРН 3. ПРН 4. ПРН 6. ПРН 8. ПРН 9. ПРН 10. ПРН 13. ПРН 14. )

1. Основні елементи національної системи кризового управління.
2. Повноваження та відповідальність державних структур під час криз.
3. Роль Міністерства оборони, Міністерства внутрішніх справ та інших відомств.
4. Законодавча база, що регулює кризове управління на національному рівні.
5. Протоколи взаємодії між урядовими структурами у кризових ситуаціях.
6. Огляд нормативно-правових актів, що регулюють кризовий менеджмент.

**1. Основні елементи національної системи кризового управління**

Система кризового менеджменту в Україні — це сукупність державних органів, законодавчих норм, механізмів реагування та інституційної взаємодії, спрямованих на запобігання, локалізацію, мінімізацію наслідків і ліквідацію кризових ситуацій. Її структура охоплює такі ключові компоненти:

* **Органи управління кризами** (РНБО, КМУ, ОВА, місцеві ради);
* **Спеціалізовані служби** (ДСНС, СБУ, МОЗ, Міноборони, НГУ, Нацполіція);
* **Оперативні та аналітичні центри** (ситуаційні центри при Президентові, в міністерствах та ОВА);
* **Система зв’язку та оповіщення населення**;
* **Механізми моніторингу та прогнозування** (включно з ГІС, супутниковим моніторингом, системами раннього попередження).Конец формы

Система кризового менеджменту України базується на інтеграції органів виконавчої влади, спеціалізованих служб, інформаційно-аналітичних центрів, нормативного регулювання та технологічних платформ. Її завдання — своєчасне **виявлення загроз**, **мобілізація ресурсів**, **координація дій**, **забезпечення безпеки населення** та **ліквідація наслідків кризових ситуацій**. Ефективність системи залежить від чіткого розподілу функцій, готовності інституцій і їх здатності діяти в уніфікованому режимі.

 **Органи управління кризами**

* **Рада національної безпеки і оборони (РНБО)** — стратегічний центр формування політики безпеки. Приймає рішення в умовах надзвичайного або воєнного стану, координує міжвідомчі дії.
* **Кабінет Міністрів України (КМУ)** — виконавчий орган, що забезпечує реалізацію державної політики у сфері цивільного захисту, організовує управління у кризових ситуаціях через міністерства.
* **Обласні та районні військові адміністрації (ОВА/РВА)** — відповідають за реалізацію кризових заходів на регіональному рівні, взаємодію з ДСНС, ЗСУ, поліцією та органами місцевого самоврядування.
* **Місцеві ради** — організують заходи безпеки на територіях громад, забезпечують евакуацію, життєзабезпечення та інформування населення.

 **Спеціалізовані служби**

* **Державна служба з надзвичайних ситуацій (ДСНС)** — основний виконавець реагування на природні, техногенні та соціальні катастрофи. Відповідає за рятувальні операції, ліквідацію пожеж, евакуацію, пошук людей.
* **Служба безпеки України (СБУ)** — забезпечує захист державного суверенітету, контррозвідку, протидію диверсіям і тероризму, контроль за критичною інфраструктурою.
* **Міністерство охорони здоров’я (МОЗ)** — координує медичне забезпечення в кризових умовах, зокрема у випадках епідемій або біозагроз.
* **Міністерство оборони, Збройні сили України (ЗСУ)** — виконують завдання у разі воєнної загрози, оборони об'єктів, логістики та гуманітарного супроводу.
* **Національна гвардія, Національна поліція** — підтримують правопорядок, беруть участь в евакуації, блокуванні небезпечних зон, патрулюванні.

 **Оперативні та аналітичні центри**

* **Ситуаційний центр при Президентові України** — координаційно-аналітична структура, яка забезпечує моніторинг загроз, оперативне реагування та інформаційне забезпечення РНБО.
* **Центри реагування в міністерствах і ОВА** — працюють у режимі 24/7, збирають оперативну інформацію, координують реагування на місцях, готують щоденні зведення та рекомендації.
* **Національний координаційний центр кібербезпеки (НКЦК)** — аналітична платформа, що відповідає за кіберзахист держави.

 **Система зв’язку та оповіщення населення**

* **Єдина система централізованого оповіщення** — дозволяє повідомляти населення про загрози через мобільні мережі, радіо, телебачення та мобільні додатки (наприклад, «Повітряна тривога»).
* **Системи екстреного зв’язку** — використовуються для координації між підрозділами ДСНС, МОЗ, поліцією та військовими структурами.
* **Засоби резервного зв’язку** — супутникові телефони, автономні ретранслятори, системи шифрованої передачі даних (в умовах втрати основних каналів зв’язку).

**Механізми моніторингу та прогнозування**

* **Геоінформаційні системи (ГІС)** — інтегрують просторові дані про ризики, аварії, зони ураження, маршрути евакуації.
* **Супутниковий моніторинг** — використовується для виявлення змін у ландшафті (пожежі, затоплення), фіксації переміщення військ, моніторингу прикордонних територій.
* **Системи раннього попередження** — вбудовані в роботу ДСНС, Держпродспоживслужби (у випадку епідемій), Держекоінспекції (моніторинг забруднень).
* **Цифрові платформи збору даних** — автоматизовані бази (типу SafeUkraine, eHealth, Geoportal), які інтегрують інформацію з різних джерел у єдину систему управління.

Система кризового управління в Україні є складною, багаторівневою і міжвідомчою. Вона поєднує централізоване стратегічне керівництво з гнучкими механізмами локального реагування. Умовою її ефективності є не лише наявність структур, а й чітка координація між ними, актуалізація нормативної бази та постійна адаптація до нових типів загроз.

**2. Повноваження та відповідальність державних структур під час криз**

Кожен орган влади має визначену компетенцію в межах єдиної системи цивільного захисту:

* **Президент України** – загальне керівництво та оголошення надзвичайного/воєнного стану;
* **Кабінет Міністрів України** – організація заходів на загальнодержавному рівні, управління ресурсами, координація міністерств;
* **РНБО** – розробка стратегічних рішень, мобілізація сил, антикризова координація;
* **Місцеві адміністрації** – реалізація заходів у регіонах, мобілізація місцевих ресурсів, забезпечення комунікації;
* **ДСНС** – реагування на НС, ліквідація наслідків, евакуація, пожежогасіння;
* **МОЗ** – медичне забезпечення, епіднагляд;
* **МЗС** – міжнародна допомога, дипломатична комунікація;
* **СБУ** – контррозвідка, запобігання диверсіям та терористичним актам.

Система кризового менеджменту в Україні функціонує на основі принципу чіткого розмежування повноважень між органами влади. Кожна інституція виконує визначені завдання в рамках **Єдиної державної системи цивільного захисту**, яка охоплює усі рівні — від національного до місцевого — і забезпечує скоординовану відповідь на надзвичайні ситуації (НС) як мирного, так і воєнного часу. Нижче подано деталізацію ключових суб’єктів та їх функціоналу.

**Президент України**

* Є **верховним головнокомандувачем** та гарантом національної безпеки;
* У разі загрози суверенітету, територіальної цілісності або масової НС **оголошує надзвичайний або воєнний стан** (за погодженням з Верховною Радою);
* Скликає засідання РНБО, затверджує її рішення указами;
* Координує діяльність силових структур та надає політичний мандат для проведення спеціальних заходів (мобілізація, евакуація, стратегічні плани реагування).

**Приклад:** указ Президента від 24.02.2022 про введення воєнного стану на всій території України після початку повномасштабного вторгнення РФ.

**Кабінет Міністрів України (КМУ)**

* Відповідальний за **організацію дій національного масштабу** — забезпечення цивільного захисту, раціонального розподілу ресурсів, управління запасами;
* Призначає **державні координатори кризових заходів** у міністерствах і відомствах;
* Забезпечує **фінансування заходів**, зокрема через резервний фонд держбюджету;
* Розробляє **національні плани реагування**, затверджує нормативні акти, регулює діяльність ОВА в умовах НС.

**Приклад:** постанова КМУ №11 від 09.01.2014 «Про єдину державну систему цивільного захисту».

**Рада національної безпеки і оборони (РНБО)**

* Виконує функції **стратегічного антикризового штабу**;
* Координує діяльність силових, оборонних і безпекових відомств;
* Визначає **пріоритети дій** у разі загрози національній безпеці;
* Розробляє аналітичні сценарії, оцінки загроз, політико-правові рішення (санкції, заборони, надзвичайні повноваження).

**Приклад:** рішення РНБО від 20.07.2022 «Про невідкладні заходи з протидії кіберзагрозам».

**Місцеві адміністрації (ОВА, РВА, органи місцевого самоврядування)**

* Забезпечують **реалізацію заходів кризового реагування на місцях**;
* Організовують **евакуацію населення, розміщення переселенців, роботу гуманітарних штабів**;
* Забезпечують **інформування населення**, підтримку роботи критичних служб (медицина, водопостачання, енергетика);
* Взаємодіють із волонтерами, громадськими організаціями, бізнесом;
* Розгортають **оперативні штаби** на рівні громади.

**Приклад:** діяльність Київської ОВА під час ракетних атак у 2022–2023 рр., координація укриттів, енергопостачання, розгортання «пунктів незламності».

**Державна служба з надзвичайних ситуацій (ДСНС)**

* Провідний виконавець дій у сфері **цивільного захисту**;
* Відповідає за **ліквідацію наслідків НС**, рятувальні операції, розмінування, пожежогасіння, аварійно-рятувальні роботи;
* Здійснює **оперативний моніторинг ситуації**, управління ресурсами, створення мобільних підрозділів;
* Забезпечує **функціонування системи оповіщення**, координацію з місцевими штабами.

**Приклад:** участь ДСНС у ліквідації наслідків підриву Каховської ГЕС — евакуація населення, водопостачання, мінімізація екологічної шкоди.

**Міністерство охорони здоров’я (МОЗ)**

* Координує **надання медичної допомоги** в умовах кризи (війна, пандемія, біологічні загрози);
* Забезпечує **епіднагляд, санітарно-гігієнічний контроль, медичну евакуацію, мобілізацію медперсоналу**;
* Співпрацює з Червоним Хрестом, ВООЗ, іноземними партнерами щодо гуманітарної та медичної допомоги;
* Здійснює **психологічну підтримку населення** у кризових ситуаціях.

**Приклад:** розгортання польових шпиталів та мобільних бригад під час бойових дій у прифронтових регіонах.

**Міністерство закордонних справ (МЗС)**

* Забезпечує **міжнародну дипломатичну комунікацію** в умовах кризи;
* Організовує **отримання іноземної гуманітарної та військової допомоги**;
* Координує **евакуацію громадян України за кордоном** у разі загрози;
* Представляє інтереси держави в міжнародних організаціях (ООН, ОБСЄ, ЄС, НАТО) для залучення підтримки.

**Приклад:** масова евакуація українців із Афганістану у 2021 році та координація дипломатичних каналів під час війни 2022–2024 рр.

**Служба безпеки України (СБУ)**

* Веде **контррозвідувальну діяльність**;
* Виявляє, запобігає та нейтралізує **диверсії, шпигунство, теракти**;
* Контролює безпеку на **критичних об’єктах інфраструктури**;
* Бере участь у **захисті інформаційного простору та кібербезпеки**;
* Має повноваження до запровадження **режиму контртерористичної операції**.

**Приклад:** виявлення агентурної мережі РФ у прифронтових областях, що передавала дані про дислокацію ЗСУ.

Розподіл повноважень і відповідальності між державними структурами дозволяє формувати **модульну, функціонально гнучку систему кризового реагування**, де кожен суб’єкт виконує спеціалізовану роль. Основою її ефективності є оперативна координація, правова визначеність дій, ресурсне забезпечення та інтеграція з міжнародними партнерами.

**3. Роль Міністерства оборони, МВС та інших відомств**

* **Міністерство оборони України** здійснює стратегічне та оперативне керівництво у разі воєнних загроз. Координує ЗСУ, бере участь у захисті критичної інфраструктури, забезпечує мобілізацію та територіальну оборону.
* **МВС України** – координує Нацполіцію, Нацгвардію, ДСНС. Забезпечує охорону громадського порядку, евакуацію, логістику, охорону стратегічних об'єктів.
* **Мінінфраструктури** – організовує транспортну евакуацію, підтримку логістики.
* **Мінцифра** – координує захист інформаційних систем, кібербезпеку.
* **Державна прикордонна служба** – контроль за переміщенням населення, прикордонна безпека.

У межах національної системи кризового управління центральні органи виконавчої влади відіграють ключову роль у реалізації оперативних, безпекових, логістичних, комунікаційних та гуманітарних функцій. Їхня діяльність регламентована законодавством України та координується через Кабінет Міністрів, РНБО та ситуаційні штаби.

**Міністерство оборони України (МОУ)**

Має провідну роль у реагуванні на воєнні загрози та кризові ситуації, пов’язані з обороною держави. Основні завдання:

* **Стратегічне управління Збройними силами України (ЗСУ)** — розгортання підрозділів, планування операцій, територіальна оборона;
* **Захист критичної інфраструктури** — об’єктів енергетики, зв’язку, транспорту, військових баз, складів боєприпасів;
* **Забезпечення мобілізаційної готовності** — формування резерву, логістичне забезпечення мобілізованих частин, медико-санітарне забезпечення;
* **Участь у спільних штабах** — інтеграція військових ресурсів у цивільне управління під час воєнного стану;
* **Координація з міжнародними безпековими партнерами (НАТО, США, ЄС)** — щодо постачання озброєння, розвідки, обміну інформацією.

**Приклад:** під час повномасштабного вторгнення РФ (2022) МОУ оперативно забезпечило мобілізацію, формування батальйонів тероборони, оборону об’єктів критичної інфраструктури.

**Міністерство внутрішніх справ України (МВС)**

МВС є ключовим органом у забезпеченні громадської безпеки, правопорядку, рятувальних операцій, а також контролю за надзвичайними ситуаціями невоєнного характеру. Координує:

* **Національну поліцію України (НПУ)** — охорона правопорядку, боротьба зі злочинністю, контроль за переміщенням населення, забезпечення безпеки на вулицях, інфраструктурі, транспорті;
* **Національну гвардію України (НГУ)** — охорона об’єктів державного значення, участь у бойових операціях, забезпечення правопорядку в умовах надзвичайного або воєнного стану;
* **Державну службу з надзвичайних ситуацій (ДСНС)** — гасіння пожеж, евакуація, розмінування, гуманітарна допомога, ліквідація наслідків природних та техногенних катастроф;
* **Координацію дій місцевих підрозділів МВС** — розгортання штабів, забезпечення логістики та транспорту.

**Приклад:** МВС забезпечило евакуацію населення з прифронтових регіонів Донецької і Харківської областей у 2022–2023 рр. через залучення поліції, ДСНС, Нацгвардії.

**Міністерство інфраструктури України (Мінінфраструктури)**

Виконує технічну та логістичну функцію в умовах кризи:

* **Організація евакуації населення** — залізничним, автомобільним, авіаційним і водним транспортом;
* **Забезпечення працездатності транспортної інфраструктури** — ремонт доріг, мостів, забезпечення паливом;
* **Підтримка гуманітарної логістики** — координація доставки допомоги, забезпечення пунктів збору;
* **Взаємодія з міжнародними логістичними мережами** — координація з Укрзалізницею, Укрпоштою, портами.

**Приклад:** у березні 2022 року Мінінфраструктури забезпечило «зелені коридори» для евакуації з Київської області та постачання гуманітарної допомоги до Чернігова.

**Міністерство цифрової трансформації України (Мінцифра)**

В умовах гібридної війни виконує критично важливу роль у кіберзахисті, безпеці даних та цифровій стійкості держави:

* **Забезпечення кібербезпеки державних ресурсів** — захист реєстрів, вебпорталів, критичних інформаційних систем;
* **Координація кіберопору** — робота з хактивістами, міжнародними партнерами (наприклад, IT Army of Ukraine);
* **Інформаційна гігієна** — боротьба з дезінформацією, фейками;
* **Підтримка комунікацій** — безперебійна робота мобільного зв’язку, інтернету (включаючи інтеграцію системи Starlink);
* **Розробка цифрових сервісів для громадян** — оповіщення, надання послуг, ID-платформи.

**Приклад:** запуск мобільного застосунку «Повітряна тривога», інтеграція повідомлень у «Дію», розгортання мережі Starlink у зонах, де зруйновано телеком-інфраструктуру.

**Державна прикордонна служба України (ДПСУ)**

Цей орган забезпечує **контроль за державним кордоном** і регулює **міграційні потоки** в умовах воєнного стану, гуманітарних криз, загроз тероризму.

* **Контроль переміщення осіб та вантажів** — як для захисту від терористичних загроз, так і для протидії контрабанді;
* **Організація евакуації громадян за кордон**;
* **Забезпечення режиму прикордонних територій** — посилення патрулювання, блокпости;
* **Взаємодія з МЗС та Міжнародною організацією з міграції** щодо допомоги біженцям.

**Приклад:** у лютому–березні 2022 року ДПСУ забезпечила евакуацію понад 3 млн українців через західні пункти пропуску, одночасно з перевіркою осіб на предмет співпраці з ворогом.

Функціонування зазначених відомств у системі кризового менеджменту є не лише операційним компонентом, а й ключовим чинником національної стійкості. Їхня ефективна взаємодія забезпечує **цілісність реагування**, оперативну адаптацію до багатовекторних загроз та реалізацію державної політики безпеки у надзвичайних умовах.

Начало формы

**4. Законодавча база, що регулює кризове управління на національному рівні**

Правове регулювання здійснюється на підставі:

* **Конституції України** – закріплює функції Президента, РНБО та КМУ у надзвичайних обставинах.
* **Закону України «Про правовий режим надзвичайного стану» (2000, № 1550-III)**;
* **Закону України «Про правовий режим воєнного стану» (2015, № 389-VIII)**;
* **Закону України «Про національну безпеку» (2018, № 2469-VIII)**;
* **Кодексу цивільного захисту України** (2012, № 5403-VI) – базовий документ щодо організації реагування на НС природного, техногенного чи соціального характеру.

Конец формы

Законодавче забезпечення кризового управління в Україні формує **інституційно-правову основу** для дій держави в умовах загроз життєво важливим інтересам суспільства, держави та громадян. Воно охоплює **нормативне регулювання процедур запобігання, реагування, відновлення і координації** у кризових ситуаціях мирного та воєнного часу.

**Конституція України**

* Встановлює **розподіл повноважень** між Президентом, Кабінетом Міністрів, Верховною Радою та органами місцевого самоврядування;
* **Стаття 92** визначає, що виключно законами встановлюється правовий режим воєнного і надзвичайного стану;
* **Стаття 106** закріплює право Президента вводити надзвичайний або воєнний стан, координувати РНБО;
* Конституційні норми є **базовими для всіх дій** у сфері національної безпеки, а також гарантують права і свободи громадян навіть у надзвичайних обставинах (з можливістю часткового обмеження за рішенням парламенту).

**Закон України «Про правовий режим надзвичайного стану» (2000, № 1550-III)**

* Визначає **умови запровадження та дії режиму НС** в разі стихійних лих, техногенних аварій, терористичних загроз або суспільної дестабілізації;
* Регламентує повноваження Президента, КМУ, місцевих органів влади;
* Встановлює перелік **обмежень прав і свобод громадян**, які можуть бути введені в умовах НС (наприклад, комендантська година, обмеження руху, заборона масових зібрань);
* Передбачає **створення оперативних штабів**, порядок інформування населення та механізми мобілізації.

**Закон України «Про правовий режим воєнного стану» (2015, № 389-VIII)**

* Регламентує механізми **запровадження та реалізації воєнного стану** у разі збройної агресії, загрози державному суверенітету;
* Визначає **структуру військового командування**, зокрема участь ЗСУ, Міноборони, ОВА;
* Встановлює **правові підстави для евакуації**, трудової мобілізації, вилучення майна для потреб армії;
* Уточнює межі **обмеження прав громадян**, порядок діяльності ЗМІ, блокування інформаційних ресурсів;
* Надає органам влади **надзвичайні повноваження** щодо управління стратегічними ресурсами.

**Закон України «Про національну безпеку» (2018, № 2469-VIII)**

* Визначає **систему національної безпеки України**, її цілі, завдання, принципи, суб’єктів;
* Встановлює **структуру сектору безпеки і оборони**, включаючи ЗСУ, СБУ, МВС, ДСНС, ДПСУ тощо;
* Описує повноваження Президента, РНБО, парламенту і КМУ у сфері безпеки;
* Регулює **стратегічне планування**: національні загрози, сценарії реагування, бюджетування безпекового сектору;
* Встановлює **засади цивільного контролю** над сектором безпеки, прозорість і підзвітність державних інституцій.

**Кодекс цивільного захисту України (2012, № 5403-VI)**

* Є **основним нормативно-правовим актом** у сфері реагування на надзвичайні ситуації невоєнного характеру;
* Регулює функціонування **єдиної державної системи цивільного захисту**;
* Визначає класифікацію надзвичайних ситуацій (природні, техногенні, соціальні), їх рівні та ступені ризику;
* Встановлює повноваження центральних і місцевих органів виконавчої влади, підприємств, установ і організацій;
* Регламентує **навчання, оповіщення, евакуацію, порядок використання матеріальних резервів**, надання допомоги населенню.

**Інші важливі нормативно-правові акти:**

* **Постанова КМУ № 11 від 09.01.2014** «Про єдину державну систему цивільного захисту» — деталізує структуру, склад і завдання системи;
* **Укази Президента України про запровадження НС чи воєнного стану** (зокрема Указ №64/2022 від 24.02.2022);
* **Національні плани реагування на надзвичайні ситуації** (затверджуються КМУ).

Законодавча база кризового менеджменту України має системний і багаторівневий характер. Вона визначає повноваження органів влади, права громадян, механізми мобілізації ресурсів і порядок дій у разі надзвичайних обставин. В умовах гібридних загроз та збройної агресії дієвим залишається постійне оновлення нормативної основи відповідно до нових викликів національній безпеці.

**5. Протоколи взаємодії між урядовими структурами у кризових ситуаціях**

Координація під час криз забезпечується за допомогою:

* **Єдиного державного плану реагування на надзвичайні ситуації**;
* **Ситуаційних центрів (національного, обласних, галузевих)**;
* **Штабів НС на місцях** (оперативно створюються при ОВА);
* **Механізму «єдиного вікна»** для швидкої міжвідомчої взаємодії;
* **Інформаційного обміну в реальному часі** (через Систему зв’язку цивільного захисту, Єдину державну платформу інформаційної взаємодії).

У кризових ситуаціях — будь то збройна агресія, техногенна катастрофа або природне лихо — оперативність, чіткість та скоординованість дій державних органів мають вирішальне значення. Саме тому в Україні сформовано **набір протоколів взаємодії**, що регламентують розподіл повноважень, послідовність дій, інформаційні канали та відповідальність кожної установи в межах **Єдиної державної системи цивільного захисту**.

 **Єдиний державний план реагування на надзвичайні ситуації**

* Це **базовий інструмент кризового планування**, який визначає порядок дій органів виконавчої влади та місцевого самоврядування у разі виникнення надзвичайної ситуації.
* Містить **типові сценарії реагування**, визначає відповідальних суб’єктів, ресурси, терміни та способи координації.
* План розробляється ДСНС за участі центральних органів виконавчої влади і затверджується Кабінетом Міністрів.
* Охоплює як **мирний, так і воєнний період**; включає класифікацію НС (природні, техногенні, соціальні) та механізми переходу з одного рівня загрози до іншого.

**Приклад:** План реагування передбачає дії при затопленнях, епідеміях, кібератаках, аваріях на підприємствах підвищеної небезпеки тощо.

**Ситуаційні центри (національний, обласні, галузеві)**

* В Україні функціонують **оперативно-аналітичні центри**, які збирають, обробляють та передають інформацію в реальному часі для ухвалення управлінських рішень.
* **Національний ситуаційний центр при Президентові України** здійснює стратегічну координацію (аналіз загроз, прийняття рішень РНБО).
* **Обласні ситуаційні центри** при ОВА — контролюють ситуацію в регіоні, координують дії між місцевими службами.
* **Галузеві центри** (при МОЗ, Мінінфраструктури, Міноборони) — відповідають за оперативний моніторинг у своїй сфері відповідальності.

**Функції:** візуалізація ситуації (включно з супутниковими даними), генерація аналітичних звітів, координація служб.

**Штаби НС на місцях**

* У разі надзвичайної ситуації на рівні області чи громади рішенням голови ОВА створюється **оперативний штаб реагування**, який очолює або сам голова ОВА, або його заступник.
* До складу входять представники ДСНС, поліції, медичних установ, військових частин, комунальних служб, волонтерських організацій.
* Штаби розробляють **місцеві плани дій**, організовують логістику, контроль руху населення, укриття, постачання гуманітарної допомоги.
* Штаби НС мають **постійний зв’язок із вищими інстанціями** через канали спеціального зв’язку та платформу інформаційної взаємодії.

**Приклад:** штаб ОВА під час обстрілів Харкова у 2022–2023 роках керував евакуацією, пошуком зниклих, доставкою води та генераторів.

 **Механізм «єдиного вікна» для міжвідомчої взаємодії**

* Це **цифровий і адміністративний протокол**, який дозволяє швидко залучати та координувати дії різних органів влади, не дублюючи функції.
* Забезпечує **уніфіковане подання запитів, повідомлень, звітів** між установами — через електронні платформи (зокрема, Система електронної взаємодії органів виконавчої влади – СЕВ ОВВ).
* Оптимізує процес отримання дозволів, погоджень, інформації — особливо актуально під час кризи, коли потрібно уникнути бюрократичних затримок.

**Приклад:** запит про розміщення евакуйованих може ініціюватися ОВА через єдину систему і буде автоматично спрямований до МОЗ, Мінсоцполітики, Укрзалізниці, Мінінфраструктури.

 **Інформаційний обмін у реальному часі**

* Забезпечується через **державну систему спеціального зв’язку, супутниковий зв’язок, канали радіозв’язку**, а також **захищені електронні платформи** (типу Єдиного вебпорталу органів виконавчої влади, Резервної платформи Мінцифри, «Дія.Центр»).
* Функціонує **Єдина державна платформа інформаційної взаємодії**, яка дозволяє обмінюватися аналітикою, зведеннями, протоколами рішень, сигналами тривоги.
* В умовах масових атак на ІТ-інфраструктуру частина даних дублюється через **резервні сервери** або зберігається на платформах партнерів (AWS, Azure, Starlink).

**Приклад:** через цю систему передаються сигнали повітряної тривоги, координати ударів, інформація про гуманітарні коридори, блокпости тощо.

Протоколи взаємодії в кризових умовах базуються на принципах **оперативності, взаємодоповнення, інформаційної синхронізації** та **чіткого розподілу відповідальності**. Вони дозволяють уникнути хаосу, дублювання рішень і втрати часу. У сучасних умовах цифрова трансформація системи управління дозволяє підвищити ефективність реагування та створити єдиний управлінський простір навіть у кризових обставинах.

**6. Огляд нормативно-правових актів, що регулюють кризовий менеджмент**

До ключових нормативно-правових документів, що формують систему кризового управління в Україні, належать:

* Постанова КМУ «Про єдину державну систему цивільного захисту» (2013, № 11);
* Указ Президента України «Про рішення РНБО щодо невідкладних заходів з протидії гібридним загрозам»;
* Національний план реагування на надзвичайні ситуації;
* Плани територіальної оборони;
* Галузеві інструкції та протоколи (ДСНС, МОЗ, СБУ, Міноборони);
* Інструкції з кризової комунікації та оповіщення.

Нормативно-правове забезпечення кризового менеджменту в Україні охоплює **постанови уряду, укази Президента, стратегічні плани, підзаконні акти, інструкції та галузеві протоколи**, що регламентують порядок запобігання, реагування, ліквідації та відновлення у разі надзвичайних ситуацій. У сукупності вони утворюють **функціональну правову рамку**, яка забезпечує ефективність Єдиної державної системи цивільного захисту (ЄДСЦЗ).

**Постанова Кабінету Міністрів України «Про єдину державну систему цивільного захисту» (від 9 січня 2014 р. № 11)**

* Це **основоположний підзаконний акт**, який визначає структуру, функції, рівні реагування, механізми управління та координації в межах ЄДСЦЗ.
* Розмежовує повноваження центральних органів виконавчої влади, місцевих органів влади, підприємств і громад.
* Визначає п’ять функціональних підсистем (моніторинг, оповіщення, реагування, евакуація, ліквідація наслідків) і чотири рівні надзвичайних ситуацій (державний, регіональний, місцевий, об'єктовий).
* Містить перелік **оперативних штабів, засобів управління, фінансових і матеріальних резервів**.

 **Указ Президента України «Про рішення РНБО щодо невідкладних заходів з протидії гібридним загрозам»**

* Регламентує **дії держави у відповідь на гібридні загрози**, зокрема в кіберпросторі, інформаційному полі, енергетичній безпеці.
* Передбачає **посилення спроможностей СБУ, Держспецзв’язку, Мінцифри** у сфері кіберзахисту та реагування на деструктивну інформаційну діяльність.
* Містить завдання з **удосконалення міжвідомчої координації**, розвитку національних центрів реагування, взаємодії з партнерами (НАТО, ЄС).

**Приклад:** Указ №685/2021 від 14.12.2021 щодо протидії загрозам інформаційній безпеці.

**Національний план реагування на надзвичайні ситуації**

* Це **стратегічний документ**, розроблений ДСНС і затверджений КМУ.
* Містить **типові сценарії загроз**, зокрема у випадку пандемій, терористичних актів, стихійних лих, аварій на об’єктах підвищеної небезпеки.
* Визначає порядок **прийняття рішень, розгортання сил, мобілізації ресурсів**, координації між ЦОВВ, ОВА, ЗСУ, поліцією.
* Містить додатки з **переліками відповідальних осіб, регіональних ресурсів, логістичних маршрутів, комунікаційних каналів**.

 **Плани територіальної оборони**

* Регулюються Законом України «Про основи національного спротиву» (2021) і підзаконними актами Міноборони.
* Визначають порядок **створення, підготовки та застосування підрозділів територіальної оборони** у разі загрози воєнного характеру або кризи.
* Передбачають:
	+ розгортання ТРО в областях і громадах;
	+ взаємодію з поліцією, ДСНС, органами влади;
	+ забезпечення логістики, зв’язку, інфраструктури укриття;
	+ мобілізаційні завдання, контроль за порядком.

**Приклад:** оперативне розгортання підрозділів ТРО у Київській, Харківській, Запорізькій областях у лютому–березні 2022 року.

 **Галузеві інструкції та протоколи (ДСНС, МОЗ, СБУ, Міноборони)**

* **ДСНС:** інструкції з ліквідації наслідків стихійних лих, техногенних аварій, протоколи дій при пожежах, затопленнях, обваленнях будівель.
* **МОЗ:** клінічні протоколи надання допомоги в умовах катастроф, алгоритми масової евакуації, інструкції з протидії біозагрозам та інфекційним спалахам.
* **СБУ:** протоколи дій при загрозі терористичного акту, блокуванні об'єктів, інформаційного ураження.
* **Міноборони:** регламенти застосування військових формувань у мирний час для допомоги в цивільних кризах (наприклад, при мінуваннях, обстрілах, евакуації з небезпечних зон).

 **Інструкції з кризової комунікації та оповіщення**

* Визначають **механізми інформування населення**, ЗМІ, міжнародних партнерів у режимі надзвичайної ситуації.
* Включають:
	+ чіткі алгоритми розповсюдження повідомлень (SMS, застосунки, теле- та радіоефіри);
	+ заборони на поширення фейкової або неперевіреної інформації;
	+ правила взаємодії пресслужб відомств (МВС, МОЗ, ДСНС, ОВА);
	+ шаблони звернень до населення, брифінгів, пресрелізів.

**Приклад:** регулярні брифінги РНБО, МОЗ і КМУ під час пандемії COVID-19 та в перші місяці вторгнення РФ у 2022 році.

Нормативно-правове забезпечення кризового менеджменту в Україні має **інтегрований характер** — від загальнонаціональних законів і стратегій до відомчих протоколів і технічних інструкцій. Вони формують правову базу для управління ризиками, забезпечення координації та підтримки функціонування держави в умовах надзвичайних загроз. Постійне оновлення цих актів — ключова умова адаптації до нових викликів безпеці.

**Змістовий модуль 2. Кризового менеджменту у сфері національної безпеки : мікрорівень**

**Тема 4. Розробка плану кризового управління на підприємстві у контексті національної безпеки (**ЗК 1. ЗК 6. ЗК 7. ЗК 10. СК 1. СК 4. СК 5. СК 7. СК 13. СК 16. ПРН 3. ПРН 4. ПРН 6. ПРН 8. ПРН 9. ПРН 10. ПРН 13. )

1. Ідентифікація та оцінка ризиків для підприємства, визначення потенційних загроз для операцій підприємства (наприклад, кіберзагрози, технологічні ризики, економічні та природні ризики) та їхній вплив на національну безпеку.
2. Створення кризового плану дій, розробка детальних сценаріїв реагування на можливі кризи, включаючи інструкції для ключового персоналу та чіткий порядок дій у разі надзвичайних ситуацій.
3. Визначення критичних ресурсів та їхній захист, ідентифікація ресурсів, необхідних для безперервної роботи підприємства (наприклад, ІТ-інфраструктура, фінансові активи, персонал) та розробка заходів для їхнього захисту.
4. Резервні плани та альтернативні ресурси, створення резервних варіантів для підтримки операцій у разі втрати основних ресурсів, зокрема дублюючі сервери, альтернативні постачальники тощо.
5. Регулярне тестування плану та навчання персоналу, проведення навчань та симуляцій кризових ситуацій для персоналу, а також тестування ефективності кризового плану для виявлення недоліків.
6. Оцінка ризиків національного рівня, аналіз якості плану підприємства на предмет його відповідності загальнонаціональним стандартам безпеки та вимогам регуляторів.

***1. Ідентифікація та оцінка ризиків для підприємства***

На першому етапі формується **реєстр потенційних загроз**, які можуть вплинути на безперервність бізнесу та створити вторинні загрози для державної безпеки. Здійснюється аналіз за категоріями:

* Кіберзагрози: атаки на ІТ-інфраструктуру, витік даних, злам систем управління.
* Технологічні ризики: аварії на виробництві, відмова обладнання, втрати контролю за небезпечними процесами.
* Економічні ризики: коливання валют, санкції, відтік капіталу, логістичні розриви.
* Природні загрози: повені, пожежі, зсуви, пандемії.

Оцінюються **ймовірність** та **ступінь впливу** кожного ризику на критичні функції підприємства (наприклад, виробництво, ланцюги постачання, захист персоналу) та **його можливий резонанс у національному масштабі** (як-от загроза стратегічній інфраструктурі або дестабілізація критичного ринку).

***2. Створення кризового плану дій***

Розробляється формалізований документ – кризовий план управління, що містить:

* Структуровані сценарії реагування для кожної категорії загроз;
* Регламент дій ключових осіб: відповідальні особи, резервні повноваження, контакти, логістичні маршрути;
* Протоколи активації кризових штабів;
* Алгоритми комунікації з державними органами (ДСНС, СБУ, ОВА);
* Процедури оповіщення персоналу і зовнішніх контрагентів.

У плані мають бути закладені положення щодо **відновлення репутації** у разі інформаційної атаки, а також протидії **інсайдерським загрозам**.

***3. Визначення критичних ресурсів та їхній захист***

Необхідно скласти **матрицю критичних ресурсів**, включно з:

* Цифровою інфраструктурою (сервери, CRM, SCADA-системи);
* Фінансовими активами (резервні фонди, страхування);
* Персоналом (ключові спеціалісти, охорона, ІТ-підтримка);
* Інтелектуальною власністю (технічна документація, патенти).

Захист ресурсів забезпечується через **багаторівневу безпеку**: шифрування, фізичний захист, режим обмеженого доступу, страхування ризиків, розміщення даних у хмарі з багатофакторною автентифікацією.

***4. Резервні плани та альтернативні ресурси***

Для кожного критичного процесу розробляється **альтернативний сценарій дій**:

* Дублюючі дата-центри, розміщені в безпечних регіонах або за кордоном;
* Запасні постачальники та транспортні маршрути (особливо для критичних комплектуючих);
* Мобільні генератори, автономні системи зв’язку;
* Підрядники на випадок знищення або втрати персоналу;
* Аварійні плани з переміщення персоналу або виробничих потужностей.

Також визначаються **умови активації резервних потужностей** (тригери), строки переходу та відповідальні за реалізацію.

***5. Регулярне тестування плану та навчання персоналу***

Ефективність кризового плану залежить від **його актуальності та готовності персоналу діяти**:

* Проводяться **регулярні симуляції криз**: сценарії аварій, зламів, евакуації;
* Впроваджуються **тренінги для керівного складу та відповідальних осіб**;
* **Тестування каналів оповіщення**, резервного доступу до ІТ-ресурсів;
* Ведеться **журнал реагувань**, де фіксуються результати перевірок і виявлені вразливості;
* План оновлюється не рідше ніж раз на рік або після кожного інциденту.

***6. Оцінка ризиків національного рівня***

Завершальним етапом є **інтеграція корпоративного плану в національну систему безпеки** через:

* **Зіставлення з державними нормативами**: Кодекс цивільного захисту, стандарти ISO 22301, ДСТУ 9001, вимоги НБУ/СБУ для стратегічних підприємств;
* Взаємодія з **обласними штабами цивільного захисту, ДСНС, кіберпідрозділами СБУ**;
* Участь у **державних тренуваннях з критичної інфраструктури**;
* Проведення **аудиту відповідності** стандартам безпеки та звітність перед регуляторами;
* Забезпечення **інформаційної сумісності** з державними платформами раннього оповіщення (через API, спеціальні канали зв’язку).

Розробка плану кризового управління на підприємстві — це не лише інструмент внутрішнього ризик-менеджменту, а й **внесок у зміцнення національної безпеки**, особливо у сферах критичної інфраструктури, оборонної промисловості, енергетики та цифрових технологій. Такий план має бути динамічним, міждисциплінарним і включеним до системи державної стійкості.

### Тема **5. Стратегія забезпечення національної безпеки на рівні підприємства: від оцінки ризиків до реагування (ЗК 1. ЗК 6. ЗК 7. . ЗК 10. СК 1. СК 4. СК 5. СК 7. СК 13. СК 16. ПРН 3. ПРН 4. ПРН 6. ПРН 8. ПРН 9. ПРН 10. ПРН 13. )**

1. **Аналіз загроз для підприємства в контексті національної безпеки,** визначення потенційних внутрішніх та зовнішніх загроз, таких як кіберзагрози, ризики ланцюга постачання, техногенні аварії та їхній вплив на національну безпеку.
2. **Розробка політики кризового менеджменту на підприємстві,** встановлення єдиної політики та стандартів для забезпечення готовності до кризових ситуацій, включаючи регулярне оновлення процедур і заходів реагування.
3. **Класифікація ресурсів за ступенем критичності,** визначення ключових ресурсів підприємства (наприклад, IT-інфраструктура, обладнання, персонал) та пріоритетність їх захисту з урахуванням впливу на національну безпеку.
4. **Планування безперервності бізнесу (Business Continuity Planning, BCP),** розробка планів, які забезпечують безперервну роботу підприємства у разі кризи, включаючи резервні канали зв'язку та альтернативні поставки.
5. **Навчання персоналу з управління кризами,** проведення тренінгів та симуляцій кризових ситуацій для співробітників, включаючи навчання швидкому реагуванню та координації дій під час надзвичайних ситуацій.
6. **Оцінка ефективності кризових заходів,** регулярний перегляд та вдосконалення планів кризового менеджменту на основі досвіду попередніх криз і змін у зовнішньому середовищі.

***1. Аналіз загроз для підприємства в контексті національної безпеки***

Аналіз загроз охоплює як **внутрішні**, так і **зовнішні ризики**, які можуть впливати не лише на операційну діяльність підприємства, а й на **стабільність сектору економіки або регіону**:

* **Кіберзагрози**: злам баз даних, проникнення в SCADA-системи, віруси типу ransomware, що можуть паралізувати управління (приклад — атака NotPetya).
* **Ризики ланцюга постачання**: блокада портів, знищення логістичних вузлів, залежність від одного критичного постачальника з-за кордону (приклад — руйнування транспортної інфраструктури під час війни РФ проти України).
* **Техногенні аварії**: витоки хімічних речовин, вибухи, пожежі, що можуть загрожувати не лише підприємству, а й екологічній і санітарній безпеці регіону.

Оцінка здійснюється за шкалою впливу на виробничий цикл і ризику для національної критичної інфраструктури.

***2. Розробка політики кризового менеджменту на підприємстві***

Політика кризового менеджменту — це **внутрішній регламент**, що визначає процедури:

* Встановлення **єдиної термінології та алгоритмів реагування** (відповідно до ISO 22301:2019).
* Визначення відповідальних осіб, їхніх повноважень і процедур делегування.
* Регулярне оновлення **планів реагування** на основі змін зовнішнього середовища та з урахуванням досвіду інших підприємств.
* Впровадження **системи внутрішнього моніторингу** та індикаторів, які сигналізують про настання кризової ситуації (наприклад, збої в ІТ-системах або порушення постачань).

Приклад: на підприємствах енергетики такі політики вже адаптовані до вимог НКРЕКП та ДСНС щодо захисту від кіберзагроз.

***3. Класифікація ресурсів за ступенем критичності***

Підприємство визначає ключові ресурси, без яких **зупиняється виробництво або втрачається контроль**, і пріоритезує їх:

* **IT-інфраструктура**: сервери, хмарні сховища, системи автоматизації виробництва.
* **Обладнання**: унікальні технологічні вузли, які неможливо оперативно замінити.
* **Людський капітал**: спеціалісти з вузькою компетенцією, керівники кризових груп.

Кожен ресурс оцінюється за параметрами:

1. Час відновлення (RTO).
2. Допустимий рівень втрат.
3. Залежність від зовнішніх ресурсів (енергія, зв’язок, паливо).

**Приклад**: для підприємства у сфері водопостачання критичним буде насосне обладнання й енергозабезпечення, а для логістичного хабу — системи GPS-навігації та охорони.

***4. Планування безперервності бізнесу (BCP)***

BCP забезпечує **стійкість функціонування** підприємства навіть за умов тривалого впливу кризових факторів:

* Створення **резервних копій даних** у безпечному середовищі (віддалене хмарне зберігання).
* Використання **альтернативних каналів зв’язку** — супутниковий інтернет, радіозв’язок.
* Встановлення **альтернативних постачальників** критичних ресурсів, розгалуження логістики.
* Розробка **«гарячих» і «холодних» майданчиків** — резервних виробничих або офісних приміщень.

**Приклад**: під час вторгнення РФ у 2022 році українські банки оперативно перемістили основні системи в західні області та вивели частину потужностей у ЄС — завдяки заздалегідь прописаним BCP-планам.

***5. Навчання персоналу з управління кризами***

Без підготовленого персоналу навіть ідеальний план залишиться неефективним:

* **Симуляції кризових ситуацій**: сценарії кібератаки, пожежі, евакуації, зникнення ключових даних.
* **Інструктажі та онлайн-тестування**: перевірка знань щодо алгоритмів дій у надзвичайних ситуаціях.
* **Внутрішні навчальні модулі**: спеціальні тренінги для ІТ-служб, логістів, HR, охорони, медичних підрозділів.
* **Координаційні навчання з органами державної влади**: участь у штабних навчаннях ДСНС, МОЗ, СБУ (для стратегічних підприємств).

Приклад: щорічне навчання персоналу аеропортів України щодо масової евакуації, вибухових загроз, авіаційної безпеки.

***6. Оцінка ефективності кризових заходів***

Здійснюється через систему **періодичного аудиту**:

* Аналіз відповідності планів до нових ризиків, нормативів (напр. ISO 31000, NIST, ДСТУ 9001).
* Ревізія результатів симуляцій: час реакції, ефективність комунікації, рівень втрат.
* Оцінка **інцидентів попередніх періодів**: які дії спрацювали, де були провали.
* **Залучення зовнішніх експертів** або аудитора з кібербезпеки, логістики, антикризового планування.
* Ведення **бази знань кризових інцидентів** (інцидент-репортинг), звітування на рівень керівництва.

**Приклад**: компанії оборонного комплексу переглядають свої BCP-плани щоквартально у зв’язку з динамічними загрозами війни, санкцій і логістичних обмежень.

Ефективна стратегія забезпечення національної безпеки на рівні підприємства — це **системне поєднання оцінки ризиків, процедурної дисципліни, технологічної готовності та людського чинника**. Такі підприємства стають не лише стійкими до зовнішніх шоків, а й опорними точками **економічної, інформаційної, екологічної та оборонної безпеки держави**. У сучасних умовах вони відіграють роль **«вузлів національної стійкості»** в системі захисту критичної інфраструктури України.

**Тема 6. Кризове планування та запобігання загрозам національній безпеці (**ЗК 1. ЗК 6. ЗК 7. . ЗК 10. СК 1. СК 4. СК 5. СК 7. СК 13. СК 16. ПРН 3. ПРН 4. ПРН 6. ПРН 8. ПРН 9. ПРН 10. ПРН 13. ПРН 14. )

1. Принципи та етапи кризового планування на національному рівні.
2. Аналіз ризиків та розробка планів реагування.
3. Прогнозування можливих сценаріїв розвитку кризових ситуацій.
4. Профілактичні заходи для зниження впливу криз на національну безпеку.
5. Стратегічне резервування ресурсів для кризових ситуацій.
6. Навчання та тренінги для підготовки державних службовців.

***1. Принципи та етапи кризового планування на національному рівні***

**Принципи:**

* **Превентивність** — акцент на раннє виявлення та зниження ймовірності виникнення кризи.
* **Системність** — координація між усіма секторами безпеки (військовим, економічним, інформаційним, гуманітарним).
* **Гнучкість** — здатність адаптувати план до динамічних умов.
* **Міжвідомча інтеграція** — узгодженість дій між органами виконавчої влади, ОВА, спецслужбами, міжнародними партнерами.

**Етапи:**

1. Визначення об'єктів критичної важливості (інфраструктура, сфери державного управління).
2. Аналіз загроз і вразливостей.
3. Формування сценаріїв розвитку подій.
4. Розробка процедур реагування.
5. Визначення відповідальних органів і осіб.
6. Впровадження, моніторинг, коригування планів.

Приклад: Національний план реагування на пандемію COVID-19 був реалізований у 2020 році за участю МОЗ, ДСНС, МВС, Мінінфраструктури.

***2. Аналіз ризиків та розробка планів реагування***

Аналіз ризиків передбачає використання таких інструментів, як:

* SWOT-аналіз, PESTLE, карти загроз;
* Оцінка ймовірності виникнення події × рівень впливу (Risk Matrix);
* Інтерв’ювання експертів, робота з даними OSINT.

На основі цього формуються **галузеві плани реагування**:

* при терористичних актах (СБУ);
* при техногенних катастрофах (ДСНС);
* у разі порушень енергетичної безпеки (Міненерго).

**Приклад:** впроваджений у 2022 році спеціальний план дій на випадок руйнування гідротехнічних споруд (зокрема, після атаки на Каховську ГЕС).

***3. Прогнозування можливих сценаріїв розвитку кризових ситуацій***

Прогнозування дозволяє заздалегідь готуватися до:

* **Багатофакторних сценаріїв** (наприклад, поєднання енергетичної кризи та інформаційної атаки).
* **Сценаріїв ескалації** — від локальної аварії до національного рівня НС.

Використовуються:

* математичні моделі,
* big data,
* сценарне планування,
* експертні симуляції.

**Приклад:** у 2021–2022 роках моделювалися сценарії широкомасштабної агресії РФ, що дозволило в окремих регіонах створити пункти оборони, мобілізації та логістики ще до активної фази вторгнення.

***4. Профілактичні заходи для зниження впливу криз на національну безпеку***

До таких заходів належать:

* Інженерний захист інфраструктури (укриття, вибухозахищені зони).
* Резервування каналів зв’язку, розміщення дата-центрів у захищених регіонах.
* Законодавче регулювання — заборона на імпорт із ризикованих держав, санкції.
* Інформаційна гігієна — медіакампанії з протидії дезінформації.

**Приклад:** встановлення бетонних захисних конструкцій довкола енергооб’єктів у Дніпропетровській області у 2023 році.

***5. Стратегічне резервування ресурсів для кризових ситуацій***

Створення та управління державними резервами:

* **Матеріальні запаси** (паливо, медикаменти, продовольство);
* **Резервні потужності** — генератори, мобільні шпиталі, транспортування;
* **Фінансові фонди** — резервний фонд КМУ, стабілізаційні бюджети.

**Інституції:** Держрезерв, Міноборони, МОЗ, НБУ (для фінансової безпеки).

**Приклад:** створення запасів генераторів і обігрівачів для «Пунктів незламності» у зимовий період 2022–2023 рр.

***6. Навчання та тренінги для підготовки державних службовців***

Навчання є ключем до злагодженості:

* **Штабні навчання** на національному та регіональному рівнях;
* **Моделювання криз** з різними сценаріями (теракт, кіберзагроза, аварія);
* **Курси з управління ризиками, кризовими комунікаціями, логістикою**.

Платформи підготовки:

* Національна академія державного управління;
* Школа державного управління при РНБО;
* Центри професійної освіти при МОЗ, ДСНС.

Приклад: багаторівневе навчання держслужбовців з управління кризами під егідою НАТО в межах програми «Розбудова стійкості» (2023).

Кризове планування на національному рівні — це **проактивний і системний процес**, що охоплює прогнозування, профілактику, реагування й навчання. У сучасних умовах гібридних загроз лише скоординоване планування, підкріплене стратегічними резервами, дає змогу мінімізувати вплив криз і зміцнити стійкість держави.

**Тема 7. Інформаційна безпека та її значення у кризовому менеджменті (**ЗК 1. . ЗК 6. ЗК 7. . ЗК 10. СК 1. СК 4. СК 5. СК 7. СК 13. СК 16. ПРН 3. ПРН 4. ПРН 6. ПРН 8. ПРН 9. ПРН 10. ПРН 13. ПРН 14. )

1. Вплив інформаційних загроз на національну безпеку в умовах кризи.
2. Основні методи забезпечення інформаційної безпеки.
3. Інструменти моніторингу інформаційного простору під час криз.
4. Протидія дезінформації та фейковим новинам.
5. Роль державних та приватних ЗМІ в кризовому менеджменті.
6. Стратегія інформаційної підтримки для населення у кризових ситуаціях.

***1. Вплив інформаційних загроз на національну безпеку в умовах кризи***

Інформаційна безпека є критичним компонентом національного кризового менеджменту. В умовах кризи (військової, економічної, соціальної) **інформаційні загрози** можуть мати не менший вплив, ніж фізичні атаки:

* **Підрив довіри до держави** через цілеспрямовані інформаційні кампанії.
* **Поширення паніки** — особливо в умовах воєнного часу або техногенних катастроф.
* **Маніпуляція громадською думкою** з метою провокацій протестів чи підриву мобілізації.
* **Кібероперації з інформаційною метою** — злам акаунтів посадовців, створення фейкових повідомлень, deepfake-записи.

**Приклад:** масове поширення фейкових повідомлень у Telegram про нібито евакуацію ЗСУ з Бахмута або фальшиві повідомлення про хімічну загрозу в Харкові у 2023 році.

***2. Основні методи забезпечення інформаційної безпеки***

Забезпечення інформаційної безпеки охоплює три рівні:

* **Технічний** — захист каналів передачі інформації (VPN, шифрування, сервіси захисту e-mail та хостингів).
* **Організаційний** — формалізація протоколів комунікації, створення crisis-команд, перевірка достовірності джерел.
* **Стратегічний** — формування довгострокової інформаційної політики держави та підприємств.

**Приклад:** застосування в Україні національного інструменту Cyber Rapid Response Teams (CRRTs) за підтримки ЄС для захисту державних порталів у період кіберкампаній РФ.

***3. Інструменти моніторингу інформаційного простору під час криз***

Для своєчасного виявлення загроз і реагування застосовуються:

* Системи моніторингу медіа та соцмереж (наприклад, SemanticForce, YouScan, Sprinklr).
* OSINT-платформи для відкритої розвідки (Bellingcat, Maltego, CrowdTangle).
* Алгоритми аналізу настроїв населення (sentiment analysis), що виявляють вогнища зростання напруги.
* Аналітичні панелі (dashboards) в урядових ситуаційних центрах.

Приклад: під час вторгнення РФ у 2022 році Центр стратегічних комунікацій та інформаційної безпеки України відстежував понад 2000 джерел дезінформації щодня.

***4. Протидія дезінформації та фейковим новинам***

Протидія фейкам — завдання не лише держави, а й журналістських спільнот та ІТ-компаній:

* Платформи фактчекінгу (StopFake, VoxCheck, MythDetector).
* Автоматизовані фільтри для фейкових акаунтів і бот-мереж.
* Створення офіційних каналів поширення інформації (застосунок "Дія", Telegram-канал МОЗ).
* Юридична відповідальність — блокування пропагандистських ресурсів, заборона мовлення ворожих ЗМІ (наприклад, Medvedchuk Media).

**Приклад:** Telegram-бот «Перевірка» від Мінцифри для ідентифікації фейкових повідомлень серед населення.

***5. Роль державних та приватних ЗМІ в кризовому менеджменті***

У кризовий час медіа стають **інструментом національної мобілізації**:

* **Державні ЗМІ** (UA:Суспільне, АрміяFM) — оперативне інформування, координація дій.
* **Приватні медіа** — забезпечення багатоканальності, доступ до аудиторій із різною довірою до джерел.
* **Медіа як елемент психологічної підтримки** — трансляції програм для дітей під час війни, популяризація історій про стійкість.

**Приклад:** об’єднаний телемарафон «Єдині новини» став платформою для централізованого інформування населення протягом всієї фази воєнного стану.

***6. Стратегія інформаційної підтримки для населення у кризових ситуаціях***

Інформаційна стратегія в умовах кризи повинна:

* **Забезпечити доступ до правдивої та своєчасної інформації** (push-сповіщення, мобільні застосунки, радіо, телебачення).
* **Формувати наративи стійкості** — не лише попередження, а й мотиваційна комунікація.
* **Використовувати просту, уніфіковану мову**, доступну різним віковим групам.
* **Включати інклюзивні та багатомовні формати** (сурдопереклад, переклади для нацменшин).

**Приклад:** застосунок «Повітряна тривога» від Ajax Systems та ІТ-команди Міністерства цифрової трансформації забезпечує безперебійне інформування громадян у реальному часі.

Інформаційна безпека є **невід'ємною складовою національної стійкості**, особливо в умовах воєнних, гуманітарних і технологічних криз. Ефективна стратегія включає моніторинг, комунікацію, протидію дезінформації та інформаційну підтримку громадян, що дозволяє **зміцнювати довіру до держави, запобігати паніці та мобілізувати ресурси на захист національної безпеки**.

**Тема 8. Координація між державними структурами під час криз (**ЗК 1. . ЗК 6. ЗК 7. . ЗК 10. СК 1. СК 4. СК 5. СК 7. СК 13. СК 16. ПРН 3. ПРН 4. ПРН 6. ПРН 8. ПРН 9. ПРН 10. ПРН 13. ПРН 14. )

1. Роль органів національної безпеки у координації під час криз.
2. Протоколи спільних дій між відомствами.
3. Співпраця з місцевими органами влади у кризових ситуаціях.
4. Алгоритми реагування та подолання кризових ситуацій на регіональному рівні.
5. Інформаційний обмін між різними структурами під час криз.
6. Використання цифрових платформ для координації дій у кризовий період.

***1. Роль органів національної безпеки у координації під час криз***

Ключовими координуючими суб’єктами є:

* **Рада національної безпеки і оборони України (РНБО)** — формує стратегічні рішення, ініціює мобілізаційні заходи, координує діяльність силових структур;
* **Кабінет Міністрів України (КМУ)** — організовує реалізацію рішень РНБО, розподіляє ресурси між міністерствами, забезпечує нормативно-правову підтримку реагування;
* **Офіс Президента та Ситуаційний центр** — оперативно реагує на загрози національній безпеці;
* **Служба безпеки України (СБУ)** — відповідає за контррозвідку, боротьбу з диверсіями, кіберзагрозами, координацію в галузі інформаційної безпеки;
* **Міністерство внутрішніх справ (МВС)** — забезпечує громадський порядок, реагує на кризові події, координує діяльність Національної поліції, ДСНС, Національної гвардії.

**Приклад**: під час повномасштабного вторгнення РФ у 2022 році саме РНБО та КМУ визначали координаційні рішення щодо евакуації, введення обмежень, розподілу гуманітарних вантажів і взаємодії між регіонами.

***2. Протоколи спільних дій між відомствами***

Для ефективної координації застосовуються стандартизовані документи:

* **Єдиний державний план реагування на надзвичайні ситуації** — фіксує повноваження міністерств, ОВА, комунальних служб;
* **Шаблонні протоколи** (SOP — Standard Operating Procedures) — визначають послідовність дій у випадках техногенних катастроф, терактів, епідемій;
* **Регламент взаємодії між ДСНС, МОЗ, СБУ, Міноборони** — при виконанні спільних операцій;
* **Оперативні накази штабу** — застосовуються для термінового реагування (наприклад, у випадку атаки БПЛА або мінування).

**Приклад**: під час знеструмлення об'єктів критичної інфраструктури внаслідок ракетних ударів у 2022–2023 рр. було реалізовано протокол швидкого розгортання “Пунктів незламності” спільно ДСНС, Мінцифри, МОЗ і ОВА.

***3. Співпраця з місцевими органами влади у кризових ситуаціях***

Місцева влада виконує функцію:

* **Оперативного реагування на рівні громад** (відкриття укриттів, евакуація, мобілізація резервів);
* **Зв’язку з населенням** — локальні канали інформування;
* **Збір даних про ситуацію «знизу»** та їх передача до центру.

ОВА та РВА створюють **оперативні штаби**, де представлені ДСНС, поліція, військові, енергетики, медики.

**Приклад**: Львівська ОВА у жовтні 2022 року першою запровадила регіональний план енергетичної безпеки в умовах обстрілів критичної інфраструктури, що стало зразком для інших областей.

***4. Алгоритми реагування та подолання кризових ситуацій на регіональному рівні***

На регіональному рівні діють:

* **Штаби з ліквідації наслідків НС**, створені при ОВА/РВА;
* **Алгоритми евакуації, укриття, медичного супроводу** — розроблені за типом загроз;
* **Плани територіальної оборони** — інтеграція військових, ТРО, місцевих ресурсів;
* **Місцеві резерви** — гуманітарні запаси, паливо, генератори, питна вода.

**Приклад**: Дніпропетровська область у 2023 році реалізувала механізм оперативної ротації лікарень при масовому надходженні постраждалих з лінії фронту на основі погодженого регіонального плану МОЗ і ОВА.

***5. Інформаційний обмін між різними структурами під час криз***

Ключовими механізмами є:

* Система електронної взаємодії органів влади (СЕВ ОВВ);
* Захищені канали зв’язку спецзв’язку (ДСЗЗІ);
* Єдині ситуаційні центри при міністерствах і в ОВА;
* Щоденні дайджести ситуаційної обстановки — оперативні зведення щодо ризиків, пошкоджень, постачань.

**Приклад**: інтегрована аналітична панель Міноборони, яка надає дані про пошкодження інфраструктури, евакуацію населення та потреби у ресурсах в режимі реального часу.

***6. Використання цифрових платформ для координації дій у кризовий період***

Сучасна координація базується на **цифрових рішеннях**, зокрема:

* **«Єдина платформа кризового управління»** (розроблена за участі Мінцифри, НАК, ДСНС) — інтегрує інформацію про запаси, запити, транспорт, розміщення населення;
* **Starlink-зв’язок у регіонах** — для безперебійної роботи штабів навіть при втраті зв’язку;
* **Інструменти супутникового моніторингу** — для оцінки масштабу руйнувань, пожеж, екологічних катастроф;
* **Геоінформаційні системи (GIS)** — для візуалізації кризових зон і планування дій.

**Приклад**: використання цифрової платформи “Trembita” для координації дій під час масового переміщення ВПО в західні області у 2022 році.

Координація між державними структурами в умовах кризи — це **багаторівнева система взаємодії**, що поєднує політичне, оперативне, технічне та інформаційне управління. Успіх такої координації залежить від **чітких протоколів, цифрових інструментів, єдиного інформаційного поля та налагодженої комунікації** між центром і регіонами. Український досвід останніх років підтверджує, що стратегічна єдність управління — ключ до стійкості держави в умовах багатовекторних криз.

Начало формы

Начало формы

**Тема 9. Запобігання та протидія тероризму у контексті національної безпеки (**ЗК 1. . ЗК 6. ЗК 7. . ЗК 10. СК 1. СК 4. СК 5. СК 7. СК 13. СК 16. ПРН 3. ПРН 4. ПРН 6. ПРН 8. ПРН 9. ПРН 10. ПРН 13. ПРН 14. )

1. Основні терористичні загрози для національної безпеки.
2. Програми антитерористичного захисту на національному рівні.
3. Профілактичні заходи проти радикалізації суспільства.
4. Система моніторингу потенційних терористичних груп.
5. Міжнародна співпраця у боротьбі з тероризмом.
6. Взаємодія з громадянським суспільством у боротьбі з тероризмом.

***1. Основні терористичні загрози для національної безпеки***

В умовах гібридної війни, відкритих збройних конфліктів та загальної дестабілізації міжнародної безпеки, терористичні загрози набувають як **класичних**, так і **нетрадиційних форм**:

* **Теракти проти цивільних об'єктів**: транспорт, заклади освіти, місця масового скупчення людей.
* **Кібертероризм**: атаки на критичну інфраструктуру (енергосистеми, лікарні, урядові портали).
* **Техногенний тероризм**: використання небезпечних хімічних або біологічних речовин.
* **Інформаційний тероризм**: кампанії страху, фейкові загрози, погрози у соцмережах.
* **Тероризм, пов’язаний із зовнішнім втручанням** — діяльність іноземних агентів, диверсійно-розвідувальних груп (ДРГ), використання безпілотників.

**Приклад**: диверсійні атаки на залізничні вузли, електропідстанції та водозабори в прифронтових регіонах України у 2022–2023 роках, що поєднували елементи тероризму та воєнної агресії.

***2. Програми антитерористичного захисту на національному рівні***

В Україні діє система **антитерористичного захисту**, яка включає:

* Закон України «Про боротьбу з тероризмом»;
* Координаційний центр Антитерористичної операції при СБУ;
* Єдина державна система запобігання, виявлення і припинення **терористичних актів**, яка об'єднує СБУ, МВС, Нацполіцію, Міноборони, прикордонну службу.

Серед дієвих програм:

* «Програма підвищення захищеності об’єктів критичної інфраструктури»;
* Регулярні антитерористичні навчання;
* Впровадження протоколів охорони шкіл, ТЕС, вокзалів, водозабірних станцій.

Приклад: у 2021–2022 роках СБУ спільно з ДСНС провели навчання з реагування на хімічні теракти у містах Харків, Одеса та Дніпро.

***3. Профілактичні заходи проти радикалізації суспільства***

Запобігання тероризму передбачає роботу з «м’якими» факторами, що стимулюють радикалізацію:

* Просвітницькі програми в навчальних закладах;
* Роз’яснювальна робота в громадах з підвищеним рівнем соціальної напруги;
* Моніторинг деструктивного онлайн-контенту;
* Програми реабілітації та соціальної адаптації ветеранів і вразливих груп;
* Профілактика міжетнічних і міжконфесійних конфліктів.

**Приклад**: реалізація програм толерантності в межах «Національної стратегії з прав людини», які фінансуються за підтримки ОБСЄ та Ради Європи.

***4. Система моніторингу потенційних терористичних груп***

Цей напрямок реалізується через:

* **Аналітичні підрозділи СБУ та Нацполіції**;
* **Оперативну інформацію з кіберпростору** (моніторинг відкритих джерел, даркнету);
* **Розробку ризик-профілів** для ідентифікації потенційних радикалізованих осіб;
* **Використання біометричних даних на кордонах**;
* **Співпрацю з міжнародними структурами** (Interpol, Europol, UN CTED).

**Приклад**: завдяки системі попередження у 2023 році СБУ запобігла серії терактів у Києві та на заході України, ідентифікувавши координаторів ДРГ через Telegram і dark web.

***5. Міжнародна співпраця у боротьбі з тероризмом***

Україна є учасником:

* **Глобального форуму з боротьби з тероризмом (GCTF)**;
* **Антитерористичного центру ОБСЄ**;
* **Програми НАТО «Партнерство заради миру»** у частині кібертероризму;
* **Спільних навчань із країнами ЄС, США, Ізраїлем**.

Співпраця охоплює:

* обмін розвідувальною інформацією;
* участь у транскордонних операціях;
* спільну розробку технічних рішень для виявлення загроз.

Приклад: Українсько-ізраїльські проєкти в галузі кібербезпеки та систем захисту громадських просторів (2022–2024 рр.).

***6. Взаємодія з громадянським суспільством у боротьбі з тероризмом***

Роль громадськості — надзвичайно важлива:

* **Громадські організації** допомагають у реабілітації жертв терактів, психологічній підтримці, роботі з молоддю;
* **Освітні платформи** поширюють знання про ознаки радикалізації;
* **Ініціативи з цифрової безпеки** (наприклад, волонтерські боти протидії дезінформації);
* **Інформування держави про підозрілі дії** — через “гарячі лінії”, онлайн-звіти.

**Приклад**: волонтерський проєкт “КіберГвардія”, що об’єднує ІТ-фахівців і громадських активістів для виявлення деструктивних онлайн-груп, пов’язаних із тероризмом.

Боротьба з тероризмом у XXI столітті вимагає **мультидисциплінарного підходу**, де поряд із силовими заходами важливу роль відіграють превенція, освіта, соціальна згуртованість і міжнародна солідарність. Умови гібридної війни та інтенсивної цифровізації вимагають від держави постійного оновлення методів боротьби, посилення аналітичних можливостей та активного залучення громадянського суспільства.

**Тема 10. Кризове управління у сфері економічної безпеки (**ЗК 1. ЗК 6. ЗК 7. . ЗК 10. СК 1. СК 4. СК 5. СК 7. СК 13. СК 16. ПРН 3. ПРН 4. ПРН 6. ПРН 8. ПРН 9. ПРН 10. ПРН 13. ПРН 14. )

1. Роль економічної стабільності для національної безпеки.
2. Основні економічні загрози та методи їх подолання.
3. Запобігання фінансовим кризам та впливу на національну безпеку.
4. Стратегічні економічні резерви та їх використання у кризових ситуаціях.
5. Державні механізми підтримки малого та середнього бізнесу під час кризи.
6. Оцінка економічних ризиків у контексті національної безпеки.

***1. Роль економічної стабільності для національної безпеки***

Економічна стабільність є базисом функціонування всіх секторів національної безпеки. Вона забезпечує:

* **Фінансову незалежність держави**;
* **Збереження платоспроможності громадян і підприємств**;
* **Можливість утримання обороноздатності та соціальних гарантій**;
* **Стійкість до зовнішніх шоків** — санкцій, ембарго, глобальних криз.

**Приклад**: збереження стабільної роботи банківської системи України у 2022–2023 роках, попри воєнні дії, стало можливим завдяки швидкому втручанню НБУ та міжнародній фінансовій допомозі.

***2. Основні економічні загрози та методи їх подолання***

До ключових загроз належать:

* Інфляція та знецінення національної валюти;
* Дефіцит бюджету і зовнішній борг;
* Втрати промислового потенціалу через війну, тероризм, катастрофи;
* Порушення ланцюгів постачання та логістики;
* Енергетична залежність і нестабільність ринку енергоносіїв.

Методи подолання:

* **Монетарна політика** (підвищення облікової ставки, валютне регулювання);
* **Фіскальні заходи** (державні програми підтримки виробництва, податкові канікули);
* **Інвестиції в критичну інфраструктуру**;
* **Інтеграція з міжнародними фінансовими структурами** (МВФ, ЄБРР, Світовий банк).

**Приклад**: запровадження податкових стимулів та пільг на імпорт генераторів у період масових відключень електроенергії в 2022–2023 рр.

***3. Запобігання фінансовим кризам та впливу на національну безпеку***

Запобігання здійснюється через:

* **Створення системи раннього попередження фінансових загроз** — аналітика макропоказників, валютних коливань, індикаторів дефолту;
* **Регулювання банківської системи** — капіталізація банків, вимоги до ліквідності, страхування вкладів;
* **Контроль за державними витратами** — прозорість закупівель, аудит.

**Приклад**: у 2014–2015 рр. Україна зазнала гострої фінансової кризи. Відповіддю стали реформи НБУ, «очищення» банківської системи, введення режиму гнучкого валютного курсу.

***4. Стратегічні економічні резерви та їх використання у кризових ситуаціях***

Резерви — це інструмент негайного реагування на кризові виклики. Вони включають:

* **Фінансові резерви** (резервний фонд бюджету, золотовалютні запаси);
* **Матеріальні запаси** (паливо, зерно, медикаменти, обладнання);
* **Інфраструктурні потужності** — резервні логістичні коридори, склади, виробничі потужності, які можуть бути оперативно мобілізовані.

**Приклад**: використання стратегічних резервів зерна в 2022 році на фоні блокування портів і зростання глобального дефіциту продовольства.

***5. Державні механізми підтримки малого та середнього бізнесу під час кризи***

МСБ відіграє критичну роль у **локальній економічній стабільності**, забезпеченні зайнятості та динаміки ВВП. Підтримка може включати:

* Дотації, гранти, пільгові кредити;
* Скасування або зниження податків у прифронтових та постраждалих регіонах;
* Інкубаційні програми для релокованого бізнесу;
* Доступ до державних і міжнародних платформ (єРобота, USAID, GIZ).

**Приклад**: програма «єРобота» у 2022–2024 рр., яка профінансувала тисячі бізнесів, що забезпечили самозайнятість та створення нових робочих місць.

***6. Оцінка економічних ризиків у контексті національної безпеки***

Оцінка проводиться на основі:

* **Показників макроекономічної стабільності** (ВВП, інфляція, зовнішній борг, облікова ставка);
* **Секторного аналізу вразливості** (енергетика, агросектор, транспорт);
* **Оцінки регіональної стійкості** (рівень зайнятості, обсяг експорту, залежність від зовнішніх ринків);
* **Моделювання сценаріїв криз** (економічне моделювання, big data, GIS-аналітика).

**Приклад**: створення Центру аналізу економічної безпеки при РНБО для стратегічної оцінки ризиків з урахуванням воєнного фактору, стану інфраструктури та глобальних ринкових тенденцій.

Кризове управління у сфері економічної безпеки є **ключовим фактором виживання держави в умовах гібридних загроз, воєнної агресії та глобальних рецесій**. Ефективність такої політики визначається поєднанням **превентивних інструментів, стратегічного резервування, підтримки бізнесу та інституційної стійкості**, яка ґрунтується на прогнозуванні, цифровізації та партнерстві з міжнародними структурами.

**Тема 11. Кібербезпека у системі національної безпеки (**ЗК 1. . ЗК 6. ЗК 7. . ЗК 10. СК 1. СК 4. СК 5. СК 7. СК 13. СК 16. ПРН 3. ПРН 4. ПРН 6. ПРН 8. ПРН 9. ПРН 10. ПРН 13. ПРН 14. )

1. Основні види кіберзагроз та їх вплив на національну безпеку.
2. Стратегія забезпечення кібербезпеки на державному рівні.
3. Інструменти захисту критичної інфраструктури від кібератак.
4. Протидія кіберзлочинності та кібертероризму.
5. Стандарти та протоколи для державних органів у сфері кібербезпеки.
6. Роль державних та приватних партнерів у забезпеченні кібербезпеки.

***1. Основні види кіберзагроз та їх вплив на національну безпеку***

Кіберзагрози — це умисні або випадкові дії в кіберпросторі, які порушують функціонування державних інституцій, бізнесу чи критичної інфраструктури. Основні види:

* **Кіберзлочинність**: фішинг, шантаж через віруси-здирники (ransomware), крадіжки фінансових даних.
* **Кібершпигунство**: збирання конфіденційної інформації з урядових систем, підприємств ОПК (оборонно-промислового комплексу).
* **Кібератаки на критичну інфраструктуру**: втручання в енергетичні, транспортні, телекомунікаційні системи.
* **Інформаційно-психологічні операції**: дезінформація, підміна офіційних повідомлень.

**Приклад:** атака вірусу NotPetya у 2017 році паралізувала ІТ-системи уряду, банків, Укрзалізниці, енергетичного сектора. У 2022–2023 роках Україна щомісяця фіксувала понад 1,5 тис. кібератак, у тому числі — на системи управління безпекою.

***2. Стратегія забезпечення кібербезпеки на державному рівні***

Державна стратегія базується на таких елементах:

* **Національна стратегія кібербезпеки України (оновлена 2021 року)** — визначає пріоритети, ризики, цілі.
* **Закон України «Про основні засади забезпечення кібербезпеки України» (2017)**.
* **Координація через НКЦК (Національний координаційний центр кібербезпеки при РНБО)** — оперативна аналітика, управління кризами.
* **Роль СБУ, Держспецзв'язку, Кіберполіції** — операційна реалізація політики.

**Приклад:** у 2023 році впроваджено державну платформу MISP-UA (Malware Information Sharing Platform) для обміну інформацією про кіберінциденти між суб’єктами кіберзахисту.

***3. Інструменти захисту критичної інфраструктури від кібератак***

Критична інфраструктура включає об’єкти енергетики, водопостачання, фінансів, транспорту, зв’язку. Захист здійснюється через:

* **Системи моніторингу загроз (SIEM, SOC)** — безперервний контроль за мережами;
* **Сегментація доступу та багатофакторна автентифікація**;
* **Резервне копіювання (backup) і відновлення (disaster recovery)**;
* **Системи виявлення вторгнень (IDS/IPS)**.

**Приклад:** атомні станції України захищаються за допомогою ізольованих ІТ-систем з багаторівневим контролем доступу й моніторингом поведінки користувачів.

***4. Протидія кіберзлочинності та кібертероризму***

Складова боротьби з гібридними загрозами:

* **Кіберполіція** МВС — виявлення злочинів у цифровому середовищі (від шахрайства до бот-мереж).
* **СБУ** — розслідує терористичні атаки в кіберпросторі, у т.ч. з боку ДРГ.
* **Міжнародна співпраця** — Europol, Interpol, CERT-структури.

**Приклад:** викриття у 2022 році понад 50 кіберугруповань, що діяли в інтересах РФ, включно з групою UAC-0056, яка атакувала держсектор через фішингові листи.

**5*. Стандарти та протоколи для державних органів у сфері кібербезпеки***

Кіберзахист регулюється через:

* **Національні стандарти ДСТУ ISO/IEC 27001, 27005, 22301**;
* **Протоколи реагування на кіберінциденти** — наприклад, Наказ № 130 від Держспецзв’язку (2022) щодо категоризації критичної інфраструктури;
* **Атестація комплексів ІТС держустанов** — перевірка їх відповідності вимогам захисту інформації.

**Приклад:** міністерства й ОДА зобов’язані впроваджувати політики кіберзахисту відповідно до постанови КМУ №518 (2021), яка визначає правила захисту державної інформації.

***6. Роль державних та приватних партнерів у забезпеченні кібербезпеки***

Сильна кібербезпека можлива лише при взаємодії:

* **Держава**: СБУ, НКЦК, Мінцифри забезпечують нагляд, координацію та нормативну базу.
* **Приватний сектор**: банки, телеком-компанії, дата-центри впроваджують власні системи захисту, беруть участь у кібернавчаннях, тестують стійкість.
* **Міжнародні партнери**: НАТО, ЄС, Ізраїль, США допомагають через постачання обладнання, спільні тренінги, обмін інформацією (наприклад, про уразливості Zero Day).

**Приклад:** співпраця Держспецзв’язку з компанією Microsoft щодо аналізу атак на державні сайти у січні 2022 року дозволила ідентифікувати інструменти, що використовувалися підрозділами РФ.

Кібербезпека — це стратегічний компонент національної безпеки. У сучасних умовах цифрових воєн і гібридних конфліктів вона потребує не лише технічних рішень, а й **системної політики, стандартів, міжсекторальної координації та постійного навчання**. Український досвід демонструє, що саме цифрова стійкість стала однією з ключових переваг держави у протистоянні зовнішній агресії.

**Тема 12. Природні та техногенні катастрофи як загроза національній безпеці (**ЗК 1. ЗК 6. ЗК 7. . ЗК 10. СК 1. СК 4. СК 5. СК 7. СК 13. СК 16. ПРН 3. ПРН 4. ПРН 6. ПРН 8. ПРН 9. ПРН 10. ПРН 13. ПРН 14. )

1. Типи природних та техногенних катастроф, що загрожують національній безпеці.
2. Планування та реагування на природні та техногенні катастрофи.
3. Роль Державної служби з надзвичайних ситуацій (ДСНС) у кризовому менеджменті.
4. Інфраструктурні заходи з запобігання техногенним катастрофам.
5. Оцінка екологічних ризиків у контексті національної безпеки.
6. Міжнародна співпраця у боротьбі з природними та техногенними катастрофами.

***1. Типи природних та техногенних катастроф, що загрожують національній безпеці***

Катастрофи природного і техногенного характеру мають прямий вплив на **життя та здоров’я населення**, **економіку**, **інфраструктуру**, а отже — на **систему національної безпеки**. Вони можуть мати локальні або системні наслідки.

**Природні катастрофи:**

* Повені, засухи, землетруси, зсуви, буревії;
* Пандемії (COVID-19, пташиний грип, холера);
* Аномальні температурні коливання.

**Техногенні катастрофи:**

* Вибухи на промислових об’єктах, пожежі;
* Радіаційні аварії (наприклад, Чорнобиль);
* Розгерметизація хімічних сховищ;
* Аварії на транспорті (залізничні, морські, авіаційні).

Приклад: підрив Каховської ГЕС у 2023 році призвів до екологічної, гуманітарної та енергетичної катастрофи на регіональному рівні, з наслідками національного масштабу.

***2. Планування та реагування на природні та техногенні катастрофи***

У кризовому менеджменті діє система планування на всіх рівнях:

* Єдиний державний план реагування на НС (затверджується КМУ);
* Галузеві та регіональні плани (ДСНС, МОЗ, Мінінфраструктури);
* Сценарії дій та зонування ризиків;
* Визначення зон евакуації, укриттів, логістики медичної допомоги.

Складові реагування:

* Оповіщення населення;
* Мобілізація ресурсів;
* Взаємодія з місцевими органами влади;
* Інформування міжнародних партнерів (при загрозах транскордонного характеру).

Приклад: оперативне реагування на масштабну пожежу в Чорнобильській зоні у 2020 році із залученням авіації, військових і пожежних підрозділів з кількох областей.

***3. Роль Державної служби з надзвичайних ситуацій (ДСНС) у кризовому менеджменті***

ДСНС — центральний орган виконавчої влади, відповідальний за:

* Моніторинг та прогнозування надзвичайних ситуацій;
* Рятувальні та евакуаційні операції;
* Навчання населення правилам поведінки у надзвичайних ситуаціях;
* Координацію з міжнародними рятувальними службами.

ДСНС має у підпорядкуванні:

* Спеціальні підрозділи (водолази, піротехніки, хіміки);
* Центри реагування (мобільні штаби, ситуаційні центри);
* Навчальні заклади для підготовки кадрів.

**Приклад:** масова евакуація з підтоплених районів Херсонської області у 2023 році проводилася силами ДСНС у взаємодії з ОВА, поліцією, військовими та волонтерами.

***4. Інфраструктурні заходи з запобігання техногенним катастрофам***

Превентивні заходи включають:

* Регулярну інспекцію промислових об’єктів;
* Будівництво захисних гідротехнічних споруд;
* Встановлення сучасних систем моніторингу та сигналізації;
* Забезпечення належного технічного стану транспорту;
* **Впровадження стандартів безпеки згідно з ISO, ДСТУ, EU norms**.

**Приклад:** реконструкція дамб і шлюзів на річках Західної України після повені 2008 року з метою запобігання новим катастрофам.

***5. Оцінка екологічних ризиків у контексті національної безпеки***

Екологічні ризики — це не лише загроза довкіллю, а й джерело політичної нестабільності, економічних втрат і соціального напруження. Основні напрямки оцінки:

* Вплив забруднення води/повітря/ґрунтів на здоров’я населення;
* Можливість поширення токсичних речовин на інші регіони/країни;
* Деградація природних ресурсів (лісів, річок, земель);
* Екологічні наслідки війни (забруднення ґрунтів після вибухів, знищення екосистем).

Приклад: масштабна фіксація екологічних збитків після підриву Каховської ГЕС, яка зруйнувала систему іригації півдня України, знищила рибне господарство і спричинила спалах хвороб.

***6. Міжнародна співпраця у боротьбі з природними та техногенними катастрофами***

Україна активно залучена до:

* Механізму цивільного захисту ЄС (UCPM);
* Угоди СЕНДАІ ООН з ризиків стихійних лих (2015–2030);
* Програми НАТО з цивільного планування надзвичайних ситуацій;
* Багатосторонніх навчань з кризового реагування (RescEU, MODEX).

Форми співпраці:

* Обмін рятувальними командами;
* Надання гуманітарної та технічної допомоги;
* Спільні тренінги й симуляції.

Приклад: допомога Україні від країн ЄС у вигляді мобільних водоочисних систем, насосних станцій та генераторів після техногенної катастрофи на півдні у 2023 році.

Природні та техногенні катастрофи — це довготривалі виклики, які потребують випереджального планування, технологічної модернізації та міжнародної інтеграції. Роль ДСНС, координація між відомствами, участь громад та сучасна інфраструктура є визначальними для ефективного управління такими кризами. Український досвід останніх років підтверджує, що екологічна, технічна та гуманітарна безпека — це не локальні, а стратегічні питання національного рівня.

**Тема 13. Соціальна безпека та підтримка стабільності під час криз (**ЗК 1. . ЗК 6. ЗК 7. . ЗК 10. СК 1. СК 4. СК 5. СК 7. СК 13. СК 16. ПРН 3. ПРН 4. ПРН 6. ПРН 8. ПРН 9. ПРН 10. ПРН 13. ПРН 14. )

1. Вплив кризових ситуацій на соціальну безпеку та громадський порядок.
2. Заходи для підтримання соціальної стабільності під час криз.
3. Соціальна підтримка постраждалих під час надзвичайних ситуацій.
4. Співпраця з громадськими організаціями та волонтерськими рухами.
5. Стратегії протидії соціальним заворушенням у кризових умовах.
6. Психологічна допомога населенню у кризових ситуаціях.

***1. Вплив кризових ситуацій на соціальну безпеку та громадський порядок***

Кризові ситуації — війна, техногенні катастрофи, пандемії чи економічні потрясіння — мають безпосередній вплив на соціальну безпеку:

* **Зростання безробіття та бідності**, що створює ризик маргіналізації груп населення;
* **Соціальна фрагментація**: конфлікти на етнічному, політичному чи мовному ґрунті;
* **Послаблення довіри до інституцій** та зростання протестних настроїв;
* **Погіршення криміногенної ситуації** внаслідок зниження рівня життя;
* **Зростання тиску на соціальні служби**.

**Приклад**: під час COVID-19 та повномасштабної війни в Україні зростання кількості ВПО та погіршення доступу до послуг спричинили навантаження на місцеві громади, медичну та освітню інфраструктуру.

***2. Заходи для підтримання соціальної стабільності під час криз***

Держава та органи місцевого самоврядування вдаються до:

* **Адресної допомоги вразливим групам** (пенсіонери, ВПО, багатодітні, люди з інвалідністю);
* **Субсидій на комунальні послуги, продуктових наборів, житлових програм**;
* **Прогнозування соціальної напруги** через аналітичні центри та соцопитування;
* **Залучення релігійних громад та неурядового сектору**;
* **Утворення мобільних центрів надання соціальних послуг** у зонах бойових дій.

Приклад: створення Центрів підтримки ВПО у Львові, Тернополі, Вінниці в 2022 році, які об'єднали функції реєстрації, медичного обслуговування та юридичної консультації.

***3. Соціальна підтримка постраждалих під час надзвичайних ситуацій***

Постраждалим від криз надається:

* **Тимчасове житло** (центри розміщення, соціальні готелі);
* **Матеріальна допомога** (грошові виплати, ваучери);
* **Доступ до медицини та освіти** (включно з онлайн-платформами та мобільними пунктами);
* **Юридична допомога**, зокрема з питань втрати документів, компенсацій, статусу ВПО;
* **Реабілітаційні програми для військових, жертв насильства, травмованих дітей**.

**Приклад**: у 2023 році понад 5 млн осіб в Україні скористались програмами гуманітарної підтримки, зокрема через “єДопомогу” та Червоний Хрест.

***4. Співпраця з громадськими організаціями та волонтерськими рухами***

Громадянське суспільство є ключовим елементом стабільності:

* Волонтерські мережі забезпечують логістику, евакуацію, медичну допомогу;
* НУО займаються психологічною підтримкою, правозахистом, освітою;
* Координаційні хаби (наприклад, Razom, Nova Ukraine, “Спілка Самаритян”);
* Залучення молоді та релігійних організацій до роботи в громадах.

**Приклад**: діяльність “Пласту” та “Будуємо Україну разом” у сферах реабілітації, ремонту житла, психологічної адаптації дітей ВПО.

***5. Стратегії протидії соціальним заворушенням у кризових умовах***

Заворушення можуть виникнути через:

* Нерівний доступ до ресурсів;
* Недовіру до державних органів;
* Масову міграцію та зростання безробіття.

Для стримування:

* Створюються оперативні штаби з моніторингу громадських настроїв;
* Використовується медіа та комунікація як засіб деескалації;
* Залучаються медіатори та лідери думок для розв'язання локальних конфліктів;
* Використовуються стратегії community policing (зокрема на територіях з високою напругою).

Приклад: протидія інформаційним кампаніям РФ у Харкові та Миколаєві у 2022–2023 роках, які намагалися розпалити сепаратистські настрої.

***6. Психологічна допомога населенню у кризових ситуаціях***

Криза призводить до:

* Посттравматичних стресових розладів (ПТСР);
* Депресії, тривожних розладів;
* Агресивної поведінки в сім’ї, залежностей.

Допомога включає:

* Психологічні “гарячі лінії” та мобільні бригади;
* Освітні програми з психологічної стійкості;
* Інтеграцію ментального здоров’я в систему первинної медичної допомоги;
* Програми для дітей та підлітків у школах та таборах.

**Приклад**: державна програма «Ти як?» за підтримки ВООЗ і проєкту «Без бар’єрів», яка поширює знання про ментальне здоров’я та доступ до безкоштовної підтримки.

Соціальна безпека в умовах кризи — це не лише захист населення від наслідків подій, а й **інструмент утримання громадянської згуртованості, стабільності та довіри до держави**. Її забезпечення вимагає **інтегрованого підходу**: законодавчої підтримки, цифрових сервісів, міжсекторальної взаємодії та активної участі громадськості. Український досвід демонструє, що **соціальна мобілізація та солідарність** є ключовими ресурсами виживання у надзвичайних умовах.

**Тема 14. Міжнародна співпраця у сфері кризового менеджменту національної безпеки (**ЗК 1. . ЗК 6. ЗК 7. . ЗК 10. СК 1. СК 4. СК 5. СК 7. СК 13. СК 16. ПРН 3. ПРН 4. ПРН 6. ПРН 8. ПРН 9. ПРН 10. ПРН 13. ПРН 14. )

1. Роль міжнародних організацій у підтримці національної безпеки.
2. Угоди та протоколи міжнародного співробітництва під час криз.
3. Обмін досвідом та технологіями для підвищення ефективності кризового менеджменту.
4. Спільні навчання та тренінги з міжнародними партнерами.
5. Використання міжнародних ресурсів для реагування на кризові ситуації.
6. Взаємодія з міжнародними гуманітарними організаціями у кризових умовах.

***1. Роль міжнародних організацій у підтримці національної безпеки***

Міжнародні організації виступають не лише партнерами у стабілізації кризових ситуацій, але й джерелом ресурсів, стандартів і механізмів реагування. Основні структури:

* **ООН (через UN OCHA, UNHCR, UNDP)** – координує гуманітарну допомогу, розвитку спроможностей держав.
* **НАТО** – забезпечує стратегічне планування, військово-цивільну координацію.
* **ЄС** – через Механізм цивільного захисту UCPM надає допомогу під час катастроф, розбудовує стійкість.
* **Червоний Хрест, Міжнародна організація з міграції (IOM)** – гуманітарне реагування, захист переміщених осіб.

**Приклад**: у 2023 році UCPM ЄС забезпечив Україні понад 1000 тонн гуманітарної допомоги, включаючи генератори, насосні станції, модулі для тимчасового житла.

***2. Угоди та протоколи міжнародного співробітництва під час криз***

Міжнародне співробітництво базується на:

* Двосторонніх угодах (наприклад, між Україною та Польщею щодо транскордонного реагування);
* Міжнародних конвенціях (Конвенція про трансграничний вплив промислових аварій, Конвенція СЕНДАІ щодо зменшення ризиків лих);
* Меморандумах про взаєморозуміння між структурами ДСНС та аналогами в інших країнах;
* Стандартах взаємодії НАТО у сфері кризового управління (Crisis Response System).

**Приклад**: угода між ДСНС України та Федеральним агентством технічної допомоги Німеччини (THW) щодо спільного реагування на надзвичайні ситуації.

***3. Обмін досвідом та технологіями для підвищення ефективності кризового менеджменту***

Україна отримує:

* Новітні технології прогнозування ризиків та аналізу супутникових знімків (GIS, дрони);
* Інструменти управління критичною інфраструктурою (системи раннього попередження, мобільні командні центри);
* Освітні програми для кризових менеджерів, рятувальників, медиків;
* Методології побудови resilience (стійкості) територіальних громад.

**Приклад**: платформа Copernicus Emergency Management Services ЄС надає Україні супутникові карти для оцінки руйнувань та планування гуманітарної відповіді.

***4. Спільні навчання та тренінги з міжнародними партнерами***

Навчання та симуляційні вправи дозволяють:

* Відпрацьовувати міжвідомчу координацію;
* Покращувати навички реагування на CBRN-загрози (хімічні, біологічні, радіаційні, ядерні);
* Тестувати взаємодію цивільних та військових структур;
* Інтегрувати місцеві громади у систему реагування.

**Приклад**: щорічні навчання MODEX (EU Civil Protection Mechanism), у яких ДСНС України бере участь як спостерігач і партнер; тренінги НАТО в рамках програми «Наука заради миру та безпеки».

***5. Використання міжнародних ресурсів для реагування на кризові ситуації***

До таких ресурсів належать:

* Мобільні госпіталі, водоочисні станції, польові кухні, гуманітарні склади;
* Міжнародні фонди швидкого реагування (CERF, ECHO, USAID DRF);
* Платформи обміну даними про небезпеки (MISP, ARISTOTLE);
* Інструменти для оцінки потреб у реальному часі (NEEDS assessment tools).

**Приклад**: залучення ресурсів UNICEF, які у 2022–2023 рр. забезпечували українські громади резервуарами для води, дизельними генераторами, системами очищення води для лікарень.

***6. Взаємодія з міжнародними гуманітарними організаціями у кризових умовах***

Гуманітарні організації:

* Допомагають у розміщенні внутрішньо переміщених осіб (ВПО);
* Забезпечують харчування, медичне обслуговування, психосоціальну підтримку;
* Проводять тренінги з гуманітарного права, захисту вразливих груп;
* Сприяють прозорості розподілу допомоги через електронні реєстри та логістичні хаби.

**Приклад**: діяльність Міжнародної організації з міграції (IOM), яка забезпечила житлові модулі для понад 100 000 осіб у Харківській, Чернігівській та Миколаївській областях.

Міжнародна співпраця в умовах кризи — це **ключовий фактор збереження функціональності держави, захисту населення та відновлення постраждалих територій**. Вона охоплює нормативну, технічну, гуманітарну та освітню складові, базується на солідарності, швидкому реагуванні та міжсекторальному партнерстві. Для України, як держави в умовах тривалої війни, така співпраця є не просто підтримкою, а **інтегральною частиною національної безпеки**.

Начало формы

Конец формы