24.04.25

***Практичне заняття №4 (самостійна робота дистанційна форма) основи кризового менеджменту у сфері національної безпеки для* НБ-7,8,9**

**ТЕМА 1. КРИЗИ. КЛАСИФІКАЦІЯ КРИЗОВИХ ЯВИЩ**.

*Завдання 1 \* : Коротко надати відповідь*

1. Що таке кризовий менеджмент у сфері національної безпеки, і які його основні цілі?
2. Які етапи включає процес кризового менеджменту у сфері національної безпеки?
3. Які типи криз найбільш поширені у сфері національної безпеки (наприклад, військові, екологічні, інформаційні)?
4. Які ключові елементи управління кризовою ситуацією вимагають найшвидшого реагування?
5. Що таке національний кризовий центр, і яку роль він відіграє в кризовому управлінні?
6. Які основні методи оцінки ризиків застосовуються у кризовому менеджменті?
7. Яка роль стратегічного планування у запобіганні криз у сфері національної безпеки?
8. Яким чином можна застосовувати міжнародну співпрацю та обмін досвідом у кризовому менеджменті на рівні національної безпеки?
9. Як важливою є роль комунікації та взаємодії між різними державними інститутами під час кризи?
10. Які кроки варто вжити після завершення кризи для оцінки ефективності дій та запобігання подібним ситуаціям у майбутньому?

*Завдання 2:*

***Завдання 2.1: Аналіз кризи в сфері національної безпеки***

 Оберіть одну з реальних кризових ситуацій, пов'язаних з національною безпекою, кожен студент індивідуально обирає завдання згідно порядкового номера згідно нижченаведеного списку\*\*, наприклад :

1.Повномасштабне військове вторгнення Росії в Україну (з 24 лютого 2022 року);

2. Анексія Криму російською федерацією (лютий–березень 2014 року);

3. Збройний конфлікт на сході України (з 2014 Року);

4.Збиття пасажирського літака рейсу MH17 Над Донбасом (17 Липня 2014 Року); 5.Кібератака Notpetya на державні та приватні системи (Червень 2017 Року); 6.Масштабна кібератака на урядові сайти України (Січень 2022 Року);

7.Ракетні удари по об’єктах критичної інфраструктури, зокрема енергетичній системі (2022–2023 роки);

9.Вибухи на військових складах у калинівці, балаклії, сватовому (2015–2018 роки);

10.Терористичний акт у Краматорську — обстріл вокзалу (2015 рік);

11.Дестабілізація внутрішньої ситуації через інформаційні та психологічні операції РФ (з 2014 року);

12.Біологічна загроза в умовах пандемії COVID-19 (2020–2021 роки);

13. Кризова ситуація з біженцями та внутрішньо переміщеними особами (з 2014 року);

 14. Захоплення українських портів та блокада експорту зерна (2022) Росія захопила кілька українських портів і заблокувала експорт зерна, що погіршило глобальну продовольчу кризу; ​

15. Масштабна кібератака на енергомережу України (грудень 2015 року) Кібератака залишила без електроенергії близько 230 тисяч людей, ставши першою в історії успішною атакою на енергомережу;

16. Кібератака на Київську енергомережу (грудень 2016 року) Атака призвела до відключення електроенергії в частині Києва, використовуючи шкідливе програмне забезпечення Industroyer;

17. Захоплення Керченської протоки (листопад 2018 року) Росія захопила три українські військові кораблі та 24 моряків, загостривши морську кризу між країнами​;

18. Підрив Каховської ГЕС (червень 2023 року), Підрив дамби спричинив масштабне затоплення, екологічну катастрофу та гуманітарну кризу в регіоні;

19. Захоплення Запорізької АЕС (березень 2022 року) Російські війська захопили найбільшу атомну електростанцію в Європі, створивши загрозу ядерної катастрофи;

20. Вибухи на військових складах у Калинівці (вересень 2017 року) Вибухи на складах боєприпасів призвели до евакуації понад 30 тисяч людей і значних матеріальних збитків;

21. Вибухи на військових складах у Балаклії (березень 2017 року) Пожежа та вибухи на складах боєприпасів спричинили евакуацію понад 20 тисяч людей і знищення інфраструктури;

22. Вибухи на військових складах у Сватовому (жовтень 2015 року) Вибухи на складах боєприпасів призвели до загибелі людей і значних руйнувань у місті;

23. Терористичний акт у Краматорську (лютий 2015 року) Обстріл залізничного вокзалу в Краматорську призвів до загибелі мирних жителів і поранень десятків людей;

24. Дестабілізація через інформаційні та психологічні операції РФ (з 2014 року) Росія активно використовує пропаганду та дезінформацію для впливу на громадську думку та політичну ситуацію в Україні;

25. Біологічна загроза під час пандемії COVID-19 (2020–2021 роки) Пандемія спричинила значне навантаження на систему охорони здоров’я та економіку України;

26. Кризова ситуація з біженцями та внутрішньо переміщеними особами (з 2014 року) Мільйони українців були змушені залишити свої домівки через конфлікти на сході та в Криму;

27. Кібератака NotPetya (червень 2017 року) Масштабна кібератака, яка паралізувала державні та приватні системи в Україні та за її межами, завдавши значних економічних збитків;

28. Масштабна кібератака на урядові сайти України (січень 2022 року) Атака вивела з ладу понад 70 урядових веб-сайтів, включаючи Міністерство закордонних справ та Кабінет Міністрів.​

Проведіть аналіз кризової ситуації та розробіть покрокову стратегію реагування (від кризового штабу національної безпеки), включаючи\*\*\*:

1. Оцінку причин кризи.
2. Опис ключових дій держави у відповідь на кризу.
3. Оцінку ефективності заходів з управління кризою.
4. Запропонуйте покращення в стратегії кризового менеджменту, які могли б зменшити наслідки.
5. Швидкі заходи для зупинки атаки та мінімізації шкоди.
6. Взаємодію з ключовими стейкхолдерами (МВС, Міноборони, приватні компанії).
7. Плани відновлення інфраструктури після атаки.
8. Заходи з підвищення безпеки для запобігання подібним атакам у майбутньому.

*Ключові терміни:* Небезпека, феномен небезпеки, безпека, феномен безпеки, принципи наукового вивчення безпеки, онтологічний підхід вивчення безпеки, гносеологічний підхід вивчення безпеки, сутність і зміст поняття «криза» і «антикризовий стан», поняття «криза» і «ризик».

***\*Виконані завдання (обсягом до 5-10 стор) надіслати на ел. пошту keb\_shpak@ztu.edu.ua до 7.05.2025 та презентувати результати на наступному практичному занятті 8.05.25 р*** . *(*завдання виконувати за допомогою комп’ютера, згідно вимог : формат А4 (210x297 мм) з використанням шрифтів текстового редактора Word розміру 14 з 1,5 міжрядковим інтервалом. Мінімальна висота шрифту 1,8 мм. Текст роботи необхідно друкувати, залишаючи поля таких розмірів: ліве - 30 мм, праве -10 мм, верхнє - 20 мм, нижнє - 20 мм. Шрифт друку має бути чітким, чорного кольору середньої жирності. Щільність тексту  роботи має бути однаковою*).* ***В роботі та назві файлу, що надсилається, обов’язково вказувати групу та П.І.Б. студента.***

**Рекомендована література**

1. Антикризове управління: навчальний посібник / Б.Г. Шелегеда, О.М. Шарнопольська, М.В. Румянцев. К : ТОВ «ВРА «Епіцентр», 2013, 252 с.
2. Бєлай С. В. Державні механізми протидії кризовим явищам соціально-економічного характеру: теорія, методологія, практика : монографія. Х. : Вид-во НАНГУ, 2015, 349 с.
3. Василенко В. О. Антикризове управління підприємством: навч. посібник [для студ. вищ. навч. закл.]. К.: ЦУЛ, 2013, 504 с.
4. Дергачова В. Моніторинг національного розвитку як фактор економічної безпеки держави. *Економіка України*, № 1, 2010, С. 19-28.
5. Карпенко О.А. Основи антикризового управління : навчально-методичний посібник. – К.: Вид-во : НАДУ, 2006, 208 с.
6. Кузнєцов Є.С. Сутність антикризового управління та принципи його здійснення //Ефективна економіка, 2012, № 10. URL: https://www.economy.nayka.com.ua/?op=1&z=1488
7. Кульчій І.О.Антикризове управління: навчальний посібник. Полтава: ПолтНТУ, 2016, 120 с.
8. Мельник Ю. М. Маркетингові стратегії антикризового управління: класифікаційні ознаки та умови їх застосування. *Маркетинг і менеджмент інновацій*, 2011, № 4, Т. 2. URL: https://: http://mmi.fem.sumdu.edu.ua/
9. Мельниченко О.А. Антикризова політика держави: сутність та пріоритетні напрями // *Теорія та практика державного управління*. URL: https: http://www.kbuapa.kharkov.ua/e-book/tpdu/2015- 2/doc/1/03.pdf
10. Мельниченко О. А. Управління структурними зрушеннями : підручник. Х. : Оберіг, 2013, 300 c.
11. Основи антикризового управління: навчально-методичний посібник. К.: Вид-во НАДУ, 2010, 208 с.
12. Питер Ф. Драккер Управление нацеленное на результаты: пер. с англ. М.: Технологическая школа бизнеса, 1994, 200 с.
13. Раєвнєва О. В. Моделювання антикризового управління регіоном. Харків: вид. ХНЕУ, 2014, 300 с.
14. Редькін Д. Концептуальні основи антикризового управління. URL: <https://www.pdaa.edu.ua/sites/default/files/nppdaa/8.1/284.pdf>
15. Скібіцький О.М. Антикризовий менеджмент. Навч. посібник. К. : Центр учбової літератури, 2009, 568 с.
16. Тарасевич В. М. Про орієнтири і напрями виходу з кризи. *Економіка України*, 2013, № 9, С. 4–17.
17. Тюріна Н. М. Антикризове управління: навч. посібник [для студ. вищ. навч. закл.] / Н. М. Тюріна, Н. С. Карвацка, І. В. Грабовська. К.: ЦУЛ, 2012, 448 с.
18. Шапуров О. О. Формування концепції антикризового управління на основі взаємодії системи латентних процесів та системи діагностики явних загроз. *Інвестиції: практика та досвід*. 2013, №23, С. 35–40.
19. Шапуров О. О. Формування концепції антикризового управління на основні взаємодії системи латентних процесів та системи діагностики явних загроз. *Інвестиції: практика та досвід*, 2013, № 23. URL: <http://www.investplan.com.ua/pdf/23_2013/9.pdf>
20. Ярова І. В. Антикризове управління: сутність поняття та його визначення. *Вісн. Акад. мит. служби України.* 2012, № 2, С. 22– 28.
21. **Інформаційні ресурси в Інтернеті**
22. . http//www.un.org/ – офіційний сайт Організації Об’єднаних Націй
23. http//www.unsystem.org/index.html - інформаційний сайт про системуООН
24. http//portal.un.kiev.ua/ – Представництво ООН в Україні
25. http//www.nato.int/ – офіційний сайт НАТО
26. http//www.сoe.int /– офіційний сайт Ради Європи
27. http//www.unesco.org/ – офіційний cайт ЮНЕСКО
28. http//freedomhouse.org/ – офіційний сайт неурядової міжнародної організації
29. Freedom House
30. http//www.osce.org – офіційний сайт Організації

\*\*

**Група НБ-7**

|  |  |
| --- | --- |
| №з/п | Прізвище, ім’я та по батькові студента |
| 1 | Байдик Олександр Олександрович |
| 2 | Бродовський Віталій Віталійович |
| 3 | Будневич Софія Русланівна |
| 4 | Гераїмчук Владислав Іванович |
| 5 | Гладун Данило Володимирович |
| 6 | Горєв Сергій Сергійович |
| 7 | Гуцало Георгій Андрійович |
| 8 | Дуб Анастасія Олександрівна |
| 9 | Іваницька Анастасія Сергіївна |
| 10 | Клименко Леонід Вікторович |
| 11 | Клімаш Валерія Вікторівна |
| 12 | Коротич Іван Олександрович |
| 13 | Круглій Марія Сергіївна |
| 14 | Кужель Владислава Сергіївна |
| 15 | Кучерук Валерія Олександрівна |
| 16 | Мартинюк Ростислав Андрійович |
| 17 | Мельниченко Наталія Юріївна |
| 18 | Мудра Юлія Олександрівна |
| 19 | Оксюковський Олег Григорович |
| 20 | Проноза Олександр Романович |
| 21 | Сидоров Олександр Сергійович |
| 22 | Скобеєв Ілля Антонович |
| 23 | Стикуц Андрій Вячеславович |
| 24 | Умінський Юрій Андрійович |
| 25 | Ховрич Олександр Олегович |
| 26 | Шумінський Роман Едуардович |
| 27 | Ярмолюк Іванна Євгенівна |

**Група НБ-8**

|  |  |
| --- | --- |
| №з/п | Прізвище, ім’я та по батькові студента |
| 1 | Бєляк Вікторія Ярославівна |
| 2 | Горкуша Антон Олександрович |
| 3 | Гранисевич Валерій Олегович |
| 4 | Гудима Ангеліна Олегівна |
| 5 | Дорощук Кирило Олегович |
| 6 | Іщенко Владіслав Валентинович |
| 7 | Катюха Андрій Олегович |
| 8 | Ковальчук Богдан Миколайович |
| 9 | Кос Дмитро Олександрович |
| 10 | Лажевський Станіслав Віталійович |
| 11 | Лапшин Олександр Олександрович |
| 12 | Левченко Андрій Юрійович |
| 13 | Малишенко Владислав Леонідович |
| 14 | Мітнічук Максим Юрійович |
| 15 | Назарова Анастасія Вікторівна |
| 16 | Новомлинець Костянтин Іванович |
| 17 | Омелянський Максим Володимирович |
| 18 | Погойдаш Ілля Віталійович |
| 19 | Поцілуйко Анастасія Іванівна |
| 20 | Талько Назар Олександрович |
| 21 | Ткачук Анна Станіславівна |
| 22 | Халімовський Владислав Васильович |
| 23 | Чабан Тимофій Костянтинович |
| 24 | Черкас Вікторія Олександрівна |
| 25 | Ярошинська Валерія Сергіївна |

**Група НБ-9**

|  |  |
| --- | --- |
| №з/п | Прізвище, ім’я та по батькові студента |
| 1 | Бойко Микола Юрійович |
| 2 | Брославська Анастасія Володимирівна |
| 3 | Вихристюк Андрій Віталійович |
| 4 | Вольфман Денис Максимович |
| 5 | Гриневич Вероніка Віталіївна |
| 6 | Дербенко Олександра Максимівна |
| 7 | Кичановська Дар`я Олександрівна |
| 8 | Ковальова Діана Юріївна |
| 9 | Кордиш Анастасія Віталіївна |
| 10 | Корнійчук Артьом Юрійович |
| 11 | Крисько Андрій Анатолійович |
| 12 | Мамон Назар Олександрович |
| 13 | Міненко Дмитро Вячеславович |
| 14 | Омельянов Денис Миколайович |
| 15 | Першко Іван Дмитрович |
| 16 | Рочняк Максим Сергійович |
| 17 | Русс Олександр Русланович |
| 18 | Слюсаренко Владислав Ігорович |
| 19 | Сокіл Софія Володимирівна |
| 20 | Солонець Олександр Романович |
| 21 | Тарасюк Євгеній Олександрович |
| 22 | Ткач Артур Анатолійович |
| 23 | Федорук Юлія Василівна |
| 24 | Янголь Віталій Олександрович |
| 25 | Янішевський Антон Геннадійович |

\*\*\*Приклад –

**Аналіз кризової ситуації: Кібератака на державні органи України у січні 2022 року**

*1. Оцінка причин кризи.*

У ніч з 13 на 14 січня 2022 року було здійснено масштабну кібератаку на державні вебресурси України, включаючи сайти Кабінету Міністрів, Міністерства освіти і науки, МЗС, Держказначейства та інші. Основною причиною кризи стало поєднання зовнішньої загрози з боку ворожих державних акторів (у першу чергу — російських спецслужб) та вразливостей в інформаційній інфраструктурі. Атака відбулася на тлі загострення геополітичної ситуації, коли Російська Федерація активно готувалася до повномасштабного вторгнення в Україну. Уразливість до кіберзагроз пояснюється відсутністю належної кібергігієни, фрагментарною системою кібербезпеки та недостатнім рівнем обміну інформацією між державними органами (Див. Zhora, 2022; CERT-UA, 2022).

*2. Опис ключових дій держави у відповідь на кризу.*

У перші години після атаки Державна служба спеціального зв’язку та захисту інформації (ДССЗЗІ), спільно з CERT-UA, МВС та СБУ, розпочала реагування. Було тимчасово вимкнено деякі ресурси для мінімізації шкоди та проведення технічного аудиту. За результатами розслідування встановлено використання шкідливого ПЗ WhisperGate, що маскувався під програму для очищення даних, але фактично мав деструктивну мету — знищення інформації. Також було активовано механізми міжнародного співробітництва, зокрема — залучено допомогу партнерів з НАТО та ЄС (NATO CCDCOE, 2022).

*3. Оцінка ефективності заходів з управління кризою.*

Попри оперативну реакцію, атака засвідчила низку недоліків у системі кіберзахисту України: низький рівень міжвідомчої координації, брак резервного збереження критичних даних, слабка захищеність вебресурсів, що використовували застаріле ПЗ або не мали резервних доменів. Водночас слід визнати, що стратегічне рішення про публічне висвітлення атаки, швидке повідомлення громадськості та залучення міжнародної допомоги зменшили панічні настрої та сприяли підвищенню рівня обізнаності щодо кіберзагроз. Загалом ефективність була частковою: кризу вдалося локалізувати, однак вона виявила структурні проблеми у сфері кібербезпеки.

*4. Пропозиції щодо покращення стратегії кризового менеджменту.*

По-перше, необхідне створення єдиної інтегрованої платформи реагування на кіберінциденти з чітко визначеними ролями суб'єктів кібербезпеки. По-друге, важливо запровадити обов’язкові щорічні стрес-тести ІТ-інфраструктури всіх органів виконавчої влади. По-третє, держава має перейти до формування сталої кіберрезильєнтності, що включає регулярне навчання персоналу, впровадження багаторівневого захисту даних, використання хмарних рішень для резервного збереження, та розробку сценаріїв реагування на кризові ситуації. Нарешті, варто підсилити міжнародну інтеграцію в сфері кібербезпеки через участь у навчаннях NATO Locked Shields і координацію з ENISA (Європейське агентство з кібербезпеки).

**Стратегія реагування на масштабну кібератаку на критичну інфраструктуру**

*5. Швидкі заходи для зупинки атаки та мінімізації шкоди:*

– Активація національного центру реагування на кіберінциденти (CERT-UA) та приведення у бойову готовність оперативних груп Державної служби спеціального зв’язку та захисту інформації (ДССЗЗІ).

– Ізоляція уражених систем шляхом фізичного або логічного відключення від мережі для запобігання подальшому розповсюдженню шкідливого коду.

– Ідентифікація векторів атаки за допомогою аналізу журналів подій (логів), сканування трафіку і застосування SIEM-систем.

– Впровадження тимчасових технічних бар’єрів: блокування IP-адрес, зміна облікових даних, активація резервних маршрутів у мережах постачання енергії, води або транспорту.

– Інформування урядових структур і громадськості з метою зниження паніки та запобігання дезінформаційним кампаніям.

*6. Взаємодія з ключовими стейкхолдерами:*

– Міністерство внутрішніх справ: забезпечення правопорядку в регіонах, де зупинено життєво важливу інфраструктуру, та запобігання мародерству чи паніці.

– Міністерство оборони: активізація кіберпідрозділів Збройних сил для протидії зовнішньому втручанню, а також розгортання військових резервних систем у разі потреби.

– Приватні компанії (оператори критичної інфраструктури): спільний аудит систем, надання тимчасового доступу до об'єктів для експертів ДССЗЗІ, організація оперативних хабів для координації.

– СБУ: ведення розслідування, фіксація доказів кіберагресії, протидія ворожим інформаційним операціям.

– Міжнародні партнери (ENISA, NATO CCDCOE, EU Cyber Rapid Response Team): запит на технічну підтримку, обмін кіберрозвідкою та експертизою.

*7. Плани відновлення інфраструктури після атаки:*

– Активація резервних систем живлення та водопостачання: підключення дизель-генераторів, мобільних станцій очищення води, польових комунікацій.

– Інтеграція резервних даних із захищених бекап-сховищ для відновлення керуючих систем SCADA, систем моніторингу та автоматизації.

– Тимчасова реконфігурація транспортної логістики: створення альтернативних маршрутів та ручне управління транспортом до повного відновлення ІТ-систем.

– Поетапне повернення систем до експлуатації після перевірки їхньої безпеки — пріоритетність надається системам, що забезпечують життєдіяльність населення.

– Аудит усіх пошкоджених вузлів з метою їхнього оновлення або заміни за рахунок резервних фондів.

*8. Заходи з підвищення кібербезпеки для запобігання подібним атакам у майбутньому:*

– Прийняття оновленої національної стратегії кібербезпеки, адаптованої до умов воєнного часу та гібридної агресії.

– Розбудова кіберрезильєнтності: регулярне проведення симуляцій кібератак (penetration testing, red teaming), впровадження кібернавчань за участю всіх стейкхолдерів.

– Інвентаризація цифрових активів критичної інфраструктури та перехід на Zero Trust Architecture.

– Інтеграція систем штучного інтелекту для раннього виявлення загроз, включаючи поведінковий аналіз та автоматизоване реагування.

– Поглиблення міжнародного співробітництва, включаючи обмін даними з ЄС, НАТО, США та використання механізмів колективної кібероборони.

Ця стратегія відповідає підходам ENISA, НАТО CCDCOE та принципам ISO/IEC 27035 з управління інцидентами безпеки.