# *Семінар 4. Найкращі практики кібербезпеки*

**Мета:** узагальнення і систематизація знань з теми семінару; формування вмінь застосовувати отримані знання для рішення практичних питань і завдань; сприяння розвитку творчої самостійності студентів, поглиблюючи їх інтерес до сучасних технологій комп'ютерних систем; розвиток культури мовлення, вмінь та навичок публічного виступу, участі в дискусії.

**План заняття**

1. Потреба у кібербезпеці.
2. Атаки, поняття і методи.
3. Захист даних і конфіденційність.
4. Захист організації.
5. Правові та етичні питання кібербезпеки

**Завдання**

**Питання для обговорення**

1. Що таке кібербезпека і для чого ми вивчали цей розділ?
2. Що таке особисті дані? Де вони зберігаються? Чим відрізняється он-лайн і офф-лайн ідентифікація?
3. Чому кіберзлочинці хочуть заволодіти особистими даними?
4. Що таке корпоративні дані і як з ними пов'язана тріада CIA?
5. Які бувають наслідки порушення кібербезпеки? Наведіть 3 приклади.
6. Наведіть класифікацію зловмисників. Чим відрізняються хакери у білих, сірих і чорних капелюхах?
7. Що таке внутрішні і зовнішні загрози? Наведіть їх приклади.
8. Що таке кібервійна? Яка її мета? Наведіть приклади.
9. Які є вразливості в системі кібербезпеки? Наведіть приклади.
10. Надайте класифікацію типів зловмисного програмного забезпечення. Опишіть детально 3 типи. Які є симптоми зараження шкідливим ПЗ?
11. Назвіть 3 способи, якими зловмисник може зламати пароль Wi-Fi. Опишіть детально 1 з них.
12. Що таке соціальна інженерія і фішинг? Наведіть 2 приклади.
13. Опишіть DoS і DDoS атаки. В чому різниця між ними? Наведіть приклади. Як зменшити їх наслідки?
14. Які є правила для безпечного використання бездротових комп'ютерних мереж? Наведіть приклади небезпеки.
15. Що таке пароль і які є правила для його вибору? Що таке надійний пароль? Наведіть приклади.
16. Для чого робити резервні копії? Як це зробити? Де можна розміщати резервні копії? Як видалити свої дані остаточно?
17. Що представляє собою двофакторна аутентифікація? Наведіть приклади.
18. Що таке відкрита авторизація? Наведіть приклади.
19. Що таке конфіденційність електронної пошти і браузера? Чому не варто поширювати конфіденційну інформацію у соціальних мережах. Наведіть приклади.
20. Чим дані організацій відрізняються від особистих даних? Наведіть приклади. Хто захищає дані організацій?
21. Що таке Фаєрвол? Назвіть типи між мережних екранів. Охарактеризуйте 2 за вашим вибором.
22. Що таке пристрої безпеки? Назвіть категорії пристроїв безпеки. Охарактеризуйте 2 за вашим вибором.
23. Що представляють собою атаки реального часу? Наведіть приклади.

24. Як можна виявити атаки реального часу? Як команда може реагувати на такі атаки?

25. Назвіть найкращі практики безпеки. Охарактеризуйте 3 з них.

26. Що таке ботнет? Хто його створює і як використовує? Як можна фільтрувати ботнет-трафік?

27. Що таке ланцюг кібервбивства? Яка послідовність цього ланцюга? Охарактеризуйте 3 будь-які кроки.

28. Наведіть еволюцію кіберзагроз. Що представляє собою безпека на основі аналізу поведінки?

29. Що представляє собою технологія NetFlow? Які дані вона збирає? Для чого NetFlow призначена?

30. Що таке CSIRT? Наведіть приклади організацій, що їх мають. Що таке сценарій з організації захисту і для чого його використовують?

31. Що таке системи IDS та IPS? Для чого їх використовують? Як працює кожна з них. Поясніть необхідність правових проблем кібербезпеки. В чому відмінність хакера від фахівця з кібербезпеки? Наведіть приклади.

32. Що означає етика з кібербезпеки? Чому її потрібно дотримуватись? Наведіть приклади.

**Виконати завдання фінального екзамену у розділі 5**