МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ ТА СИСТЕМНОГО АНАЛІЗУ

ЗАТВЕРДЖЕНО
Протоколом засідання вченої ради
економіко-правового факультету
від 19.11.2020 № 5

Програма підсумкової атестації для здобувачів вищої освіти ОС «Бакалавр»

Освітньо-професійна програма «Кібербезпека»
Спеціальність «125 Кібербезпека»
Економіко-правовий факультет

Маріуполь – 2020

Програма підсумкової атестації для студентів освітньо-професійної програми Кібербезпека, спеціальності 125 «Кібербезпека» денної та заочної форми навчання

Розробники: С.В. Крівенко, доцент кафедри математичних методів та системного аналізу МДУ, кандидат технічних наук, доцент

Д.В. Гранкін, доцент кафедри математичних методів та системного аналізу МДУ, кандидат фізико-математичних наук, доцент

Ю.А. Лазаревська, старший викладач кафедри математичних методів та системного аналізу МДУ.

Програму підсумкової атестації схвалено на засіданні кафедри математичних методів та системного аналізу
Протокол від «17» листопада 2020 року № 6

ЗМІСТ

ЗАГАЛЬНА ЧАСТИНА

Державні іспити проводяться з метою перевірки рівня теоретичних знань та практичних навиків студентів-випускників напряму 125 «Кібербезпека» після вивчення теоретичних курсів спеціальних дисциплін:

- Теорія ймовірностей та математична статистика;
- Організація баз даних та знань;
- Захист інформації в комп'ютерних системах та мережах;
- Кібернетична безпека підприємства.

Перевірка якості знань проводиться після проходження студентами виробничої практики та екзаменаційної сесії 8-го семестру, передбачених навчальним планом підготовки фахівців.

Завдання, складені у відповідності з програмами спеціальних дисциплін, місять у собі три блока завдань:

перший блок – тестові завдання;

другий блок - теоретичні питання;

третій блок – практичні завдання та задачі.

Усього один пакет завдань для проведення державних іспитів містить 18 варіантів.

Час виконання завдань - 3 години. Передбачається користування обчислювальною технікою.

ПРОГРАМА

МОДУЛЬ 1. ТЕОРІЯ ЙМОВІРНОСТЕЙ ТА МАТЕМАТИЧНА СТАТИСТИКА

ТЕОРЕТИЧНИЙ БЛОК

Питання для самоконтролю

1. Випробування і події. Типи подій.
2. Дії з подіями. Повна група подій.
3. Простір елементарних подій.
4. Класичне визначення ймовірності.
5. Комбінаторика. Типи комбінацій.
6. Відносна частота подій.
7. Статистичне визначення ймовірності.
8. Геометричне визначення ймовірності.
9. Теорема додавання ймовірностей несумісних подій та її слідства.
10. Теорема додавання ймовірностей довільних подій.
11. Залежні і незалежні події. Умовна ймовірність.
12. Теорема множення ймовірностей залежних подій.
13. Теорема множення ймовірностей незалежних подій.
14. Попарно - незалежні події. Незалежні в сукупності події. Ймовірність появи хоча би однієї з незалежних подій.
15. Повна група подій. Формула повної ймовірності.
16. Формула Бейєса.
17. Випробування Бернуллі. Формула Бернуллі.
18. Локальна теорема Лапласа.
19. Теорема Пуассона.
20. Інтегральна теорема Лапласа.
21. Найімовірніше число успіхів у випробуваннях Бернуллі.
22. Відхилення відносної частоти від постійної ймовірності в незалежних випробуваннях Бернуллі.
23. Випадкова величина. Види випадкових величин.
24. Дискретна випадкова величина (ДВВ). Закон розподілу ДВВ.
25. Числові характеристики дискретної випадкової величини (математичне очікування, дисперсія, середньоквадратичне відхилення).
26. Дискретні розподіли: біноміальний, пуассонівський.
27. Неперервна випадкова величина (НВВ). Функція розподілу та щільність розподілу ймовірностей НВВ. Їх властивості та зв’язок.
28. Числові характеристики неперервної випадкової величини (математичне очікування, дисперсія, середньоквадратичне відхилення).
29. Основні розподіли НВВ: рівномірний, нормальний.

30. Предмет та задачі математичної статистики.
31. Генеральна і вибіркова сукупності. Способи відбору.
32. Варіаційний ряд і статистичний розподіл вибірки.
33. Полігон і гістограма.
34. Статистичні оцінки параметрів розподілу.
35. Властивості оцінок.
36. Поняття статистичних гіпотез. Перевірка статистичних гіпотез. Види гіпотез. Основні принципи перевірки статистичних гіпотез.
37. Статистичні критерії: параметричні і непараметричні.
38. Помилки першого та другого роду. Рівень значущості. Потужність критерію.
39. Критична область. Область ухвалення гіпотези Спостережуване і критичне значення критерію. Види критичних областей.
40. Основний принцип перевірки статистичних гіпотез. Етапи перевірки статистичних гіпотез.
41. Вибірковий коефіцієнт кореляції. Перевірка гіпотези про значущість вибіркового коефіцієнта кореляції.
42. Перевірка гіпотези про нормальний розподіл генеральної сукупності по критерію Пірсона.
43. Побудова прямої лінії регресії.

ПРАКТИЧНИЙ БЛОК

1. Автомобільний номер складається з трьох букв та чотирьох цифр. Знайти кількість всіх можливих номерів, якщо використовуються 32 букви російського алфавіту.

2. З 3 дівчат і 7 юнаків потрібно шляхом жеребкування обрати трьох делегатів на наукову конференцію. Чому дорівнює ймовірність того, що виявляться обраними три юнаки?

3. Робітник обслуговує чотири верстати. Ймовірність того, що протягом години кожен верстат не потребує уваги робітника дорівнює 0.3. Знайти ймовірність того, що протягом години хоча б один верстат зламається.

4. У піраміді встановлено 5 гвинтівок, з яких 3 мають оптичний приціл. Ймовірність того, що стрілець влучить у мішень при пострілі з гвинтівки з прицілом, дорівнює 0.95, для гвинтівки без прицілу ця ймовірність дорівнює 0.7. Знайти ймовірність того, що мішень буде поцілена, якщо стрілець зробить один постріл з навмання узятої гвинтівки.

5. Нехай схожість насіння даної рослини складає 90%. Знайти

ймовірність того, що з чотирьох посаджених зернят насіння зійдуть не менш трьох.

6. Автоматичне штампування клем для запобіжників дає 10% відхилень від прийнятого стандарту. Скільки стандартних клем варто очікувати з ймовірністю 0.0587 серед 400 клем?

7. Ймовірність поразки мішені стрільцем при одному пострілі становить 0.75. Знайти ймовірність того, що при 100 пострілах мішень буде поцілена не менш 70 і не більш 80 разів.

8. Задано функцію f(x). Необхідно знайти: а) значення постійної А, при якому f(x) буде щільністю розподілу деякої випадкової величини X; б) інтегральну функцію розподілу F(x) цієї випадкової величини X; в) математичне сподівання M(X), дисперсію D(X), середньоквадратичне відхилення □(X); г) ймовірність влучення випадкової величини X в інтервал (a,b). Побудувати графіки функцій f(x) і F(x).

$$f(x)=\begin{cases}\cos x, & |x|<\pi/2\\ 0, & |x|\geq\pi/2\end{cases}$$

$$a=0;\quad b=\pi$$

9. Наведено результати n спостережень за ознакою X. Необхідно: **а)** побудувати розподіл вибірки і полігон частот; **б)** знайти емпіричну функцію розподілу і побудувати її графік; **в)** знайти вибіркове середнє, вибіркову дисперсію і вибіркове середньоквадратичне відхилення; **г)** припускаючи, що ознака X розподілена в генеральній сукупності за нормальним законом, знайти з надійністю $\gamma=0{,}95$ інтервали довіри для оцінки невідомого математичного сподівання і невідомого середньоквадратичного відхилення у генеральній сукупності.

4	8	4	12	12	16	12	20	16	12	20	24	4	16
12	4	20	12	4	20	8	8	16	20	20	8	12	12
12	16	12	16	20	24	16	20	20	8	4	4		

10. Наведено дані, що характеризують залежність ознаки Y від ознаки X. На підставі цих даних: **а)** обчислити вибірковий коефіцієнт кореляції; **б)** знайти вибіркове рівняння лінійної регресії, що описує кореляційну залежність Y від X.

Y	X					
	6	12	18	24	30	36
4	4	1	3	–	–	–
9	–	6	11	–	–	–
14	–	2	1	52	–	–
19	–	–	–	5	6	–
24	–	–	–	–	3	6

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Гмурман В. Е. Теория вероятностей и математическая статистика. – М.: Высш. шк., 1999. – 480 с.
2. Практикум з теорії ймовірностей та математичної статистики / Р. К. Чорней та ін. – К.: МАУП, 2003.
3. Жлуктенко В. І., Наконечний С. І. Практикум з курсу “Теорія ймовірностей і математична статистика”. – К.: Вид-во КІНГ, 1991.
4. Жлуктенко В. І., Наконечний С. І. Практикум з математичної статистики. – К.: Вид-во КІНГ, 1991.
5. Каніовська І. Ю. Теорія ймовірностей у прикладах і задачах. – К.: Політехніка НТУУ КПІ, 2004. — 154 с.
6. Гихман И. И., Скороход А. В., Ядренко М. И. Теория вероятностей и математическая статистика. — К.: Выща шк., 1979. – 408 с.
7. Кремер Н. Ш. Теория вероятностей и математическая статистика. – М.: ЮНИТИ, 2000.
8. Шефтель З. Г. Теорія ймовірностей. – К., 1994.
9. Тюрин Ю. Н., Макаров А. А. Анализ данных на компьютере: — М.: ИНФРА-М, 2003. – 544 с.
10. Конет І. М. Теорія ймовірностей та математична статистика в прикладах і задачах. –Кам’янець-Подільський: Абетка, 2001. – 218 с.
11. Сеньо П. С. Теорія ймовірностей та математична статистика. – К.: Центр навч. літ., 2004. – 360 с.

МОДУЛЬ 2. ОРГАНІЗАЦІЯ БАЗ ДАНИХ ТА ЗНАНЬ

ТЕОРЕТИЧНИЙ БЛОК

1. Концептуальні та фізичні ER-моделі.
2. Логічні моделі даних на основі записів.
3. Методологія концептуального проектування баз даних.
4. Методологія логічного проектування бази даних.
5. Методологія фізичного проектування баз даних.
6. Модель „сутність-зв'язок". EER-модель.
7. Модель „сутність-зв'язок". Концепції ER-моделі.
8. Модель „сутність-зв'язок". Проблеми ER - моделювання.
9. Модель „сутність-зв'язок". Структурні обмеження.
10. Нормалізація. Мета нормалізації. Надмірність даних і аномалії відновлення.
11. Нормалізація. Перша нормальна форма 1НФ.
12. Нормалізація. Друга нормальна форма 2НФ.
13. Нормалізація. Третя нормальна форма 3НФ.
14. Нормалізація. Нормальна форма Бойса-Кодда НФБК.
15. Основні етапи процесу оптимізації запитів. Декомпозиція запитів.
16. Реляційна алгебра. Операції реляційної алгебри.
17. Реляційна алгебра. Операція вибірки. Операція різниці.
18. Реляційна алгебра. Операція проекції. Операція природного з'єднання
19. Реляційна алгебра. Операція декартового добутку.
20. Реляційна алгебра. Операція вибірки.
21. Реляційна алгебра. Операція вибірки.
22. Реляційна алгебра. Операція перетинання
23. Реляційна алгебра. Операція проекції.
24. Реляційна алгебра. Операція ділення.
25. Реляційна алгебра. Операція проекції.
26. Реляційна алгебра Операція об'єднання
27. Реляційна алгебра.. Операція різниці.
28. Реляційна алгебра Операція зовнішнього з'єднання.
29. Реляційна модель даних. Відношення. Властивості відношень.
30. Реляційна модель даних. Реляційні ключі.
31. Реляційна модель даних. Відношення. Властивості відношень.
32. Реляційна цілісність.
33. Розподілені СУБД. Основні концепції.
34. Системи з базами даних. База даних.
35. Системи з базами даних. Компоненти середовища СУБД.
36. Системи з базами даних. СУБД.
37. Транзакції. Відновлення бази даних.
38. Транзакції. Властивості транзакцій.
39. Транзакції. Управління паралельністю.
40. Файлові системи.

ПРАКТИЧНИЙ БЛОК

1. Для бази даних Відділення банку скласти відношення R1, у якому ступінь відношення дорівнює 5, кардинальне число відношення рівне 5. Скласти відношення R2, ступінь якого дорівнює 3, а кардинальне число - 2. Заповнити відношення R1 та R2 даними. Навести приклади реалізації операцій реляційної

алгебри на цих відношеннях.

2. Предметна область: База даних реалізації товарів у супермаркеті. Скласти SQL-запити по їх заданому змістовному опису. Визначити всіх клієнтів з таблиці Customers, імена яких починаються на букву J або M і відсортуйте в алфавітному порядку
3. Предметна область: База даних реалізації товарів у супермаркеті. Скласти SQL-запити по їх заданому змістовному опису. Отримати список всіх клієнтів і число зроблених ними замовлень, обов'язково включити в результат всіх клієнтів, навіть тих, які не зробили жодного замовлення.
4. Для бази даних Рибна фабрика скласти відношення R1, у якому ступінь відношення дорівнює 5, кардинальне число відношення рівне 4. Скласти відношення R2, ступінь якого дорівнює 3, а кардинальне число - 2. Заповнити відношення R1 та R2 даними. Навести приклади реалізації операцій реляційної алгебри на цих відношеннях.
5. Предметна область: База даних реалізації товарів у супермаркеті. Скласти SQL-запити по їх заданому змістовному опису. Визначити всі значення, що містять текст bean bag в будь-якому місці назви, незалежно від кількості символів перед зазначеним текстом або після нього.
6. Предметна область: База даних реалізації товарів у супермаркеті. Створити запит, який виводить два стовпці: vend_id, що містить ідентифікатор постачальника товару, і num prods, що містить поля, що обчислюються, впорядкувати дані і згрупувати їх за стовпцем vend id. В результаті значення num_prods має обчислюватися по одному разу для кожної групи записів vend id, а не один раз для всієї таблиці Products.
7. Предметна область: База даних реалізації товарів у супермаркеті. Створити запит, в якому перераховуються всі постачальники, що пропонують не менше двох товарів за ціною 4 долари і більш за одиницю.
8. Для бази даних Кондитерська фабрика скласти відношення R1, у якому ступінь відношення дорівнює 4, кардинальне число відношення рівне 4. Скласти відношення R2, ступінь якого дорівнює 4, а кардинальне число - 2. Заповнити відношення R1 та R2 даними. Навести приклади реалізації операцій реляційної алгебри на цих відношеннях.
9. Предметна область: База даних реалізації товарів у супермаркеті. Витягти список товарів, пропонованих усіма постачальниками, крім DLL01 і впорядкувати в алфавітному порядку.
10. Предметна область: База даних реалізації товарів у супермаркеті. Витягти усі товари, пропоновані або постачальником DLL01, або постачальником BRS01, які коштують 10 доларів і більше.
11. Проектується база даних Магазин мережевого устаткування. Дати стислий опис предметної області. Навести перелік базових сутностей та склад і характеристики їх атрибутів. Обґрунтувати типи зв'язків між базовими сутностями. Навести умови підтримки цілісності у базі даних. Побудувати початкову ER-модель (нотація IDEF1X). Перетворити модель таким чином, щоб вона була придатна для реалізації бази даних.
12. Для бази даних Магазин мережевого устаткування скласти відношення R1, у якому ступінь відношення дорівнює 5, кардинальне число відношення рівне 5. Скласти відношення R2, ступінь якого дорівнює 3, а кардинальне число - 2. Заповнити відношення R1 та R2 даними. Навести приклади реалізації операцій реляційної алгебри на цих відношеннях.
13. Предметна область: База даних реалізації товарів у супермаркеті. Створити запит для відображення підсумкової інформації для кожного клієнта, що містить три стовпці з таблиці Customers: cust_name, cust_state і orders. Поле Orders є обчислюваним.

14. Предметна область: База даних реалізації товарів у супермаркеті. За допомогою запиту створіть таблицю Orders, яка складається з трьох стовпців: номер і дата замовлення, а також ідентифікатор клієнта. Два стовпці не можуть містити відсутніх значень.
15. Предметна область: База даних реалізації товарів у супермаркеті. Вивести список клієнтів, які замовили товар RGAN01.
16. Для бази даних Продаж квитків на залізниці скласти відношення R1, у якому ступінь відношення дорівнює 4, кардинальне число відношення рівне 5. Скласти відношення R2, ступінь якого дорівнює 4, а кардинальне число - 3. Заповнити відношення R1 та R2 даними. Навести приклади реалізації операцій реляційної алгебри на цих відношеннях.
17. Для бази даних Автовокзал скласти відношення R1, у якому ступінь відношення дорівнює 4, кардинальне число відношення рівне 5. Скласти відношення R2, ступінь якого дорівнює 5, а кардинальне число - 2. Заповнити відношення R1 та R2 даними. Навести приклади реалізації операцій реляційної алгебри на цих відношеннях.
18. Для бази даних Фітнес-клуб скласти відношення R1, у якому ступінь відношення дорівнює 4, кардинальне число відношення рівне 5. Скласти відношення R2, ступінь якого дорівнює 4, а кардинальне число - 2. Заповнити відношення R1 та R2 даними. Навести приклади реалізації операцій реляційної алгебри на цих відношеннях.
19. Предметна область: База даних реалізації товарів у супермаркеті. Скласти SQL-запит по їх заданому змістовному опису, який вибере тільки ті товари, які відносяться до постачальника DLL01 і знайти середню вартість.
20. Для бази даних Аптека скласти відношення R1, у якому ступінь відношення дорівнює 4, кардинальне число відношення рівне 5. Скласти відношення R2, ступінь якого дорівнює 5, а кардинальне число - 2. Заповнити відношення R1 та R2 даними. Навести приклади реалізації операцій реляційної алгебри на цих відношеннях.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Бази даних у питаннях і відповідях : навч. посібн. / В. В. Чубук, Р. М. Чен, Л. А. Павленко та ін. – Х. : Вид. ХНЕУ, 2004. – 288 с.
2. Дейт Дж. Введение в системы баз данных / К. Дж. Дейт.– 8-е изд. – М. : Вильямс, 2005. –1328 с.
3. ДСТУ 2874-94. Системи оброблення інформації. Бази даних. Терміни та визначення. – К. : Держстандарт України, 1995. – 29 с.
4. Конноли Т. Базы данных: проектирование, реализация и сопро-вождение : учебн. пособ. / Т. Конноли // Теория и практика. 2-е изд. ; пер. с англ. – М. : Издательский дом "Вильямс", 2000. – 1120 с.
5. Пономаренко В. С. Інструментальні засоби розробки та підтрим-ки баз даних розподілених інформаційних систем / В.С. Пономаренко, Павленко Л.А. – Х. : Вид. ХДЕУ, 2001. – 132 с.
6. Федько В. В. Лабораторний практикум з модуля "Основи баз даних та знань" навчальної дисципліни "Організація баз даних та знань".
7. Шаров С.В. , Осадчий В.В. Бази даних та інформаційні системи. Навчальний посібник / С.В. Шаров, В.В. Осадчий. – Мелітополь: Вид-во МДПУ ім. Б.Хмельницького, 2014. – 352 с.

Інформаційні ресурси

1. American National Standards Institute (1975). ANSI/X3/SPARC Study Group on Data Base Management Systems. Interim Report, FDT. ACM SIGMOD Bulletin, 7(2).

2. ГОСТ 34.320-96 Межгосударственный стандарт. Информационные технологии. Система стандартов по базам данных. Концепции и терминология для концептуальной схемы и информационной базы // http://dp-beg.narod.ru/gost1.doc
3. Кузнецов С.Д. Базы данных. Вводный курс // http://www.citforum.ru/database/advanced_intro/

МОДУЛЬ 3. ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ

ТЕОРЕТИЧНИЙ БЛОК

1. Інформаційна безпека: сутність, поняття, схема забезпечення.
2. Модель безпеки CIA (Confidentiality, Integrity, and Availability), інші категорії моделі безпеки.
3. Нормативно-правове регулювання інформаційної безпеки.
4. Типи міжнародних організацій в сфері інформаційної безпеки.
5. Закон України № 80/94-ВР «Про захист інформації в інформаційно-телекомунікаційних системах».
6. Загальні принципи і специфічні методи забезпечення інформаційної безпеки.
7. Принципи побудови системи інформаційної безпеки.
8. Системний підхід до захисту інформації.
9. Методи і засоби забезпечення інформаційної безпеки.
10. Поняття уразливості і витоку інформації. Види уразливості.
11. Сутність криптографічних методів забезпечення інформаційної безпеки.
12. Організаційно-адміністративні заходи забезпечення комп'ютерної безпеки.
13. Принципи забезпечення інформаційної безпеки на основі інженерно-технічного забезпечення.
14. Принципи забезпечення інформаційної безпеки на основі інженерно-технічного забезпечення.
15. Основні види каналів витоку інформації. Шляхи несанкціонованого доступу до інформації.
16. Стратегія і тактика зловмисника при несанкціонованому доступі.
17. Шкідливе програмне забезпечення (malware), його види.
18. Способи практичної реалізації механізмів захисту інформації.
19. Організація конфіденційного діловодства.
20. Структура і функції служби інформаційної безпеки компанії.
21. Забезпечення інформаційної безпеки автоматизованих банківських систем.
22. Інформаційна безпека електронної комерції.
23. Електронний цифровий підпис та особливості його застосування.
24. Інформаційна безпека користувачів мобільних пристроїв.
25. Протоколи мережевого доступу AAA (Authentication, Authorization, Accounting).
26. Технології взаємодії між інформаційними системами та UNIX-подібні системи.
27. Розмежування прав доступу в UNIX-подібній системі.
28. Командні інтерпретатори, їх різновиди та відмінності. Оболонки (shells).
29. Конвеєри і перенаправлення вводу-виводу. Налаштування shell.
30. Взаємодія shell-скриптів з користувачем.
31. Умовні оператори, цикли в програмах на shell.
32. Створення функцій у програмах на shell.
33. Процеси і їх ідентифікатори. Взаємодія процесів в UNIX-подібній системі.

34. Файлові підсистеми. Робота з таблицями розділів MBR і GPT. Відновлення таблиць розділів в разі збоїв.
35. Забезпечення цілісності та доступності даних. Raid, LVM.
36. Пошук у файловій системі і в текстовому файлі. Утиліти find і grep.
37. Комп'ютерна криміналістика (форензіка): вирішувані завдання і методи.
38. Відновлення даних. Утиліти TestDisk, PhotoRec, Extundelete, Foremost.
39. Симетричні алгоритми шифрування даних.
40. Асиметричні алгоритми шифрування даних.
41. Шифрування даних. PGP / GPG: можливості та особливості програмного забезпечення.
42. Шифрування даних. TrueCrypt: можливості, особливості, нюанси програми.
43. Специфікація шифрування диску / блочного пристрою LUCKS/dm-crypt (Linux Unified Key Setup).
44. Призначення, цілі, опис ідентифікатора MAC. Засоби отримання MAC-адреси стороннього пристрою. Мотивація зловмисника при отриманні MAC-адреси чужого пристрою.
45. Налаштування і використання мережевих комунікацій в UNIX-системах.
46. Статичний і динамічний IP-адреси. Метод сканування протоколів IP.
47. Основні методи сканування Nmap.
48. Призначення, цілі, опис Honeypot.
49. Способи виявлення Honeypot.
50. Недоліки Honeypot. Проблеми, які можуть виникнути при його використанні.
51. RPC-сервіси. Цілі RPC-сканування. Важливість інформації щодо активності та розміщення таких сервісів.
52. Балансування навантаження (load balancing). Методи балансування навантаження на веб-сервер.
53. DoS / DDoS-атаки. Чотири основні класи атак, що відповідають рівням моделі ISO OSI.
54. Виявлення ознак DDoS-атаки. Основні способи захисту від DDoS-атак.
55. Брандмауер: призначення. Принцип роботи Netfilter. Таблиці брандмауера Netfilter, їх призначення.
56. Правила брандмауера. Створення правил для брандмауера утилітою Iptables.
57. Міжмережеві екрани WAF (Web Application Firewall).
58. Пісочниця (sandbox). Принцип роботи. Приклади використання. Переваги та недоліки пісочниць. Альтернативи використанню пісочниць.

ПРАКТИЧНИЙ БЛОК

1. Відкрийте два термінали (tty). В обох отримайте права суперкористувача. Використовуючи useradd, створіть користувачів «usr1» і «usr2» з домашніми каталогами «usr1» і «usr2», відповідно. Встановіть паролі для користувачів «usr1» і «usr2». Вийдіть з режиму суперкористувача в обох терміналах. Увійдіть під першим терміналом в користувача «usr1», у другому – в користувача «usr2». Подивіться, який ідентифікатор отримав користувач «usr1» і користувач «usr2» (id); результат перенаправте в файл ~/usrs.log. Подивіться права доступу на домашній каталог користувачів «usr1» і «usr2»; отриманий результат додайте в ~/usrs.log. Створіть файл під користувачем «usr2» з маскою 0077 (umask). Змініть права доступу на файл так, щоб користувач «usr1» міг записувати в файл, але не читати його. Запишіть текстову інформацію в файл з-під користувача «usr1», використовуючи консольний текстовий редактор (vi, nano, тощо). Перевірте права на файл і прочитайте його вміст з-під користувача «usr2». Створіть каталог з-під користувача «usr2». Встановіть права

запису для групи користувачів на даний каталог. Додайте користувача «usr1» в групу «usr2» (usermod). Додайте в файл ~/usrs.log інформацію про те, в які групи входить користувач «usr1». Створіть декілька файлів в каталозі, який був створений користувачем «usr2», з-під користувача «usr1». Проскануйте вміст домашньої директорії (ls -la); результати перенаправте, доповнивши файл ~/usrs.log. Вміст файлів ~/usrs.log продемонструвати у відповіді.

2. Додайте в віртуальну машину з операційною системою Linux віртуальний жорсткий диск. Запустіть віртуальну машину з операційною системою Linux. Створіть таблицю розділів (3 первинних і 1 логічний) за допомогою команди fdisk на доданому віртуальному диску. Запишіть зміни на диск. Відформатуйте створені розділи в файлову систему ext4. Змонтуйте створені розділи і створіть там довільні файли. Зробіть резервну копію MBR за допомогою утиліти DD. Зітріть таблицю розділів MBR за допомогою утиліти DD. Відновіть MBR за допомогою утиліти DD. Змонтуйте розділи і перевірте цілісність даних. Список використаних в завданні команд (fc -l <номер першої> <номер останньої>) записати в файл ~/dd.log. Вміст файлу ~/dd.log продемонструвати у відповіді.
3. Додайте в віртуальну машину з операційною системою Linux віртуальний жорсткий диск. Запустіть віртуальну машину з операційною системою Linux. Встановіть gdisk. Створіть таблицю розділів GPT (5 первинних розділів) за допомогою gdisk. Відформатуйте створені розділи в файлову систему ext3. Змонтуйте створені розділи і створіть там довільні файли. Зробіть резервну копію GPT за допомогою утиліти DD, попередньо визначивши необхідну кількість байт для резервної копії. Зітріть GPT за допомогою утиліти DD. Відновіть GPT за допомогою утиліти DD. Змонтуйте розділи і перевірте цілісність даних. Список використаних в завданні команд (fc -l <номер першої> <номер останньої>) записати в файл ~/dd.log. Вміст файлу ~/dd.log продемонструвати у відповіді.
4. Додати в віртуальну машину з операційною системою Linux 5 (п'ять) віртуальних жорстких дисків. Запустити віртуальну машину з операційною системою Linux. Встановити mdadm. Зібрати RAID 1 за допомогою mdadm. В окремому терміналі (tty) стежити за станом файлу /proc/mdstat. Встановити на створеному RAID файлову систему ext4. Змонтувати створену файлову систему. Записати туди файл raid.txt з довільним вмістом. Зруйнувати один з дисків RAID і простежити за тим, що відбувається в файлі /proc/mdstat. Перевірити цілісність файлу raid.txt. Зупинити RAID 1. Очистити інформацію дисків про приналежність до програмного RAID. Список використаних в завданні команд (fc -l <номер першої> <номер останньої>) записати в файл ~/hist.log. Вміст файлу ~/hist.log продемонструвати у відповіді. Описати зміни, що відбувалися в файлі /proc/mdstat.
5. Додати в віртуальну машину з операційною системою Linux 5 (п'ять) віртуальних жорстких дисків. Запустити віртуальну машину з операційною системою Linux. Встановити mdadm. Зібрати RAID 0 з допомогою mdadm. В окремому терміналі (tty) стежити за станом файлу /proc/mdstat. Створити на створеному RAID файлову систему ext3. Змонтувати створену файлову систему. Записати туди файл raid.txt з довільним вмістом. Зруйнувати один з дисків RAID і простежити за тим, що відбувається в файлі /proc/mdstat. Перевірити цілісність файлу raid.txt. Зупинити RAID 0. Очистити інформацію дисків про приналежність до програмного RAID. Список використаних в завданні команд (fc -l <номер першої> <номер останньої>) записати в файл ~/hist.log. Вміст файлу ~/hist.log продемонструвати у відповіді. Описати зміни, що відбувалися в файлі /proc/mdstat.
6. Додати в віртуальну машину з операційною системою Linux 5 (п'ять) віртуальних жорстких дисків. Запустити віртуальну машину з операційною системою Linux. Встановити mdadm. Зібрати RAID 5 з диском гарячої заміни за допомогою mdadm. В окремому терміналі (tty) стежити за станом файлу /proc/mdstat. Створити на

створеному RAID файлову систему ext4. Змонтувати створену файлову систему. Записати туди файл raid.txt з довільним вмістом. Зруйнувати три диска RAID і простежити за тим, що відбувається в файлі /proc/mdstat. Перевірити цілісність файлу raid.txt. Зупинити RAID 5. Очистити інформацію дисків про приналежність до програмного RAID. Список використаних в завданні команд (fc -l <номер першої> <номер останньої>) записати в файл ~/hist.log. Вміст файлу ~/hist.log продемонструвати у відповіді. Описати зміни, що відбувалися в файлі /proc/mdstat.

7. Додати в віртуальну машину з операційною системою Linux 5 (п'ять) віртуальних жорстких дисків. Запустити віртуальну машину з операційною системою Linux. Встановити mdadm. Зібрати RAID 10 з диском гарячої заміни за допомогою mdadm. В окремому терміналі (tty) стежити за станом файлу /proc/mdstat. Створити на створеному RAID файлову систему ext2. Змонтувати створену файлову систему. Записати туди файл raid.txt з довільним вмістом. Зруйнувати два диска RAID і простежити за тим, що відбувається в файлі /proc/mdstat. Перевірити цілісність файлу raid.txt. Зупинити RAID 10. Очистити інформацію дисків про приналежність до програмного RAID. Список використаних в завданні команд (fc -l <номер першої> <номер останньої>) записати в файл ~/hist.log. Вміст файлу ~/hist.log продемонструвати у відповіді. Описати зміни, що відбувалися в файлі /proc/mdstat.
8. Додати в віртуальну машину з операційною системою Linux 5 (п'ять) віртуальних жорстких дисків. Запустити віртуальну машину з операційною системою Linux. Встановити mdadm. Ініціалізувати фізичні диски, поверх яких буде створено LVM (Logical Volume Manager). Створити групу томів на основі чотирьох віртуальних жорстких дисків. Створити логічний том. На створеному логічному томі створити файлову систему. Змонтувати систему і створити файл LVM.txt. Додати в групу томів ще один віртуальний жорсткий диск. Визначити кількість доданих екстентів. Розширити створений логічний том на розмір доданих екстентів. Збільшити розмір файлової системи. Зробити снапшот логічного тому. Видалити групу томів і снапшот. Список використаних в завданні команд (fc -l <номер першої> <номер останньої>) записати в файл ~/lvm.log. Вміст файлу ~/lvm.log продемонструвати у відповіді.
9. Додайте в віртуальну машину з операційною системою Linux віртуальний жорсткий диск. Запустіть віртуальну машину з операційною системою Linux. Запустіть fdisk (gdisk або parted) і створіть таблицю розділів MBR з розділами. Відформатуйте створені розділи в файлову систему ext4. Встановіть TestDisk. Видаліть MBR (або таблицю розділів) за допомогою команди DD. Відновіть MBR (або таблицю розділів) за допомогою TestDisk. Змонтуйте відновлені розділи і створіть там довільні файли. Видаліть створені файли. За допомогою TestDisk відновите дані. Створіть довільний каталог і запишіть туди дані каталогу /var/log/. Видаліть дані зі створеного каталогу. За допомогою PhotoRec відновите дані. Створіть довільний каталог і запишіть туди дані каталогу /etc/. За допомогою Extundelete або Foremost відновите дані. Список використаних в завданні команд (fc -l <номер першої> <номер останньої>) запишіть у файл ~/dd.log. Вміст файлу ~/dd.log продемонструйте у відповіді.
10. Встановити PGP, GPG. Провести операції шифрування і дешифрування над довільними файлами. Встановити TrueCrypt версії 7.1a (https://www.truecrypt71a.com/downloads/). Створити криптоконтейнер, примонтувати його як віртуальний диск. Помістити до криптоконтейнера якусь інформацію. Отмонтувати диск і перемістити криптоконтейнер. Повторно примонтувати криптоконтейнер як віртуальний диск. Список використаних в завданні команд (fc -l <номер першої> <номер останньої>) запишіть у файл ~/crypt.log. Вміст файлу ~/crypt.log продемонструвати у відповіді.
11. Встановити LUKS/dm-crypt. Створити файл для зберігання зашифрованих даних, заповнивши його випадковими даними: dd if=/dev/urandom of=/root/testfile bs=1M count=512. Створити криптоконтейнер: cryptsetup -y luksFormat /root/testfile. Відкрити

контейнер, задавши йому ім'я volume1: cryptsetup luksOpen /root/test1 volume1. Створити в ньому файлову систему ext4: mkfs.ext4 -j /dev/mapper/volume1. Створити папку для монтування: mkdir /mnt/files. Монтувати: mount /dev/mapper/volume1 /mnt/files. Скопіювати папку /etc до криптоконтейнера. Розмонтувати: /mnt/files. Закрити volume1: cryptsetup luksClose volume1. Переконатися, що дані зашифровано. Відкрити їх, виконавши: <cryptsetup luksOpen /root/test1 volume1> і <mount /dev/mapper/volume1 /mnt/files>. Список використаних в завданні команд (fc -l <номер першої> <номер останньої>) записати в файл ~/crypt.log. Вміст файлу ~/crypt.log продемонструвати у відповіді.

12. Виконайте сканування веб-серверу методом TCP Connect. Для цього створіть дві ідентичні, за винятком MAC-адреси, віртуальні машини з Linux. Налаштуйте мережу, що складається з двох комп'ютерів, вибравши тип підключення «Мережевий міст» на обох машинах. На одну з віртуальних машин встановіть веб-сервер: sudo apt install apache2. На іншу – встановіть Nmap: sudo apt install nmap. Визначте IP-адрес віртуальної машини, де встановлений веб-сервер Apache. Проведіть сканування веб-серверу методом TCP Connect. Результат сканування запишіть в файл ~/nmapvst.log. Вміст файлу ~/nmapvst.log продемонструйте у відповіді. Прокоментуйте результати сканування.
13. Виконайте сканування веб-серверу методом TCP SYN. Для цього створіть дві ідентичні, за винятком MAC-адреси, віртуальні машини з Linux. Налаштуйте мережу, що складається з двох комп'ютерів, вибравши тип підключення «Мережевий міст» на обох машинах. На одну з віртуальних машин встановіть веб-сервер: sudo apt install apache2. На іншу – встановіть Nmap: sudo apt install nmap. Визначте IP-адрес віртуальної машини, де встановлений веб-сервер Apache. Проведіть сканування веб-серверу методом TCP SYN. Результат сканування запишіть в файл ~/nmapvss.log. Вміст файлу ~/nmapvss.log продемонструйте у відповіді. Прокоментуйте результати сканування.
14. Виконайте сканування веб-серверу методами FIN, Xmas Tree і NULL. Для цього створіть дві ідентичні, за винятком MAC-адреси, віртуальні машини з Linux. Налаштуйте мережу, що складається з двох комп'ютерів, вибравши тип підключення «Мережевий міст» на обох машинах. На одну з віртуальних машин встановіть веб-сервер: sudo apt install apache2. На іншу – встановіть Nmap: sudo apt install nmap. Визначте IP-адрес віртуальної машини, де встановлений веб-сервер Apache. Проведіть сканування веб-серверу методами FIN, Xmas Tree і NULL. Результат сканування запишіть в файли ~/nmapvsf.log, ~/nmapvsx.log, ~/nmapvsn.log. Вміст log-файлів продемонструйте у відповіді. Прокоментуйте результати сканування.
15. Виконайте сканування веб-серверу методом сканування протоколів IP. Для цього створіть дві ідентичні, за винятком MAC-адреси, віртуальні машини з Linux. Налаштуйте мережу, що складається з двох комп'ютерів, вибравши тип підключення «Мережевий міст» на обох машинах. На одну з віртуальних машин встановіть веб-сервер: sudo apt install apache2. На іншу – встановіть Nmap: sudo apt install nmap. Визначте IP-адрес віртуальної машини, де встановлений веб-сервер Apache. Проведіть сканування веб-серверу методом сканування протоколів IP. Результат сканування запишіть в файл ~/nmapvso.log. Вміст файлу ~/nmapvso.log продемонструйте у відповіді. Прокоментуйте результати сканування.
16. Виконайте сканування веб-серверу методом ACK-сканування. Для цього створіть дві ідентичні, за винятком MAC-адреси, віртуальні машини з Linux. Налаштуйте мережу, що складається з двох комп'ютерів, вибравши тип підключення «Мережевий міст» на обох машинах. На одну з віртуальних машин встановіть веб-сервер: sudo apt install apache2. На іншу – встановіть Nmap: sudo apt install nmap. Визначте IP-адрес віртуальної машини, де встановлений веб-сервер Apache. Проведіть сканування веб-серверу методом ACK-сканування. Результат сканування запишіть в файл

~/nmapvsa.log. Вміст файлу ~/nmapvsa.log продемонструйте у відповіді. Прокоментуйте результати сканування.

17. Виконайте сканування веб-серверу методом TCP Window. Для цього створіть дві ідентичні, за винятком MAC-адреси, віртуальні машини з Linux. Налаштуйте мережу, що складається з двох комп'ютерів, вибравши тип підключення «Мережевий міст» на обох машинах. На одну з віртуальних машин встановіть веб-сервер: sudo apt install apache2. На іншу – встановіть Nmap: sudo apt install nmap. Визначте IP-адрес віртуальної машини, де встановлений веб-сервер Apache. Проведіть сканування веб-серверу методом TCP Window. Результат сканування запишіть в файл ~/nmapvsw.log. Вміст файлу ~/nmapvsw.log продемонструйте у відповіді. Прокоментуйте результати сканування.
18. Виконайте сканування веб-серверу методом RPC-сканування. Для цього створіть дві ідентичні, за винятком MAC-адреси, віртуальні машини з Linux. Налаштуйте мережу, що складається з двох комп'ютерів, вибравши тип підключення «Мережевий міст» на обох машинах. На одну з віртуальних машин встановіть веб-сервер: sudo apt install apache2. На іншу – встановіть Nmap: sudo apt install nmap. Визначте IP-адрес віртуальної машини, де встановлений веб-сервер Apache. Проведіть сканування веб-серверу методом RPC-сканування. Результат сканування запишіть в файл ~/nmapvsr.log. Вміст файлу ~/nmapvsr.log продемонструйте у відповіді. Прокоментуйте результати сканування.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Захист інформації в комп'ютерних системах та мережах : навч. посібник / С. Г. Семенов [та ін.] ; Нац. техн. ун-т "Харків. політехн. ін-т". – Харків : НТУ "ХПІ", 2014. – 251 с.
2. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ-2000», 2020 . – 678 с.
3. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
4. Захист інформації в автоматизованих системах управління: навч. посібник / Уклад. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.
5. Інформаційна безпека України: теорія і практика : підручник / В.В. Лизанчук. – Львів : ЛНУ імені Івана Франка, 2017. – 728 с.
6. Криворучко О.В. Захист систем електронних комунікацій: навч.посіб./ В.О. Хорошко, О.В. Криворучко, М.М. Браіловський та ін. – Київ: Київ. нац. торг.-екон. ун-т, 2019. – 164 с..
7. Телекомунікаційні системи передавання інформації. Методи кодування [Текст] : навч. посібник / Р. А. Бурачок, М. М. Климаш, Б. В. Коваль. – Львів : Вид-во Львів. політехніки, 2015. – 476 с.
8. Інформаційна безпека : навчальний посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, С. С. Войтусік, А. Я. Горпенюк, О. А. Нємкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик ; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів : Видавництво Львівської політехніки, 2019. – 580 с.

Інформаційні ресурси

1. ДСТУ 3396.2–97. Захист інформації. Технічний захист інформації. Терміни та визначення. – К. : Укр. НДІССІ, 1997. – 11 с.

2. ДСТУ 4145–2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. – К. : Держстандарт України, 2002. – 40 с.
3. НД ТЗІ 1.1-003-99: Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999. ДСТСЗІ СБУ. – К., 1999. – 34 с.
4. НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999. ДСТСЗІ СБУ. – К., 1999. – 34 с.
5. НД ТЗІ 2.5-005-99: Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999. ДСТСЗІ СБУ. – К., 1999. – 34 с.
6. НД ТЗІ 3.7-001-99: Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999 р. ДСТСЗІ СБУ. – К., 1999. – 34 с.
7. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 18.04.2006, – К. : Урядовий кур'єр. – 2006. № 73 – 74.

Про інформацію : Закон України від 03.04.1997. – К. : Урядовий кур'єр. – 1997. – № 62

МОДУЛЬ 4. КІБЕРНЕТИЧНА БЕЗПЕКА ПІДПРИЄМСТВА

ТЕОРЕТИЧНИЙ БЛОК

1. Дайте визначення понять інформаційний простір і кібернетичний простір. Назвіть основних дійових осіб кіберпростору.
2. Що таке кібероборотьба? Які основні особливості їй притаманні?
3. Дайте визначення поняття кібернетична безпека. Назвіть істотні ознаки, які його характеризують.
4. Які документи регламентують діяльність із забезпечення інформаційної та кібернетичної безпеки в Україні? Наведіть приклади внеску в реалізацію цих процесів державних підрозділів спецпризначення.
5. За якими принципами мають розвиватися взаємовідносини між Україною та НАТО у сфері інформаційної та кібернетичної безпеки? Назвіть основні напрямки співробітництва Україна – НАТО у сфері кіберзахисту.
6. Що слід розуміти під поняттям інциденту у сфері високих технологій? Розкрийте сутність процесу управління інцидентами.
7. Опишіть модель системи управління інцидентами та розкрийте сутність її складових.
8. Дайте визначення внутрішнього і зовнішнього інциденту. Наведіть приклади таких інцидентів класифікації згідно з кодифікатором Інтерполу.
9. Які з відомих інцидентів становлять нині найбільшу небезпеку?
10. Назвіть найбільш критичні заходи захисту інформації від кіберзагроз.
11. Перелічіть основні кроки, які мають бути дотримані співробітниками служб безпеки в разі фіксації порушень інформаційної та кібернетичної безпеки.
12. За якими основними ознаками кібератаки можуть бути класифіковані?
13. Назвіть основні типи кібератак за класифікацією П. Ноймана.
14. Що таке сніфер пакетів? Які заходи сприятимуть зниженню загрози сніфінгу?
15. Що таке IP-спуфінг? Завдяки чому можна послабити загрозу IP-спуфінгу?

16. Що таке DoS та DDoS атаки? Назвіть найбільш відомі їх різновиди. За рахунок чого можна послабити загрози від DoS та DDoS атак?

17. Наведіть приклад алгоритму реалізації кібератак.

18. Назвіть основні риси кібертероризму. Що сприяє сучасним терористам у веденні їх протиправної діяльності та забезпечує їм успіх?

19. Назвіть головні прийоми, якими користуються сучасні кібертерористи у процесі своєї протиправної діяльності.

20. Дайте визначення понять «інформаційна зброя» та «кіберзброя». Чим зумовлюється перевага цих видів зброї над усіма іншими видами зброї?

21. Назвіть напрямки діяльності зі створення дієвої системи кібербезпеки.

22. Що відіграє роль базису для розробки моделей кібернападу і кіберзахисту? Наведіть приклади найбільш відомих таких моделей.

23. Які вимоги має задовольняти система інформаційного забезпечення кібернетичної безпеки? Перелічіть основні вимоги до програмно-апаратних комплексів кіберрозвідки.

24. Назвіть основні особистісно-професійні характеристики поведінки працівників і дій користувачів, що сприятимуть реалізації загроз інформаційної та кібернетичної безпеки.

25. Які тактики та інструменти може використовувати соціальний інженер для отримання доступу до IP-конкурента?

26. Що може впливати на розголошення в організації інформації з обмеженим доступом? Перелічіть фактори, які можуть впливати на лояльність працівників, а також на процес прийняття нових співробітників на роботу.

27. Якими механізмами користуються зловмисники, здійснюючи соціальний інжиніринг? Розкрийте сутність цих механізмів.

28. Перелічить основні заходи та засоби організаційного, програмного та технічного забезпечення захисту інформації.

29. За рахунок чого можна зменшити наслідки соціальної інженерії на рівні програмного забезпечення?

30. Наведіть узагальнену класифікацію методів соціальної інженерії. Розкрийте сутність методів соціальної інженерії, що спираються на взаємодії з політикою безпеки.

31. Назвіть категорії кібератак із використанням соціальної інженерії. Які проблеми дасть змогу розв’язати їх реалізація?

32. Опишіть алгоритм дій зловмисників методом соціальної інженерії. Наведіть приклади.

33. Що може вплинути на успіх у реалізації соціотехнічної атаки?

34. Якими інструментами користується соціальний інженер при організації та проведенні соціотехнічних атак?

35. Поясніть сутність використання електронної пошти як інструмента соціальної інженерії.

36. Назвіть спільні та відмінні риси фішингових і вішингових атак. У чому полягає механізм фармінгу? Наведіть приклади.

37. Які особистісні підходи використовують соціальні інженери для отримання інформації від працівників фірми-конкурента?

38. Назвіть головні переваги та недоліки реверсивної соціальної інженерії. Які чинники покладено в її основу?

39. Назвіть основні прийоми запобігання реалізації стандартної атаки вторгнення.

40. За якими ознаками здійснюється класифікація каналів несанкціонованого отримання інформації?

41. На скільки класів поділяються канали несанкціонованого отримання інформації? Назвіть їх.

42. Назвіть основні методи і заходи забезпечення безпеки інформації.

43. Що може призвести до порушення конфіденційності інформації?

44. Що може призвести до порушення цілісності інформації?
45. Що може призвести до порушення доступності інформації?
46. Опишіть загальну схему визначення показників уразливості інформації.
47. Назвіть головні способи вдосконалення засобів захисту інформації.
48. Що являє собою процедура тестування системи захисту на проникнення? У чому полягає її сутність? Як класифікують тести на проникнення?
49. Охарактеризуйте комплексний тест на проникнення. Дотримання яких технічних і соціоінженерних правил він вимагає?
50. На яких рівнях має проводитись тестування на проникнення? Розкрийте їх сутність.
51. Що є логічним продовженням тесту на проникнення? Які завдання покладаються на комплексну систему управління рівнем захищеності?
52. Яких заходів необхідно вживати в процесі моніторингу захищеності периметра корпоративної мережі?
53. З якою метою розробляється програма поінформованості? Які роботи мають бути виконані в процесі її реалізації?
54. Розкрийте особливості впровадження системи управління інформаційною безпекою.

ПРАКТИЧНИЙ БЛОК

1. Розглянути та проаналізувати інцидент інформаційної безпеки, з ціллю виявлення загроз ІБ та подальшого їх аналізу:

За повідомленнями світових інформаційних агентств, невідомі хакери зламали сервер Hotmail.com, після чого в будь-яку з 40 млн. віртуальних поштових скриньок, розташованих на цьому сервері, можна було проникнути без пароля – просто ввівши ім'я користувача. Протягом якого часу поштові адреси користувачів Hotmail.com були доступні будь-якому охочому, залишилося невідомим.

У понеділок вранці, компанія Microsoft (власниця Hotmail) на дві години відключила сервер і, за її заявою, повністю відновила систему безпеки Hotmail.

Незабаром після цього шведські ЗМІ повідомили, що відповідальність за здійснення атаки (а саме упровадження шкідливого коду) на сервер Hotmail, взяла на себе група хакерів під назвою Hackers Unite, до якої входить один швед і сім американців.

«Ми зробили це не для того, щоб щось зруйнувати, – заявив 21-річний шведський представник Hackers Unite. – Ми хотіли показати світові, наскільки погана система безпеки Microsoft».

На основі проведеного аналізу заповнити таблицю аналізу інцидентів ІБ та виявлених загроз (для кожного з розглянутих інцидентів ІБ).

Інцидент	Тип виявленої (реалізованої загрози	Джерело загрози та тип порушника	Спосіб реалізації загрози	Використані уразливості	Вид активів, які підлягають захисту	Наслідки порушення		
						К	Ц	Д

2. Розглянути та проаналізувати інцидент інформаційної безпеки, з ціллю виявлення загроз ІБ та подальшого їх аналізу:

В помсту за дуже маленьку премію 63-річний Рожер Дурон (колишній системний адміністратор компанії UBS Paine Webber) встановив на серверах компанії «логічну бомбу», яка знищила всі дані і паралізувала роботу компанії на тривалий час.

Впровадження «логічної бомби» Дурон здійснив з домашнього комп'ютера за кілька місяців до того, як отримав дуже маленьку, на його погляд, премію. «Логічна бомба» була

встановлена приблизно на 1500 комп'ютерів в мережі філій по всій країні і налаштована на певний час – 9.30, якраз на початок банківського дня.

Звільнився Дурон з UBS Paine Webber 22 лютого 2002 року, а четвертого березня 2002 «логічна бомба» послідовно видалила всі файли на головному сервері центральної бази даних і 2000 серверів в 400 філіях банку, при цьому відключивши систему резервного копіювання.

На основі проведеного аналізу заповнити таблицю аналізу інцидентів ІБ та виявлених загроз (для кожного з розглянутих інцидентів ІБ).

Інцидент	Тип виявленої (реалізованої загрози	Джерело загрози та тип порушника	Спосіб реалізації загрози	Використані уразливості	Вид активів, які підлягають захисту	Наслідки порушення		
						К	Ц	Д

3. Розглянути та проаналізувати інцидент інформаційної безпеки, з ціллю виявлення загроз ІБ та подальшого їх аналізу:

Наприкінці 1999 року були виведені з ладу веб-сервери таких корпорацій, як Amazon, Yahoo, CNN, eBay, E-Trade і ряду інших, трохи менш відомих. Через рік, у грудні 2000-го «різдвяний сюрприз» повторився: сервери найбільших корпорацій були атаковані за технологією DDoS при повному безсиллі мережевих адміністраторів. З тих пір повідомлення про DDoS-атаки вже не є сенсацією. Головною небезпекою тут є простота організації і те, що ресурси хакерів є практично необмеженими, так як атака є розподіленою.

На основі проведеного аналізу заповнити таблицю аналізу інцидентів ІБ та виявлених загроз (для кожного з розглянутих інцидентів ІБ).

Інцидент	Тип виявленої (реалізованої загрози	Джерело загрози та тип порушника	Спосіб реалізації загрози	Використані уразливості	Вид активів, які підлягають захисту	Наслідки порушення		
						К	Ц	Д

4. Розглянути та проаналізувати інцидент інформаційної безпеки, з ціллю виявлення загроз ІБ та подальшого їх аналізу:

Японська фірма Dai Nippon Printing, що спеціалізується на випуску поліграфічної продукції, допустила найбільший витік інформації в історії своєї країни. Хирофумі Йокояма, колишній співробітник одного з підрядників компанії, скопіював на мобільний вінчестер і вкрав персональні дані клієнтів фірми. В цілому під загрозу потрапили 8,64 млн. чоловік, так як викрадена інформація містила імена, адреси, телефони і номери кредитних карт. У викраденій інформації містилися відомості про клієнтів 43 різних компаній, наприклад про 1 504 857 клієнтів компанії American Home Assurance, 581 293 клієнтів компанії Aeon Co та 439 222 клієнтів NTT Finance.

На основі проведеного аналізу заповнити таблицю аналізу інцидентів ІБ та виявлених загроз (для кожного з розглянутих інцидентів ІБ).

Інцидент	Тип виявленої	Джерело загрози та	Спосіб реалізації	Використані	Вид	Наслідки порушення

	(реалізованої загрози	тип порушника	загрози	уразливості	активів, які підлягають захисту	К	Ц	Д

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Закон України «Про захист персональних даних».
2. Законі України «Про інформацію».
3. Закону України «Про основні засади забезпечення кібербезпеки України».
4. Кодекс України «Про адміністративні правопорушення».
5. Кримінальний кодекс України.
6. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: посібник / В. Л. Бурячок, С. В. Толюпа, В. В. Семко, Л. В. Бурячок, П. М. Складанний, Н. В. Лукова-Чуйко. – Київ: ДУТ – КНУ, 2016. – 178 с.
7. Бурячок, В. Л. Основи формування державної системи кібернетичної безпеки: монографія/ В. Л. Бурячок.— К.: НАУ, 2013.— 432 с.
8. Гнатюк, С. О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / С. О. Гнатюк// Безпека інформації.— 2013.— Т. 19, № 2.— С. 118–129.
9. Корченко, О. Г. Кібернетична безпека держави: характерні ознаки та проблемні аспекти

/ О. Г. Корченко, В. Л. Бурячок, С. О. Гнатюк // Безпека інформації.— 2013.— Т. 19, № 1.— С. 40–45.

10. Мельник, С. В. До проблеми формування понятійно-термінологічного апарату кібербезпеки / С. В. Мельник, О. О. Тихомиров, О. С. Лєнков // Зб. наук. праць Військового ін-ту КНУ ім. Тараса Шевченка.— К.: ВІКНУ, 2011.— Вип. 30.— С. 159–165.
11. Словник термінів із кібербезпеки / За заг. ред. О. В. Копана, Є. Д. Скулиша — К.: ВБ «Аванпост-Прим», 2012.— 214 с.
12. Бурячок, В. Л. Кібернетична безпека — головний фактор сталого розвитку сучасного інформаційного суспільства // Сучасна спец. техніка.— 2011.— № 3.— С. 104–114.
13. Бурячок В. Л. Модель формування дерева атак для одержання інформації в інформаційно-телекомунікаційних системах і мережах при вилученому доступі / В. Л. Бурячок // Науковий журнал «Інформатика та математичні методи в моделюванні» Одеського національного політехнічного університету. – № 2, 2013, с. 123 – 131
14. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В.. Інформаційна та кібербезпека: соціотехнічний аспект Підручник / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. — Київ: ДУТ, 2015. — 288 с.
15. Гулак Г. М. Основи криптографічного захисту інформації: підручник / Г. М. Гулак, В. А. Мухачов, В. О. Хорошко, Ю. Є. Яремчук. – Вінниця: ВНТУ, 2011. – 199 с.
16. Кавун С. В. Інформаційна безпека. Навчальний посібник. Ч. 2 / С. В. Кавун, В. В. Носов, О. В. Манжай. – Харків: ХНЕУ, 2008. – 196 с
17. Остапов С. Е. Технології захисту інформації: навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Харків: ХНЕУ, 2013. – 476 с.
18. Силаенков А. Н. Проектирование системы информационной безопасности: учебное пособие / А. Н. Силаенков – Омск: Изд-во ОмГТУ, 2009. – 128 с.

19. Сухов А. М. Механизмы безопасности в Linux: Методические указания к лабораторной работе / А. М. Сухов. – Самара: СГАУ, 2010. – 24 с.
20. Сычев Ю. Н. Основы информационной безопасности: учебно-практическое пособие / Ю. Н. Сычев – Москва: Изд. центр ЕАОИ, 2007. – 300 с
21. Хамухин А. А. Практикум по информационной безопасности: учебное пособие / А. А. Хамухин, А. А. Захарова – Томск: ТПУ, 2011. – 196 с.
22. Цирлов В. Л. Основы информационно безопасности автоматизированных систем. Краткий курс / В. Л. Цирлов. – Ростов-на-Дону: Феникс, 2008. – 253 с.

СТРУКТУРА ЕКЗАМЕНАЦІЙНОГО БІЛЕТА

Екзаменаційний білет державного іспиту для студентів-випускників напряму 125 «Кібербезпека» складається з трьох блоків, які містять завдання теоретичних курсів спеціальних дисциплін:

- Теорія ймовірностей та математична статистика;
- Організація баз даних та знань;
- Захист інформації в комп'ютерних системах та мережах;
- Кібернетична безпека підприємства.

Перший блок містить 5 тестових завдань. Кожне тестове завдання містить питання та 5 відповідей з котрих потрібно обрати вірні відповіді (одну чи декілька).

Другий блок містить 3 теоретичних питання, на які потрібно надати розгорнуту відповідь. Якщо потрібно, навести схематичні представлення, математичні докази або логічні обґрунтування і формули.

Третій блок містить 3 практичних завдання або задачі, вирішення яких потрібно навести. Усі формули, логічні розв'язання або схематичні представлення наводяться обов'язково.

КРІТЕРІЇ ОЦІНЮВАННЯ

Перший блок містить 5 тестових питань. Кожен с 5-ти тестових питань оцінюється за 5 бальною шкалою, у разі надання вірних варіантів відповідей. Якщо відповіді надані у неповному обсязі, завдання оцінюється у 2,5 бали. Якщо відповідь невірна, то за відповідь надається 0 балів. Максимальна кількість балів, яку можливо отримати за перший блок – 25 балів.

Другий рівень містить 3 теоретичних питання. Кожен з 3-х теоретичних питань оцінюється за 10-бальною шкалою залежно від рівня знань. Максимальна кількість балів, яку можливо отримати за цей блок – 30 балів. Критерії оцінювання відповіді на теоретичне питання наведено у таблиці:

Оцінка відповіді за 10-бальної шкалою	**Критерії оцінювання відповіді**
9-10 балів	Відповідь студента: - містить повний, розгорнутий, правильний виклад матеріалу з поставленого питання; - демонструє знання основних понять і категорій та взаємозв'язку між ними, вірне розуміння змісту основних

	теоретичних положень; - вказує на вміння давати змістовний та логічний аналіз матеріалу з поставленого питання; - демонструє знання різних наукових концепцій та підходів щодо певної науково-теоретичної чи науково-практичної проблеми, пов'язаної з поставленим питанням; - здатність робити власні висновки в разі неоднозначності, спірного чи проблемного характеру поставленого питання чи проблеми.
5-8 балів	Студент дав досить змістовну відповідь на поставлене питання, але відповідь містить наступні недоліки: - недостатня повнота, незначні неточності чи прогалини при поясненні того чи іншого аспекту питання; - недостатньо детально розкритий предмет запитання, а основні поняття носять тезисний характер; - окремі формулювання є нечіткими; міститься інформація, котра не відноситься до змісту екзаменаційного питання; - відповідь на ситуаційне завдання є недостатньо аргументованою.
1-4 балів	Студент дав відповідь на поставлене питання, однак допустив суттєві помилки як змістовного характеру, так і при оформлені відповіді на питання, а саме: - зміст відповіді свідчить про прогалини у знаннях з відповідного питання або ж про невірне розуміння окремих аспектів поставленого питання; - відповідь викладена недостатньо аргументовано та/або з порушенням правил логіки при поданні матеріалу; - відповідь не містить аналізу проблемних аспектів поставленого питання, свідчить про недостатню обізнаність з основними науковими теоріями і концепціями, що стосуються відповідного питання; - обґрунтування відповіді до ситуаційного завдання є слабко аргументованим і/або в окремих аспектах алогічним.
0 балів	Студент взагалі не відповів на питання, або його відповідь є неправильною, тобто містить грубі змістовні помилки щодо принципових аспектів поставленого питання. Аргументація відсутня взагалі або ж є абсолютно безсистемною чи алогічною. Відповідь на ситуативне завдання є необґрунтованою та алогічною.

Третій рівень містить 3 практичних завдання (або задачі). Кожне з 3-х практичних завдань оцінюється за 15-бальною шкалою залежно від рівня знань. Максимальна кількість балів, яку можливо отримати за цей блок – 45 балів. Критерії оцінювання відповіді на розв'язання практичного завдання або задачі наведено у таблиці:

Оцінка відповіді за 15-бальної шкалою	**Критерії оцінювання відповіді**
15-13 балів	Відповідь студента:

	- містить повний, розгорнутий, правильний виклад матеріалу з поставленого питання; - вказує на вміння давати змістовний та логічний аналіз матеріалу з поставленого питання; - містить послідовний та аргументований розв'язок задачі (практичного завдання); вірно зроблені розрахунки до задачі; - демонструє знання різних наукових концепцій та підходів щодо певної науково-теоретичної чи науково-практичної проблеми, пов'язаної з поставленим питанням; - здатність робити власні висновки в разі неоднозначності, спірного чи проблемного характеру поставленого питання чи проблеми.
7-12 балів	Студент дав досить змістовну відповідь на поставлене питання, але відповідь містить наступні недоліки: - недостатня повнота, незначні неточності чи прогалини при поясненні того чи іншого аспекту питання; - окремі формулювання є нечіткими; міститься інформація, котра не відноситься до змісту екзаменаційного питання; - відповідь на ситуаційне завдання є недостатньо аргументованою; - алгоритм розв'язку задачі є вірним, однак допущені помилки при розрахунках.
1-6 балів	Студент дав відповідь на поставлене питання, однак допустив суттєві помилки як змістовного характеру, так і при оформлені відповіді на питання, а саме: - зміст відповіді свідчить про прогалини у знаннях з відповідного питання або ж про невірне розуміння окремих аспектів поставленого питання; - відповідь викладена недостатньо аргументовано та/або з порушенням правил логіки при поданні матеріалу; - відповідь не містить аналізу проблемних аспектів поставленого питання, свідчить про недостатню обізнаність з основними науковими теоріями і концепціями, що стосуються відповідного питання; - порушено алгоритм розв'язку задачі і/або присутні помилки при розрахунках, відсутні висновки; - обґрунтування відповіді до ситуаційного завдання є слабко аргументованим і/або в окремих аспектах алогічним.
0 балів	Студент взагалі не відповів на питання, або його відповідь є неправильною, тобто містить грубі змістовні помилки щодо принципових аспектів поставленого питання. Аргументація відсутня взагалі або ж є абсолютно безсистемною чи алогічною. Задача розв'язана невірно. Відповідь на ситуативне завдання є необґрунтованою та алогічною.

ФАХОВІ КОМПЕТЕНТНОСТІ

Під час навчання за напрямом 125 «Кібербезпека» здобувачі вищої освіти набувають наступні фахові компетентності:

КФ 1. Здатність використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності.

КФ 2. Здатність до використання інформаційних і комунікаційних технологій з метою пошуку нової інформації, створення баз даних, аналізу розподілених АС, каналів зв'язку, систем управління процесами, баз даних, оперативного планування роботи систем на основі аналізу інформаційних потоків та їх оптимізації.

КФ 3. Здатність здійснювати проектування (розробку) систем, технологій і засобів інформаційної безпеки

КФ 4. Здатність здійснювати протидію несанкціонованому проникненню в ІТ системи і мережі.

КФ 5. Здатність прогнозувати, виявляти та оцінювати стан інформаційної безпеки об'єктів і систем.

КФ 6. Здатність відновлювати нормальне функціонування ІТ систем і мереж після здійснення кібернападів, збоїв та відмов.

КФ 7. Здатність виконувати спеціальні дослідження технічних і програмно-апаратних засобів захисту обробки інформації в ІТС.

КФ 8. Здатність проводити техніко-економічний аналіз й обґрунтовувати проектні рішення з забезпечення кібербезпеки.

КФ 9. Здатність формувати комплекс заходів (правил, процедур, практичних прийомів та ін.) для управління інформаційною безпекою.

КФ 10. Здатність здійснювати управління інцидентами інформаційної та кібербезпеки.

КФ 11. Здатність здійснювати управління ризиками інформаційної та кібербезпеки.

КФ 12. Здатність виконувати моніторинг даних, комп’ютерних зловживань та аномалій.

КФ 13. Здатність прогнозувати, виявляти та оцінювати можливі загрози інформаційному простору держави та дестабілізуючі чинники.

КФ 14. Здатність проводити дослідження у практичній професійній діяльності.