

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

Навчально-науковий інститут автоматики та електротехніки
Кафедра комп'ютерних технологій та інформаційної безпеки

Код за ОПП

ОК6

«ЗАТВЕРДЖУЮ»

Проректор з науково-педагогічної
роботи, к.т.н., доцент



С.О. Слободян

» _____ 2025 р.

ПРОГРАМА

кваліфікаційного екзамену

для здобуття ступеня вищої освіти магістр

Галузь знань F Інформаційні технології

Спеціальність F5 Кібербезпека та захист інформації

Освітньо-професійна програма Системи технічного захисту інформації,
автоматизація її обробки

Програма кваліфікаційного екзамену, для здобуття ступеня вищої освіти магістр, є однією зі складових комплексної підготовки фахівців галузі знань F «Інформаційні технології» спеціальності F5 «Кібербезпека та захист інформації» за освітньо-професійною програмою «Системи технічного захисту інформації, автоматизація її обробки». «24» 04 2025 р.

Розробники:

Нужний С.М., завідувач кафедри Комп'ютерних технологій та інформаційної безпеки, канд. техн. наук, доцент;

Передерій В.І., професор кафедри Комп'ютерних технологій та інформаційної безпеки, док. техн. наук, доцент;

Турти М.В., доцент кафедри Комп'ютерних технологій та інформаційної безпеки, канд. техн. наук, доцент;

Сірівчук А.С., доцент кафедри Комп'ютерних технологій та інформаційної безпеки, канд. техн. наук, доцент.

Проект Програми кваліфікаційного екзамену, для здобуття ступеня вищої освіти магістр, узгоджено з гарантом освітньої програми

Гарант освітньої програми «Системи технічного захисту інформації, автоматизація її обробки»

Передерій В.І., професор кафедри Комп'ютерних технологій та інформаційної безпеки, док. техн. наук, доцент 

Проект Програми кваліфікаційного екзамену, для здобуття ступеня вищої освіти магістр, розглянуто на засіданні кафедри КТІБ.

Протокол від «24» 04 2025 р. № 12.

Завідувач кафедри КТІБ, к.т.н., доцент  С.М. Нужний

Проект Програми кваліфікаційного екзамену, для здобуття ступеня вищої освіти магістр, розглянуто методичною радою Навчально-наукового інституту автоматики і електротехніки.

Протокол від «15» 05 2025 р. № 5.

Заступник голови МР ННІАЕ, к.т.н., доц.  С.М. Новогрецький

Проект Програми кваліфікаційного екзамену, для здобуття ступеня вищої освіти магістр, погоджено з навчальним відділом.

Начальник навчального відділу, к.т.н., доцент  А.В. Лабарткава

Програму кваліфікаційного екзамену, для здобуття ступеня вищої освіти магістр, затверджено Навчально-методичною радою НУК ім. адм. Макарова.

Протокол від «21» 05 2025 р. № 5.

Голова Навчально-методичної ради НУК ім. адм. Макарова, к.т.н., доцент  С.О. Слободян

ЗМІСТ

1. Загальні положення	4
2. Організація та порядок проведення кваліфікаційного іспиту	6
3. Зміст кожного розділу програми.....	7
3.1. Розділ I.....	7
3.1.1. Проектування комплексних систем захисту інформації	7
3.1.2. Радіомоніторинг та радіопротидія на об'єктах інформаційної діяльності....	15
3.2. Розділ II.....	26
3.2.1. Інформаційно-комунікаційні системи водного транспорту	26
3.2.2. Теорія захисту інформаційних ресурсів обмеженого доступу	32
3.3. Розділ III.....	41
3.3.1. Моделювання та оптимізація об'єктів і процесів захисту інформації	41
4. Література.....	52
5. Критерії та норми оцінювання.....	58
6. Додаток А.....	59

1. Загальні положення

Фахове випробування (державний екзамен) спрямоване на комплексну перевірку умінь та навичок студентів, що навчаються за спеціальністю F5 «Кібербезпека та захист інформації» освітньо-професійної програми «Системи технічного захисту інформації, автоматизація її обробки» з метою оцінки їх відповідності вимогам освітньо-професійної програми.

Головним завданням іспиту є перевірка якості професійної підготовки, виявлення відповідності підготовки випускника до вимог освітньо-професійної програми.

Метою іспиту є оцінювання рівня засвоєних здобувачем вищої освіти спеціальних (фахових, предметних) компетентностей, визначених стандартами вищої освіти та достатніх для ефективного виконання професійної діяльності за обраною спеціальністю.

Обсяг знань та умінь здобувачів освіти визначається вимогами Стандарту спеціальності F5 «Кібербезпека та захист інформації» та освітньо-професійною програмою за якими велась підготовка майбутніх фахівців. Програма та порядок проведення державного іспиту визначається «Положенням про організацію освітнього процесу в Національному університеті кораблебудування ім. адм. Макарова».

Проходження іспиту повинно забезпечити набуття студентами наступних **компетентностей:**

Інтегральна компетентність:

- Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

Загальні компетентності

- (ЗК3) Здатність до абстрактного мислення, аналізу та синтезу.

Фахові компетентності:

- (ФК2) Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки;
- (ФК3) Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури;
- (ФК4) Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог;
- (ФК7) Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому;

- (ФК8) Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації;
- (ФК11) Здатність виявляти закладні пристрої на об'єктах інформаційної діяльності (як члени команди);
- (ФК12) Здатність виконувати передпроектні роботи щодо систем та комплексів захисту інформації;
- (ФК13) Здатність проводити спеціалізовані дослідження засобів обробки інформації, технічних засобів та об'єктів інформаційної діяльності;
- (ФК14) Здатність впроваджувати(активізувати) програмні та апаратні засоби захисту інформації в системах і на об'єктах;
- (ФК17) Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимог технічного та організаційного спрямування щодо системи технічного криптографічного захисту інформації.

2. Організація та порядок проведення кваліфікаційного іспиту

Екзамен проводиться приймальною комісією письмово у формі тестування. До складу екзаменаційного білету входить 50 завдань з трьох дисциплін (п'ять модулів):

- «Технології створення та застосування комплексів захисту інформації з обмеженим доступом. Модуль 1. Проектування комплексних систем захисту інформації (10 завдань);
- «Технології створення та застосування комплексів захисту інформації з обмеженим доступом. Модуль 2. «Радіомоніторинг та радіопротидія на об'єктах інформаційної діяльності» (10 завдань);
- «Інформаційна та кібербезпека спеціалізованих інформаційно-комунікаційних систем на водному транспорті. Модуль 1. Інформаційно-комунікаційні системи водного транспорту» (10 завдань);
- «Інформаційна та кібербезпека спеціалізованих інформаційно-комунікаційних систем на водному транспорті. Модуль 2. «Теорія захисту інформаційних ресурсів обмеженого доступу» (10 завдань);
- «Моделювання та оптимізація об'єктів і процесів захисту інформації» (10 завдань).

Тривалість проведення фахового вступного випробування 120 хвилин. Виконання всіх екзаменаційних завдань кваліфікаційного іспиту є обов'язковим. Оцінки (бали) виставляються шляхом перевірки відповідей на тестові питання (загальна кількість питань - 50, рівень таксономії 1 до 5, кількість балів за вірну відповідь - 2). Підсумкову оцінку кваліфікаційного іспиту завіряють всі члени комісії.

Критерії оцінювання фахового вступного випробування відповідають «Положенням про організацію навчального процесу в Національному університеті кораблебудування імені адмірала Макарова».

3. Зміст кожного розділу

3.1. Розділ 1

Розділ перший кваліфікаційного екзамену, на здобуття ступеня вищої освіти магістр складається з завдань першого і другого модулів дисципліни «Технології створення та застосування комплексів захисту інформації з обмеженим доступом».

Метою вивчення навчальної дисципліни «Технології створення та застосування комплексів захисту інформації з обмеженим доступом» є ознайомлення студентів із основами побудови, проектування, впровадження і супроводження роботи КСЗІ на ОІД критичної інфраструктури. В процесі навчання передбачається вивчення нормативних документів та технологій проведення робіт з використанням спеціальних технічних засобів, в тому числі й в умовах забезпечення режиму секретності, на підприємствах, установах, організаціях з різними формами власності, по визначенню рівня захищеності ІзОД.

3.1.1. Модуль 1. «Проектування комплексних систем захисту інформації»

Здобувачі, які проходять випробування, повинні володіти знаннями та навичками розв'язання завдань за наступними темами:

Запитання 1	Таємна інформація це (згідно з ДСТУ 3396.2-97)
A	Інформація з обмеженим доступом, яка містить відомості, що становлять державну або іншу передбачену законом таємницю
B	Інформація з обмеженим доступом, якою володіють, користуються чи розпоряджаються окремі фізичні чи юридичні особи або держава і порядок доступу до якої встановлюється ними
C	Інформація, право доступу до якої обмежено встановленими правовими нормами і (чи) правилами
D	Інформація з обмеженим доступом, яка містить відомості, що становлять комерційну таємницю

Запитання 2	Конфіденційна інформація (згідно з ДСТУ 3396.2-97)
A	Інформація з обмеженим доступом, якою володіють, користуються чи розпоряджаються окремі фізичні чи юридичні особи або держава і порядок доступу до якої встановлюється ними
B	Інформація, право доступу до якої обмежено встановленими правовими нормами і (чи) правилами
C	Інформація з обмеженим доступом, яка містить відомості, що становлять державну або іншу передбачену законом таємницю
D	Інформація з обмеженим доступом, яка містить відомості, що становлять комерційну таємницю

Запитання 3	Інформація з обмеженим доступом (згідно з ДСТУ 3396.2-97)
A	Інформація, право доступу до якої обмежено встановленими правовими нормами і (чи) правилами
B	Інформація з обмеженим доступом, яка містить відомості, що становлять державну або іншу передбачену законом таємницю
C	Інформація з обмеженим доступом, якою володіють, користуються чи розпоряджаються окремі фізичні чи юридичні особи або держава і порядок доступу до якої встановлюється ними
D	Інформація з обмеженим доступом, яка містить відомості, що становлять комерційну таємницю

Запитання 4	Модель загроз для інформації (згідно з ДСТУ 3396.2-97)
A	Формалізований опис методів та засобів здійснення загроз для інформації
B	Формалізований опис методів, засобів та можливостей технічної розвідки
C	Сукупність носія інформації, середовища його поширення та засобу технічної розвідки
D	Сукупність вимог (в тому числі і тих, що нормуються), які визначається режимом доступу до інформації та загрозами для неї

Запитання 5	Модель технічної розвідки (згідно з ДСТУ 3396.2-97)
A	Формалізований опис методів, засобів та можливостей технічної розвідки
B	Формалізований опис методів та засобів здійснення загроз для інформації
C	Сукупність носія інформації, середовища його поширення та засобу технічної розвідки
D	Сукупність вимог (в тому числі і тих, що нормуються), які визначається режимом доступу до інформації та загрозами для неї

Запитання 6	Носій інформації (ТЗІ) (згідно з ДСТУ 3396.2-97)
A	Матеріальний об'єкт, що містить інформацію з обмеженим доступом
B	Фізичне поле та(чи) хімічна речовина, що містять інформацію з обмеженим доступом
C	Електромагнітне випромінювання та навід, що є побічним результатом функціонування технічного засобу
D	Документи, що містять інформацію з обмеженим доступом

Запитання 7	Технічний захист інформації; ТЗІ
A	Діяльність, спрямована на запобігання порушенню цілісності, блокуванню та (чи) витоку інформації технічними каналами
B	Пристрій та (чи) програмний засіб, основне призначення яких - захист інформації від загроз
C	Спосіб технічного захисту інформації, який полягає в унеможливленні або суттєвому утрудненні несанкціонованого одержання інформації
D	Приховування інформації ослабленням енергетичних характеристик фізичних полів або зниженням концентрації речовин
E	Правильна відповідь відсутня

Запитання 8	Засіб технічного захисту інформації
A	Пристрій та (чи) програмний засіб, основне призначення яких - захист інформації від загроз
B	Діяльність, спрямована на запобігання порушенню цілісності, блокуванню та (чи) витоку інформації технічними каналами
C	Спосіб технічного захисту інформації, який полягає в унеможливленні або суттєвому утрудненні несанкціонованого одержання інформації
D	Приховування інформації ослабленням енергетичних характеристик фізичних полів або зниженням концентрації речовин
E	Правильна відповідь відсутня

Запитання 9	Маніпуляція сигналу це
A	Дискретна зміна параметрів вихідного сигналу відповідно до значення первинного (вхідного) сигналу
B	Несанкціонований вплив на первинний (вхідний) сигнал, наприклад цифрову фонограму, з метою внесення змін
C	Синтез цифрової фонограми на основі базових фрагментів мови шляхом різних алгоритмічних маніпуляцій звуковому сигналу для надання необхідної форми
D	Корегування цифрових даних на носії з метою їх дискредитації (порушення цілісності інформації)
E	Правильна відповідь відсутня

Запитання 10	Маскування ознак об'єкту це:
A	Перетворення ознак об'єкту під ознаки інших об'єктів, що є не цікавими для зловмисників
B	Трансформування вихідного інформаційного портрета в новий, який відповідає помилковій ознаці речовини – тобто створення фальшивого об'єкту
C	Заміна реквізитів інформаційного портрета об'єкту, що захищається, на інформаційний портрет другого «відкритого» об'єкту (в тому випадку, коли інформаційний портрет об'єкта захисту схожий і не має специфічних інформаційних ознак)
D	Підтримання версії з ознаками, запозичення з різних інформаційних портретів реальних об'єктів
E	Правильна відповідь відсутня

Запитання 11	Підвищення ймовірності правильного виявлення зловмисника і пожежі та зменшення ймовірності помилкової тривоги не досягається:
A	Спільним застосуванням декількох однотипних сповіщувачів, що виявляють однакові ознаки джерел загроз
B	Вдосконаленням технічних рішень, які застосовані в сповіщувачах
C	Установкою сповіщувачів у місцях контрольованої зони з мінімальним рівнем перешкод
D	Спільним застосуванням декількох сповіщувачів, що виявляють різні ознаки джерел загроз

Запитання 12	Який тип перешкод створює шумове засвічення екрану локатора?
A	Гармонійне коливання на частоті РЛС, створюване генератором перешкод у місці знаходження об'єкта, що захищається
B	Покриття об'єкта екранами, що змінюють напрямку поширення відбитого електромагнітного поля
C	Використання противником димової завіси
D	Шумове засвічення екрану локатора є проявом його несправності

Запитання 13	Високочастотне ущільнення мовного сигналів в телекомунікаційному каналі є
A	Подальшим розвитком частотних маскувальників мови (частотних скремблерів)
B	Методом частотної модуляції
C	Подальшим розвитком методу частотного кодування
D	Методом передачі сигналів по багатомодовій оптичній лінії зв'язку
E	Правильна відповідь відсутня

Запитання 14	Який з вказаних нижче засобів не може використовуватися в складі АС-1 класу
A	Маршрутизатори Cisco
B	Персональний комп'ютер із захистом інформації «EXPERT»
C	Пристрій захисту телефонних та радіотрансляційних ліній «Топаз-1»
D	Система захисту інформації ЛОЗА-1
E	Правильна відповідь відсутня

Запитання 15	Комплекс засобів захисту інформації від НСД системи захисту інформації «ЛОЗА-2» призначений для
A	Захист від НСД до інформаційних ресурсів в автоматизованих системах класу «2».
B	Забезпечення захисту мовної інформації з обмеженим доступом від витоку каналами цифрових абонентських телефонних ліній
C	Централізований захист операційних систем робочих станцій та серверів від шкідливого програмного забезпечення (вірусів, троянів, шпигунських програм) в масштабах підприємства
D	Програмно-апаратний засіб, основною функцією якого є маршрутизація кадрів у мережах, побудованих за технологією Ethernet, забезпечує захист інформації від НСД.
E	Правильна відповідь відсутня

Запитання 16	Автоматизовані комплекси «Акор» не можуть бути застосовані для:
A	Контролю інформаційних потоків для виявлення і запобігання випадкам несанкціонованого використання конфіденційних даних
B	Перевірки і контролю приміщень, електромережі, телефонних та інших дротових ліній на наявність пристроїв нелегального зняття мовної інформації, відеокамер-передавачів та інфрачервоних передавачів
C	Виконання функцій пошукового комплексу
D	Виконання функцій вимірювального комплексу
E	Правильна відповідь відсутня

Запитання 17	Біометрична система контролю доступу призначена для:
A	Ідентифікації та/або автентифікації суб'єкта по його біометричним характеристикам
B	Ідентифікації суб'єкта по документу, наприклад паспорту, з вбудованим спеціальним мікропроцесорним чипом, в якому міститься інформація про власника
C	Автентифікації суб'єкта по документу, наприклад паспорту, з вбудованим спеціальним мікропроцесорним чипом, в якому міститься інформація про власника
D	Ідентифікації та/або автентифікації суб'єкта по документу, наприклад паспорту, з вбудованим спеціальним мікропроцесорним чипом, в якому міститься інформація про власника

Запитання 18	Дальність дії RFIT мітки залежить від
A	Діапазону робочої частоти
B	Кількості міток в районі зчитувача
C	Наявності «прямого бачення» мітки зчитувачем
D	Швидкості руху мітки

Запитання 19	Компрометуюче випромінювання (Compromising emanation), це
A	Канал витоку інформації за рахунок побічних електромагнітних полів та наведень
B	Термін, що вказує на наявність в контрольованій зоні радіозакладних пристроїв (жучків)
C	Радіаційне поле навколо об'єкту, де зберігається та/або застосовується в технологічному процесі радіоактивний матеріал (наприклад, радіаційне випромінювання реакторів підводних човнів)
D	Свічення спеціальних красок в ультрафіолетовому світлі (наприклад, при фіксуванні хабаря)

Запитання 20	Високочастотне «накачування» використовується для
A	Збудження напівпровідникових каскадів радіоелектронної апаратури або спеціально розроблених резонансних контурів для створення каналу витоку інформації
B	Збільшення потужності радіопередавача
C	Створення лазерного випромінювання
D	Створення об'ємного електромагнітного зашумлення
E	Створення перешкод роботі радіолокаційним станціям

Запитання 21	Локатори нелінійних викривлень використовуються для
A	Пошук технічних засобів розвідки, які не санкціоновано встановлені в контрольованій зоні, за рахунок виявлення напівпровідникових елементів (p-n переходів)
B	Визначення координат апаратури для несанкціонованої передачі інформації по радіоелектронному каналу
C	Виявлення апаратури радіоелектронної боротьби зловмисника
D	Збільшення потужності радіопередавача

Запитання 22	Яким повинно бути співвідношення рівнів сигналів другої та третьої гармоніки в локаторі нелінійних викривлень при виявленні «природних» напівпровідників
A	Рівні сигналів однакові
B	Рівень другої гармоніки на 20 дБ та більше за рівень третьої гармоніки
C	Рівень третьої гармоніки на 20 дБ та більше за рівень другої гармоніки
D	Наявність значних коливань (змінної складової) в рівні третьої гармоніки

Запитання 23	Яким повинно бути співвідношення рівнів сигналів другої та третьої гармонік в локаторі нелінійних викривлень при виявленні «природних» напівпровідників
A	Рівні сигналів однакові
B	Рівень другої гармоніки на 20 дБ та більше за рівень третьої гармоніки
C	Рівень третьої гармоніки на 20 дБ та більше за рівень другої гармоніки
D	Наявність значних коливань (змінної складової) в рівні третьої гармоніки

Запитання 24	Як називаються лінії, що з'єднують на графіку точки, які характеризують собою чисті тони рівної гучності, але різної частоти
A	Ізобари
B	Ізотерми
C	Криві рівної гучності
D	Лінії чутливості акустичного приладу
E	Правильна відповідь відсутня

Запитання 25	Акустичним еталоном, близьким до абсолютного порогу слухового сприйняття, є рівень тиску
A	2 мПа
B	20 мкПа
C	10 мкПа
D	1 мкПа
E	Правильна відповідь відсутня

Запитання 26	Інтенсивність акустичний сигнал, яка створюється динаміком з рівнем тиску 2 мПа, і виміряна на відстані 1 м від джерела становить
A	20 дБ
B	40 дБ
C	60 дБ
D	80 дБ
E	Правильна відповідь відсутня

Запитання 27	Якщо інтенсивність акустичного сигналу в точці вимірювання становить 80 дБ, то на якій відстані рівень інтенсивності знизиться до 40 дБ
A	10 м
B	50 м
C	100 м
D	200 м

Запитання 28	Чому дорівнює інтенсивність акустичного сигналу в точці встановлення направленої мікрофона, якщо джерело сигналу з інтенсивністю 80 дБ знаходиться на відстані 1000 м
A	10 дБ
B	20 дБ
C	30 дБ
D	40 дБ

Запитання 29	Який рівень звукоізоляції необхідно забезпечити на границі контрольованої зони, якщо інтенсивність джерела акустичного сигналу в контрольованій зоні становить 80 дБ, а виміряний на відстані 100 м сигнал має інтенсивність 20 дБ
A	10 дБ
B	20 дБ
C	30 дБ
D	40 дБ

Запитання 30	Еталоном (пороговим) значення віброприскорення ϵ (мм/с ²)
A	3×10^{-4}
B	1×10^{-4}
C	3×10^{-6}
D	1×10^{-6}

Запитання 31	Металошукачі імпульсного типу визначають матеріалу прихованого предмета за рахунок:
A	Аналізу амплітуди та часу спадання рівня вторинного електромагнітного поля, яке збуджується вихровим струмом
B	Порівняння рівнів другої та третьої гармонік
C	Порівняння частоти вимірювального LC-генератора
D	Порівняння добротності вимірювального LC-генератора

Запитання 32	Детектори поля використовуються для:
A	Виявлення джерел радіосигналів, незалежно від їх типу - як аналогових, так і цифрових
B	Виявлення джерел акустичних полів та аномалій, в незалежності від частоти їх коливань
C	Виявлення побічного випромінювання електронного обладнання
D	Виявлення вторинних полів вихрових струмів середніх та високих частот

Запитання 33	Направлений мікрофон лінзового типу це:
A	Відбивач звуку параболічної форми, у фокусі якого розташований звичайний (ненаправлений) мікрофон
B	Трубчасті мікрофони, що приймають звук не на площині, а уздовж деякої лінії, що збігається з напрямком на джерело звуку.
C	Пристрої, що реалізують ідею одночасного прийому звукового поля в дискретних точках деякої площині, перпендикулярної до напрямку на джерело звуку, до яких під'єднані відкриті торці звуководів (трубок малого діаметру)
D	Пристрої, які використовують операцію віднімання у напрямку приходу сигналу, що дозволяє суттєво зменшити рівень статичних завад

Запитання 34	Направлений мікрофон з плоскими акустичними фазованими решітками це:
A	Відбивач звуку параболічної форми, у фокусі якого розташований звичайний (ненаправлений) мікрофон
B	Трубчасті мікрофони, що приймають звук не на площині, а уздовж деякої лінії, що збігається з напрямком на джерело звуку.
C	Пристрої, що реалізують ідею одночасного прийому звукового поля в дискретних точках деякої площині, перпендикулярної до напрямку на джерело звуку, до яких під'єднані відкриті торці звуководів (трубок малого діаметру)
D	Пристрої, які використовують операцію віднімання у напрямку приходу сигналу, що дозволяє суттєво зменшити рівень статичних завад

Запитання 35	Направлений мікрофон трубчатого типу це:
A	Відбивач звуку параболічної форми, у фокусі якого розташований звичайний (ненаправлений) мікрофон
B	Трубчасті мікрофони, що приймають звук не на площині, а уздовж деякої лінії, що збігається з напрямком на джерело звуку.
C	Пристрої, що реалізують ідею одночасного прийому звукового поля в дискретних точках деякої площині, перпендикулярної до напрямку на джерело звуку, до яких під'єднані відкриті торці звуководів (трубок малого діаметру)
D	Пристрої, які використовують операцію віднімання у напрямку приходу сигналу, що дозволяє суттєво зменшити рівень статичних завад

Запитання 36	Методу синфазної низькочастотної маскувальної перешкоди полягає в:
A	Подаванні під час розмови в кожний провід телефонної лінії відносно єдиної системи заземлення апаратури АТС і захисного заземлення електромережі абонента узгоджених за амплітудою та фазою перешкоджаючих сигналів, спектральна густина потужності яких зосереджена у тональному діапазоні
B	Подаванні під час розмови в телефонну лінію білого шуму або псевдовипадкових імпульсних послідовностей із надтонального 6–20 кГц та ультразвукового (понад 20 кГц) діапазонів
C	Подавання під час розмови в лінію постійної напруги, що відповідає напрузі в лінії при піднятій слухавці, але оберненої полярності.
D	Подавання в лінію низькочастотної маскувальної перешкоди для створення завад роботі виносних мікрофонів, що використовують телефонну лінію для передавання інформації

Запитання 37	Метод високочастотної маскувальної перешкоди полягає в:
A	Подаванні під час розмови в кожний провід телефонної лінії відносно єдиної системи заземлення апаратури АТС і захисного заземлення електромережі абонента узгоджених за амплітудою та фазою перешкоджаючих сигналів, спектральна густина потужності яких зосереджена у надтональному (6–20 кГц) та ультразвуковому (понад 20 кГц) діапазонах
B	Подаванні під час розмови в телефонну лінію білого шуму або псевдовипадкових імпульсних послідовностей із надтонального (6–20кГц) та ультразвукового (понад 20 кГц) діапазонів
C	Подавання під час розмови в лінію постійної напруги, що відповідає напрузі в лінії при піднятій слухавці, але оберненої полярності.
D	Подавання в лінію низькочастотної маскувальної перешкоди для створення завад роботі виносних мікрофонів, що використовують телефонну лінію для передавання інформації

Запитання 38	В пристрою захисту телефонних апаратів типу «Граніт-8» та аналогічних використовується зустрічно-паралельне включення діодів, які призначені для:
A	Обмеження мінімального рівня електричного сигналу, який може пройти через пристрій
B	Обмеження максимального рівня електричного сигналу, який може пройти через пристрій
C	Випрямлення електричного сигналу, який проходить через пристрій
D	Створення синфазної завади для захисту розмови від прослуховування

Запитання 39	Лазерні стетоскопи це пристрої, що:
A	Дозволяють зчитувати лазерним променем вібрацію з предметів, промодульованих акустичним сигналом
B	Дозволяють зчитувати лазерним променем інформацію, яка передається в оптоволоконному кабелі
C	Використовуються в пристроях запису/читання оптичних дисків (CD та DVD-приводах)
D	Використовуються в медицині для моніторингу хвороби серця та легень

Запитання 40	Електронні стетоскопи це пристрої, що:
A	Використовуються для перехоплення мовної інформації по віброакустичним каналам и встановлюються на межі контрольованої зони
B	Використовуються для перехоплення віброакустичної інформації и встановлюються всередині контрольованої зони
C	Дозволяють зчитувати лазерним променем вібрацію з предметів, промодульованих акустичним сигналом
D	Використовуються в пристроях запису/читання оптичних дисків (CD та DVD-приводах)

Запитання 41	При навмисній дезінформації застосовують як свідому брехню, так і напівправду, що повинне призвести до прийняття супротивником хибних рішень. Найбільш поширеними прийомами тут є:
A	Всі перелічені прийоми
B	Подання правди в такому контексті (додавання помилкового факту або натяку), щоб вона сприймалася як брехня
C	Повідомлення інформації такими словами, які можна тлумачити по-різному
D	Пряме приховування фактів

Запитання 42	Спотворення, що виникають в процесі ретрансляції інформації через носіїв, найчастіше відбуваються через:
A	Всі перелічені фактори
B	Передачу тільки частини повідомлення
C	Переказу почутого своїми словами («зіпсований телефон»)
D	Пропуску фактури через призму суб'єктивно-особистісних відносин

Запитання 43	Для успішності боротьби з ймовірною дезінформацією слід :
A	Всі перелічені заходи
B	Розуміти, чи здатний інформатор за своїм становищем мати доступ до відповідної інформації
C	Враховувати суб'єктивні (зарозумілість, фантазійність і т.д.) характеристики джерела і його передбачуване ставлення до повідомлення
D	Пам'ятати, що особливо легко сприймається та дезінформація, яку ви припускаєте, чи бажаєте почути

Запитання 44	Переробка інформації після попереднього збирання фактури і конкретної постановки проблеми має на увазі:
A	Всі перелічені заходи
B	Систематизацію фактів, які сортують за ступенем їх ставлення до того чи іншого питання
C	Побудова припущень, що пояснюють основні факти
D	Оформлення висновків і їх перевірка на відповідність іншим фактами

Запитання 45	Хибна інтерпретація фактури, що отримана при спілкуванні з інформатором, імовірна, якщо:
A	Всі перелічені випадки
B	Представлені не всі матеріали
C	Деякі з наявних під рукою фактів сумнівні
D	Вся увага зосереджується лише на тих повідомленнях, котрі підтверджують очікування і припущення аналітика

Запитання 46	Суб'єктами відносин, пов'язаних із захистом інформації в системах, є:
A	Володільці інформації
B	Власники системи
C	Користувачі
D	Всі перераховані

Запитання 47	До основних завдань контролю у сфері електронно-цифрового підпису НЕ належить:
A	Усунення проблем, зв'язаних із несанкціонованим використанням ЕЦП
B	Забезпечення відповідності порядку застосування ЕЦП державними установами
C	Оцінка діяльності суб'єктів правових відносин у сфері послуг електронного цифрового підпису щодо дотримання законодавства
D	Захист авторських прав у сфері інформаційних технологій

Запитання 48	Носії ключової інформації згідно з нормативними документами можуть розміщуватися
A	На всіх перерахованих носіях
B	На USB-накопичувачі
C	На компакт диску
D	На аркуші паперу чи фотоплівці

Запитання 49	Скільки рівнів можливостей порушника визначається залежно від вірогідних умов експлуатації засобів криптографічного захисту інформації та відповідно до цінності інформації?
A	2
B	3
C	4
D	5

Запитання 50	Під час діяльності іноземних інспекційних груп на території України ДСТСЗІ перевіряють:
A	Чи увезена ІІГ інспекційна апаратура та обладнання
B	Дотримання договірних умов використання ІІГ інспекційного обладнання під час інспекційних перевірок та використання апаратури спостереження під час спостережних польотів
C	Своєчасність та повнота оповіщення об'єктів інспектування та об'єктів спостереження
D	Всі наведені пункти

3.1.2. Модуль 2. «Радіомоніторинг та радіопротидія на об'єктах інформаційної діяльності»
Здобувачі, які проходять випробування, повинні володіти знаннями та навичками розв'язання завдань за наступними темами:

<u>Запитання 1</u>	До якого діапазону відноситься радіохвиля з частотою 1 кГц?
A	Наддовгі хвилі
B	Довгі хвилі
C	Середні хвилі
D	Короткі хвилі
E	Ультракороткі хвилі

<u>Запитання 2</u>	До якого діапазону відноситься радіохвиля з частотою 100 кГц?
A	Наддовгі хвилі
B	Довгі хвилі
C	Середні хвилі
D	Короткі хвилі
E	Ультракороткі хвилі

<u>Запитання 3</u>	До якого діапазону відноситься радіохвиля з частотою 1 МГц?
A	Наддовгі хвилі
B	Довгі хвилі
C	Середні хвилі
D	Короткі хвилі
E	Ультракороткі хвилі

<u>Запитання 4</u>	До якого діапазону відноситься радіохвиля з частотою 10 МГц?
A	Наддовгі хвилі
B	Довгі хвилі
C	Середні хвилі
D	Короткі хвилі
E	Ультракороткі хвилі

<u>Запитання 5</u>	До якого діапазону відноситься радіохвиля з частотою 100 МГц?
A	Наддовгі хвилі
B	Довгі хвилі
C	Середні хвилі
D	Короткі хвилі
E	Ультракороткі хвилі

<u>Запитання 6</u>	До якого піддіапазону УКХ відноситься радіохвиля з частотою 200 МГц?
A	Метрові хвилі
B	Дециметрові хвилі
C	Сантиметрові хвилі
D	Міліметрові хвилі
E	Субміліметрові хвилі

<u>Запитання 7</u>	До якого піддіапазону УКХ відноситься радіохвиля з частотою 2 ГГц?
A	Метрові хвилі
B	Дециметрові хвилі
C	Сантиметрові хвилі
D	Міліметрові хвилі
E	Субміліметрові хвилі

<u>Запитання 8</u>	До якого піддіапазону УКХ відноситься радіохвиля з частотою 20 ГГц?
A	Метрові хвилі
B	Дециметрові хвилі
C	Сантиметрові хвилі
D	Міліметрові хвилі
E	Субміліметрові хвилі

<u>Запитання 9</u>	До якого піддіапазону УКХ відноситься радіохвиля з частотою 200 ГГц?
A	Метрові хвилі
B	Дециметрові хвилі
C	Сантиметрові хвилі
D	Міліметрові хвилі
E	Субміліметрові хвилі

<u>Запитання 10</u>	До якого піддіапазону УКХ відноситься радіохвиля з частотою 2 ТГц?
A	Метрові хвилі
B	Дециметрові хвилі
C	Сантиметрові хвилі
D	Міліметрові хвилі
E	Субміліметрові хвилі

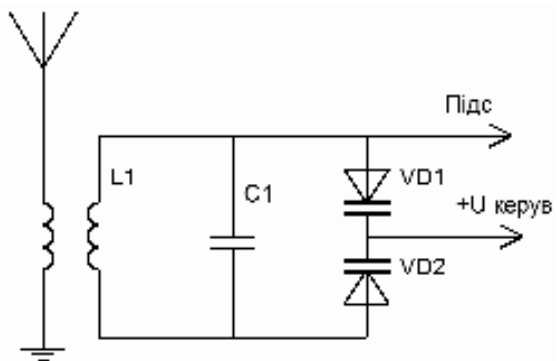
<u>Запитання 11</u>	Якого типу антена зображена на рисунку?	
A	Хвильовий канал	
B	Симетричний диполь	
C	Рамочна антена	
D	Штиркова антена	
E	Логоперіодична антена	

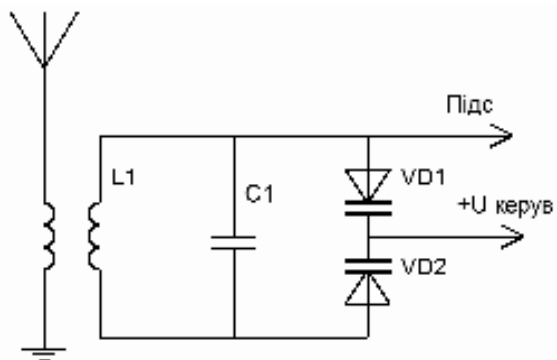
<u>Запитання 12</u>	Якого типу антена зображена на рисунку?	
A	Хвильовий канал	
B	Симетричний диполь	
C	Рамочна антена	
D	Штиркова антена	
E	Логоперіодична антена	

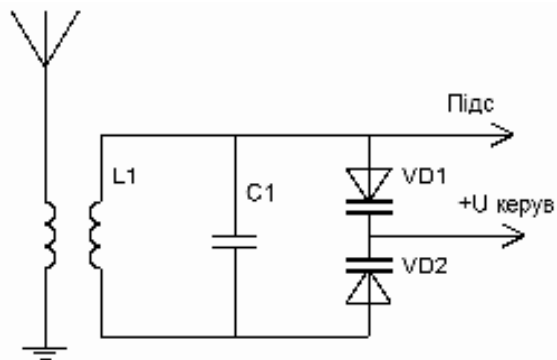
<u>Запитання 13</u>	Якого типу антена зображена на рисунку?	
A	Хвильовий канал	
B	Симетричний диполь	
C	Рамочна антена	
D	Штиркова антена	
E	Логоперіодична антена	

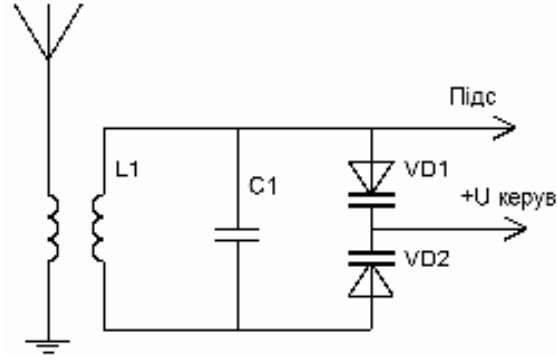
<u>Запитання 14</u>	Якого типу антена зображена на рисунку?	
A	Хвильовий канал	
B	Симетричний диполь	
C	Рамочна антена	
D	Штиркова антена	
E	Логоперіодична антена	

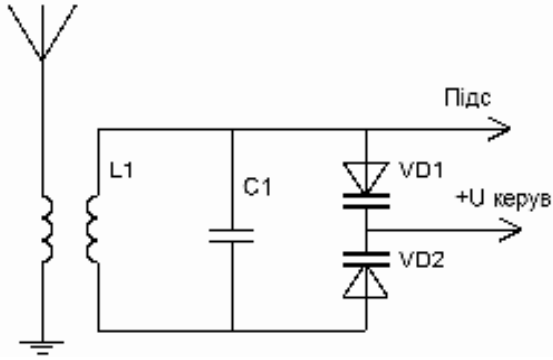
<u>Запитання 15</u>	Якого типу антена зображена на рисунку?	
A	Хвильовий канал	
B	Симетричний диполь	
C	Штиркова антена	
D	Щільова антена	
E	Логоперіодична антена	

<u>Запитання 16</u>	На схемі подано вхідний тракт пристрою радіомоніторингу зі скануванням частоти. Ємність C1 становить 6 пФ, ємність варікапу змінюється у межах 6-33 пФ. У яких межах змінюється частота контуру (коефіцієнт зміни)?	
A	1,8	
B	2	
C	3,25	
D	4	
E	5,5	

<u>Запитання 17</u>	На схемі подано вхідний тракт пристрою радіомоніторингу зі скануванням частоти. Ємність C1 становить 4 пФ, ємність варікапу змінюється у межах 4-22 пФ. У яких межах змінюється частота контуру (коефіцієнт зміни)?	
A	1,8	
B	2	
C	3,25	
D	4	
E	5,5	

<u>Запитання 18</u>	На схемі подано вхідний тракт пристрою радіомоніторингу зі скануванням частоти. Ємність C1 становить 8 пФ, ємність варікапу змінюється у межах 8-44 пФ. У яких межах змінюється частота контуру (коефіцієнт зміни)?	
A	1,8	
B	2	
C	3,25	
D	4	
E	5,5	

<u>Запитання 19</u>	На схемі подано вхідний тракт пристрою радіомоніторингу зі скануванням частоти. Ємність C1 становить 2 пФ, ємність варікапу змінюється у межах 2-11 пФ. У яких межах змінюється частота контуру (коефіцієнт зміни)?	
A	1,8	
B	2	
C	3,25	
D	4	
E	5,5	

<u>Запитання 20</u>	На схемі подано вхідний тракт пристрою радіомоніторингу зі скануванням частоти. Ємність C1 становить 10 пФ, ємність варикапу змінюється у межах 10-55 пФ. У яких межах змінюється частота контуру (коефіцієнт зміни)?	
A	1,8	
B	2	
C	3,25	
D	4	
E	5,5	

<u>Запитання 21</u>	При радіомоніторингу виявлено сигнал, локалізований у діапазоні 400-405 кГц. Оцініть, на який інформаційний потік розрахований даний канал, якщо відношення сигнал-шум очікується на рівні 30 дБ.
A	Близько 5 кбіт/с
B	Близько 10 кбіт/с
C	Близько 50 кбіт/с
D	Близько 100 кбіт/с
E	Близько 400 кбіт/с

<u>Запитання 22</u>	При радіомоніторингу виявлено сигнал, локалізований у діапазоні 500-505 кГц. Оцініть, на який інформаційний потік розрахований даний канал, якщо відношення сигнал-шум очікується на рівні 30 дБ.
A	Близько 5 кбіт/с
B	Близько 10 кбіт/с
C	Близько 50 кбіт/с
D	Близько 100 кбіт/с
E	Близько 500 кбіт/с

<u>Запитання 23</u>	При радіомоніторингу виявлено сигнал, локалізований у діапазоні 600-605 кГц. Оцініть, на який інформаційний потік розрахований даний канал, якщо відношення сигнал-шум очікується на рівні 30 дБ.
A	Близько 5 кбіт/с
B	Близько 10 кбіт/с
C	Близько 50 кбіт/с
D	Близько 100 кбіт/с
E	Близько 600 кбіт/с

<u>Запитання 24</u>	При радіомоніторингу виявлено сигнал, локалізований у діапазоні 450-455 кГц. Оцініть, на який інформаційний потік розрахований даний канал, якщо відношення сигнал-шум очікується на рівні 30 дБ.
A	Близько 5 кбіт/с
B	Близько 10 кбіт/с
C	Близько 50 кбіт/с
D	Близько 100 кбіт/с
E	Близько 450 кбіт/с

<u>Запитання 25</u>	При радіомоніторингу виявлено сигнал, локалізований у діапазоні 550-555 кГц. Оцініть, на який інформаційний потік розрахований даний канал, якщо відношення сигнал-шум очікується на рівні 30 дБ.
A	Близько 5 кбіт/с
B	Близько 10 кбіт/с
C	Близько 50 кбіт/с
D	Близько 100 кбіт/с
E	Близько 550 кбіт/с

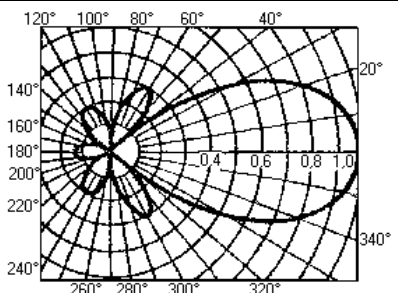
<u>Запитання 26</u>	Засоби радіопротидії створюють білий шум у деякому діапазоні частот. Приймач налаштований на прийом сигналу у тому ж діапазоні. Як зміниться відношення сигнал-шум у приймачі, якщо ширина частотної смуги вхідного кола приймача (селективність) зменшиться удвічі?
A	-6 дБ
B	-3 дБ
C	0 дБ (не зміниться)
D	+3 дБ
E	+6 дБ

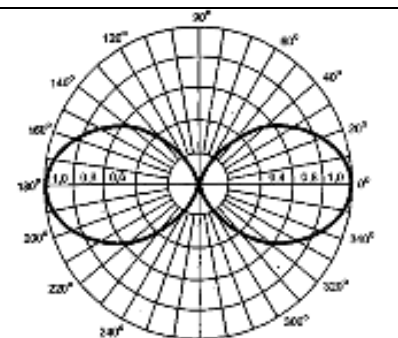
<u>Запитання 27</u>	Засоби радіопротидії створюють білий шум у деякому діапазоні частот. Приймач налаштований на прийом сигналу у тому ж діапазоні. Як зміниться відношення сигнал-шум у приймачі, якщо ширина частотної смуги вхідного кола приймача (селективність) збільшиться удвічі?
A	-6 дБ
B	-3 дБ
C	0 дБ (не зміниться)
D	+3 дБ
E	+6 дБ

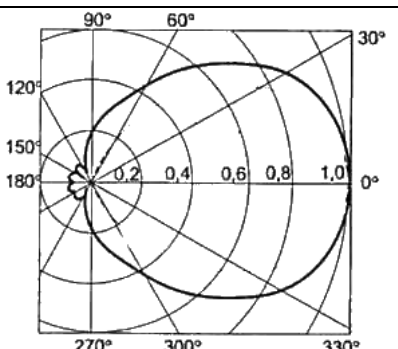
<u>Запитання 28</u>	Засоби радіопротидії створюють білий шум у деякому діапазоні частот. Приймач налаштований на прийом сигналу у тому ж діапазоні. Як зміниться відношення сигнал-шум у приймачі, якщо ширина частотної смуги вхідного кола приймача (селективність) зменшиться у 4 рази?
A	-6 дБ
B	-3 дБ
C	0 дБ (не зміниться)
D	+3 дБ
E	+6 дБ

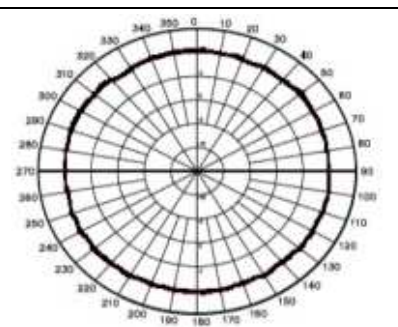
<u>Запитання 29</u>	Засоби радіопротидії створюють білий шум у деякому діапазоні частот. Приймач налаштований на прийом сигналу у тому ж діапазоні. Як зміниться відношення сигнал-шум у приймачі, якщо ширина частотної смуги вхідного кола приймача (селективність) збільшиться у 4 рази?
A	-6 дБ
B	-3 дБ
C	0 дБ (не зміниться)
D	+3 дБ
E	+6 дБ

<u>Запитання 30</u>	Засоби радіопротидії створюють білий шум у деякому діапазоні частот. Приймач налаштований на прийом сигналу у тому ж діапазоні. Як зміниться відношення сигнал-шум у приймачі, якщо ширина частотної смуги вхідного кола приймача (селективність) зменшиться у 10 разів?
A	-20 дБ
B	-10 дБ
C	0 дБ (не зміниться)
D	+10 дБ
E	+20 дБ

<u>Запитання 31</u>	Для якої антени типовою є дана діаграма спрямованості?	
A	Логоперіодична	
B	Штирєва	
C	Симетричний диполь	
D	Параболічна	
E	Хвильовий канал	

<u>Запитання 32</u>	Для якої антени типовою є дана діаграма спрямованості?	
A	Логоперіодична	
B	Штирєва	
C	Симетричний диполь	
D	Параболічна	
E	Хвильовий канал	

<u>Запитання 33</u>	Для якої антени типовою є дана діаграма спрямованості?	
A	Логоперіодична	
B	Штирєва	
C	Симетричний диполь	
D	Параболічна	
E	Хвильовий канал	

<u>Запитання 34</u>	Для якої антени типовою є дана діаграма спрямованості?	
A	Логоперіодична	
B	Штирєва	
C	Симетричний диполь	
D	Параболічна	
E	Хвильовий канал	

<u>Запитання 35</u>	Для якої антени типовою є дана діаграма спрямованості?	
A	Логоперіодична	
B	Штирєва	
C	Симетричний диполь	
D	Параболічна	
E	Хвильовий канал	

<u>Запитання 36</u>	Засіб радіопротидії встановлений у куті квадратного приміщення і забезпечує у найвіддаленішому куті відношення сигнал-шум (SNR) на рівні -30 дБ. Яким буде SNR якщо засіб перенести до центру приміщення?
A	-60 дБ
B	-36 дБ
C	-33 дБ
D	-27 дБ
E	-24 дБ

<u>Запитання 37</u>	Засіб радіопротидії встановлений у центрі квадратного приміщення і забезпечує у куті приміщення відношення сигнал-шум (SNR) на рівні -30 дБ. Яким буде SNR у тому ж куті якщо засіб перенести до найвіддаленішого кута приміщення?
A	-60 дБ
B	-36 дБ
C	-33 дБ
D	-27 дБ
E	-24 дБ

<u>Запитання 38</u>	Засіб радіопротидії встановлений у куті квадратного приміщення і забезпечує у найвіддаленішому куті відношення сигнал-шум (SNR) на рівні -20 дБ. Яким буде SNR якщо засіб перенести до центру приміщення?
A	-40 дБ
B	-26 дБ
C	-23 дБ
D	-17 дБ
E	-14 дБ

<u>Запитання 39</u>	Засіб радіопротидії встановлений у центрі квадратного приміщення і забезпечує у куті приміщення відношення сигнал-шум (SNR) на рівні -20 дБ. Яким буде SNR у тому ж куті якщо засіб перенести до найвіддаленішого кута приміщення?
A	-40 дБ
B	-26 дБ
C	-23 дБ
D	-17 дБ
E	-14 дБ

<u>Запитання 40</u>	Засіб радіопротидії встановлений у куті квадратного приміщення і забезпечує у сусідньому куті відношення сигнал-шум (SNR) на рівні -30 дБ. Яким буде SNR якщо засіб перенести до центру приміщення?
A	-60 дБ
B	-36 дБ
C	-33 дБ
D	-27 дБ
E	-24 дБ

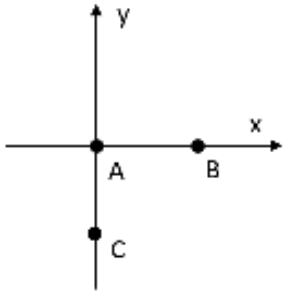
<u>Запитання 41</u>	Джерело перешкоди при випробуваннях було підключене до неспрямованої антени. На відстані 1 м від неї напруженість електромагнітного поля складала 1 В/м. У робочому режимі було використано антену з наведеною на рисунку діаграмою спрямованості. Яку напруженість матиме поле перешкоди на відстані 10 м вздовж осі антени?	
A	32 мВ/м	
B	320 мВ/м	
C	1 В/м	
D	3,2 В/м	
E	32 В/м	

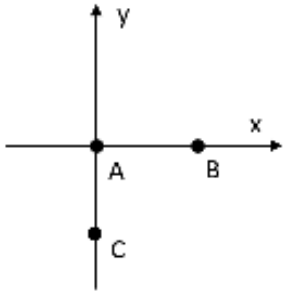
<u>Запитання 42</u>	Джерело перешкоди при випробуваннях було підключене до неспрямованої антени. На відстані 1 м від неї інтенсивність електромагнітного поля було прийнято за 0 дБ. У робочому режимі було використано антену з наведеною на рисунку діаграмою спрямованості. Яку інтенсивність матиме поле перешкоди на відстані 10 м під кутом 60° до осі антени?	
A	-16 дБ	
B	-6 дБ	
C	0 дБ	
D	4 дБ	
E	14 дБ	

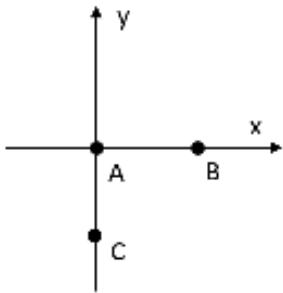
<u>Запитання 43</u>	Джерело перешкоди при випробуваннях було підключене до неспрямованої антени. На відстані 1 м від неї інтенсивність електромагнітного поля було прийнято за 0 дБ. У робочому режимі було використано антену з наведеною на рисунку діаграмою спрямованості. Яку інтенсивність матиме поле перешкоди на відстані 10 м під кутом 300° до осі антени?	
A	-16 дБ	
B	-6 дБ	
C	0 дБ	
D	4 дБ	
E	14 дБ	

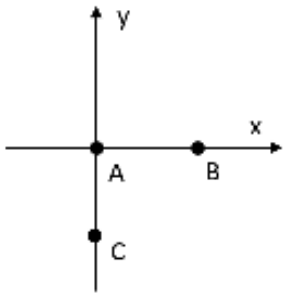
<u>Запитання 44</u>	Джерело перешкоди при випробуваннях було підключене до неспрямованої антени. На відстані 1 м від неї інтенсивність електромагнітного поля було прийнято за 0 дБ. У робочому режимі було використано антену з наведеною на рисунку діаграмою спрямованості. Яку інтенсивність матиме поле перешкоди на відстані 1 м під кутом 90° до осі антени?	
A	0 дБ	
B	2 дБ	
C	8 дБ	
D	10 дБ	
E	12 дБ	

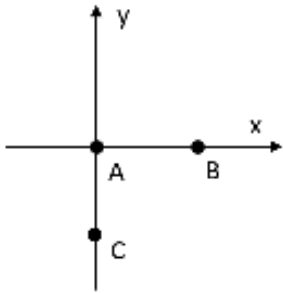
<u>Запитання 45</u>	Джерело перешкоди при випробуваннях було підключене до неспрямованої антени. На відстані 1 м від неї напруженість електромагнітного поля складала 1 В/м. У робочому режимі було використано антену з наведеною на рисунку діаграмою спрямованості. Яку напруженість матиме поле перешкоди на відстані 100 м вздовж осі антени?	
A	32 мВ/м	
B	320 мВ/м	
C	1 В/м	
D	3,2 В/м	
E	32 В/м	

<u>Запитання 46</u>	Засіб радіомоніторингу знаходиться у т. А і фіксує наявність стороннього сигналу. При переміщенні засобу у т. В фаза сигналу не змінюється, при переміщенні у т. С змінюється на $-\pi/2$. Вкажіть очікуване положення джерела сигналу.	
A	Вздовж осі x	
B	Вздовж осі y	
C	$+45^\circ$ к осі x	
D	$+45^\circ$ к осі y	
E	Проти осі x	

<u>Запитання 47</u>	Засіб радіомоніторингу знаходиться у т. А і фіксує наявність стороннього сигналу. При переміщенні засобу у т. В фаза сигналу змінюється на $-\pi/2$, при переміщенні у т. С змінюється на $-\pi/2$. Вкажіть очікуване положення джерела сигналу.	
A	Вздовж осі x	
B	Вздовж осі y	
C	$+45^\circ$ к осі x	
D	$+45^\circ$ к осі y	
E	Проти осі x	

<u>Запитання 48</u>	Засіб радіомоніторингу знаходиться у т. А і фіксує наявність стороннього сигналу. При переміщенні засобу у т. В фаза сигналу змінюється на $+\pi/2$, при переміщенні у т. С змінюється на $-\pi/2$. Вкажіть очікуване положення джерела сигналу.	
A	Вздовж осі x	
B	Вздовж осі y	
C	$+45^\circ$ к осі x	
D	$+45^\circ$ к осі y	
E	Проти осі x	

<u>Запитання 49</u>	Засіб радіомоніторингу знаходиться у т. А і фіксує наявність стороннього сигналу. При переміщенні засобу у т. С фаза сигналу не змінюється, при переміщенні у т. В змінюється на $+\pi/2$. Вкажіть очікуване положення джерела сигналу.	
A	Вздовж осі x	
B	Вздовж осі y	
C	$+45^\circ$ к осі x	
D	$+45^\circ$ к осі y	
E	Проти осі x	

<u>Запитання 50</u>	Засіб радіомоніторингу знаходиться у т. А і фіксує наявність стороннього сигналу. При переміщенні засобу у т. С фаза сигналу не змінюється, при переміщенні у т. В змінюється на $-\pi/2$. Вкажіть очікуване положення джерела сигналу.	
A	Вздовж осі x	
B	Вздовж осі y	
C	$+45^\circ$ к осі x	
D	$+45^\circ$ к осі y	
E	Проти осі x	

3.2. Розділ другий

Розділ другий кваліфікаційного екзамену, на здобуття ступеня вищої освіти магістр складається з завдань першого і другого модулів дисципліни «Інформаційна та кібербезпека спеціалізованих інформаційно-комунікаційних систем на водному транспорті».

Метою вивчення навчальної дисципліни «Інформаційна та кібербезпека інформаційно-комунікаційних систем на водному транспорті» є ознайомлення з методами та засобами захисту інформації і відповідними нормативно-правовими актами в сфері спеціалізованих інформаційно-комунікаційних систем (ІКС) об'єктів морської інфраструктури, особливостями побудови і експлуатації ІКС водотранспортного комплексу та основним напрямком проведення робіт по забезпеченню кібербезпеки як безпосередньо на об'єктах морської інфраструктури, так і на ІКС водотранспортного комплексу в цілому, з урахуванням вимог українських та міжнародних нормативних документів.

3.2.1. Модуль 1. Інформаційно-комунікаційні системи водного транспорту».

Здобувачі, які проходять випробування, повинні володіти знаннями та навичками розв'язання завдань за наступними темами:

<u>Запитання 1</u>	Об'єктами захисту на водотранспортному комплексі України є:
A	Всі перераховані об'єкти
B	Морські рухомі об'єкти (транспортні та пасажирські судна, наукові та спеціальні судна і плавзасоби, судна технічного флоту тощо);
C	Об'єкти морської інфраструктури (підводні транспортні трубопроводи та кабелі зв'язку, морські стаціонарні платформи, гідротехнічні споруди та акваторії портів і ВПШ, акваторії приморських об'єктів енергетики та промисловості, рекреаційні зони тощо)
D	Об'єкти берегової інфраструктури (портові причали, системи управління рухом суден, тощо).

<u>Запитання 2</u>	Загрозами безпеці інформаційних і телекомунікаційних систем водотранспортного комплексу України є:
A	Всі перераховані загрози
B	Впровадження електронних, гідроакустичних і інших пристроїв для перехоплення інформації в технічні засоби обробки, зберігання й передачі інформації з каналів зв'язку, а також у службові приміщення суден та офісів незалежно від форми власності
C	Впровадження в апаратні й програмні засоби комунікацій водного транспорту елементів, що реалізують функції, не передбачені документацією на ці засоби;
D	Впровадження в засоби комунікацій водного транспорту апаратних і програмних засобів, що порушують нормальне функціонування їхніх інформаційно-телекомунікаційних систем;

<u>Запитання 3</u>	Загрозами безпеці інформаційних і телекомунікаційних систем водотранспортного комплексу України є:
A	Всі перераховані загрози
B	Знищення, пошкодження, радіоелектронне й гідроакустичне придушення або фізичне руйнування морських засобів і систем телекомунікації й зв'язку
C	Витік інформації про об'єкти водного транспорту й морської інфраструктури по технічним каналам
D	Несанкціонований збір інформації про об'єкти водного транспорту й морської інфраструктури, про рельєф дна й гідрологію морського району

<u>Запитання 4</u>	Загрозами безпеці інформаційних і телекомунікаційних систем водотранспортного комплексу України є:
A	Всі перераховані загрози
B	Знищення, пошкодження, радіоелектронне й гідроакустичне придушення або фізичне руйнування морських засобів і систем телекомунікації й зв'язку
C	Витік інформації про об'єкти водного транспорту й морської інфраструктури по технічним каналам
D	Перехоплення інформації в мережах передачі даних і на лініях зв'язку, дешифрування цієї інформації й нав'язування хибної інформації

<u>Запитання 5</u>	Оцінка ризику, загрози і вразливості з точки зору охорони на судні
A	Всі перераховані знання
B	Знання, що дозволяють на недискримінаційній основі розпізнавати осіб, що можуть створювати загрозу охороні
C	Знання, що дозволяють розпізнавати зброю, небезпечні речовини і устаткування
D	Знання методів управління масами людей та їх контролю, де це необхідно
<u>Запитання 6</u>	До сфери компетенції осіб командного складу, відповідальних за охорону на судні НЕ ВХОДИТЬ («Манільські поправки до Додатка до Міжнародної конвенції про підготовку і дипломування моряків...»)
A	Надання невідкладної медичної допомоги у разі нещасного випадку або захворювання на судні
B	Ведення плану охорони судна та контроль за його здійсненням
C	Оцінка ризику, загрози і вразливості з точки зору охорони
D	Заохочення поінформованості та пильності у питаннях охорони

<u>Запитання 7</u>	Усі особи, які не є пасажиром, повинні пройти ознайомлювальну підготовку з питань, пов'язаних з охороною, щоб мати змогу:
A	Всі вказані випадки
B	Повідомляти про випадки, пов'язані з охороною, у тому числі загрозу нападу або напад піратів або озброєних грабіжників;
C	Знати процедури, які необхідно виконувати у випадку виявлення загрози для охорони
D	Приймати участь в пов'язаних з охороною процедурами та діях у надзвичайних ситуаціях

<u>Запитання 8</u>	Головним офіцером, відповідальним за охорону на судні, є:
A	Капітан
B	Старший помічник капітана
C	Старший механік
D	Боцман

<u>Запитання 9</u>	Міжнародний Кодекс з охорони суден і портових засобів містить ряд функціональних вимог. Які з вказаних нижче вимог НЕ РЕГЛАМЕНТУЮТЬСЯ Кодексом:
A	вимоги стосовно наявності озброєного підрозділу охорони суден при їх перебуванні з зоні військового конфлікту чи піратської загрози
B	збір й оцінку інформації, що стосується загроз охороні, й обмін такою інформацією з відповідними Договірними Урядами
C	вимоги з дотримання протоколів зв'язку для суден і портових засобів
D	забезпечення засобами подачі сигналів тривоги для реагування на загрозу охороні або інциденти, пов'язані з охороною

<u>Запитання 10</u>	"Рівень охорони 1", в відповідності до Кодексу ОСПЗ, означає:
A	Рівень, за якого повинні постійно підтримуватися мінімальні належні заходи з охорони
B	Рівень, за якого, через підвищену небезпеку інциденту, пов'язаного з охороною, протягом певного періоду повинні підтримуватися спеціальні додаткові заходи з охорони
C	Рівень, за якого протягом обмеженого періоду, коли інцидент, пов'язаний з охороною, є ймовірним або неминучим, повинні підтримуватися підвищені спеціальні заходи з охорони, хоча може бути неможливим визначити конкретну ціль нападу
D	Інша відповідь

<u>Запитання 11</u>	"Рівень охорони 2", в відповідності до Кодексу ОСПЗ, означає:
A	Рівень, за якого повинні постійно підтримуватися мінімальні належні заходи з охорони
B	Рівень, за якого, через підвищену небезпеку інциденту, пов'язаного з охороною, протягом певного періоду повинні підтримуватися спеціальні додаткові заходи з охорони
C	Рівень, за якого протягом обмеженого періоду, коли інцидент, пов'язаний з охороною, є ймовірним або неминучим, повинні підтримуватися підвищені спеціальні заходи з охорони, хоча може бути неможливим визначити конкретну ціль нападу
D	Інша відповідь

<u>Запитання 12</u>	"Рівень охорони 3", в відповідності до Кодексу ОСПЗ, означає:
A	Рівень, за якого повинні постійно підтримуватися мінімальні належні заходи з охорони
B	Рівень, за якого, через підвищену небезпеку інциденту, пов'язаного з охороною, протягом певного періоду повинні підтримуватися спеціальні додаткові заходи з охорони
C	Рівень, за якого протягом обмеженого періоду, коли інцидент, пов'язаний з охороною, є ймовірним або неминучим, повинні підтримуватися підвищені спеціальні заходи з охорони, хоча може бути неможливим визначити конкретну ціль нападу
D	Інша відповідь

<u>Запитання 13</u>	При встановленні належного рівня охорони, в відповідності до Кодексу ОСПЗ, НЕ ВРАХОВУЮТЬСЯ чинники, що визначають:
A	Ступінь того, що можливі наслідки такого інциденту вплинуть на порядок проходження процедури атестації судна
B	Ступінь того, що інформація про загрозу заслуговує довіри
C	Ступінь того, що інформацію стосовно загрози підтверджено
D	Ступінь того, що загроза, зазначена в інформації, є конкретною або неминучою

<u>Запитання 14</u>	Договірні Уряди, в відповідності до Кодексу ОСПЗ, можуть передавати визнаній у сфері охорони організації деякі зі своїх обов'язків, пов'язаних з охороною, а саме:
A	Схвалення плану охорони судна
B	Встановлення рівня охорони, що може бути застосований
C	Визначення портових засобів, на які повинно бути призначено офіцера охорони портового засобу
D	Схвалення плану охорони портового засобу

<u>Запитання 15</u>	В відповідності до Кодексу ОСПЗ, Декларація з охорони судна повинна оформлюватися (якщо може бути застосовано):
A	Капітаном чи офіцером охорони судна
B	Офіцером охорони чи капітаном порту, де знаходиться судна на даний момент
C	Організацією, відповідальною за охорону в порту реєстрації судна
D	Власником вантажу, що знаходиться на судні, або страховою компанією

<u>Запитання 16</u>	Які вимоги НЕ Є ОБОВ'ЯЗКОВИМИ при розробці «Плану охорони судна»:
A	Відомості про капітана судна, зокрема інформацію для зв'язку з ним у будь-який час доби
B	Заходи, спрямовані на запобігання занесення на судно зброї, небезпечних речовин і пристроїв, які призначено для застосування проти людей, суден або портів і на перевезення яких немає дозволу
C	Визначення районів обмеженого доступу й заходів із запобігання несанкціонованому доступові до них
D	Відомості про офіцера охорони компанії, зокрема інформацію для зв'язку з ним у будь-який час доби

<u>Запитання 17</u>	У плані охорони судна повинні передбачатися чіткі позначення всіх районів обмеженого доступу. До таких районів НЕ МОЖУТЬ бути віднесені:
A	Приміщення та трюми, для розміщення особливо важливих вантажів
B	Ходовий місток, машинні приміщення категорії а та інші пости управління
C	Приміщення, що містять небезпечні вантажі або шкідливі речовини
D	Житлові приміщення екіпажу
<u>Запитання 18</u>	Для якого рівня охорони у плані охорони судна повинні бути встановлені заходи з охорони, що підлягають застосуванню в районах обмеженого доступу, які можуть уключати використання засобів спостереження для контролю цих місць:
A	1
B	2
C	3
D	Не використовуються

<u>Запитання 19</u>	Для якого рівня охорони у плані охорони судна повинні бути встановлені заходи з охорони, що підлягають застосуванню в районах обмеженого доступу, які можуть уключати безперервний контроль засобів спостереження для контролю цих місць:
A	1
B	2
C	3
D	Не використовуються

<u>Запитання 20</u>	Для якого рівня охорони у плані охорони судна повинні бути встановлені заходи з охорони, що підлягають застосуванню в районах обмеженого доступу, які можуть уключати зачинення або перекриття місць доступу
A	1
B	2
C	3
D	Не використовуються

<u>Запитання 21</u>	Для якого рівня охорони у плані охорони судна повинні бути встановлені заходи з охорони, що підлягають застосуванню в районах обмеженого доступу, які можуть уключати виставлення постів охорони або патрулів
A	1
B	2
C	3
D	Не використовуються

<u>Запитання 22</u>	Для якого рівня охорони у плані охорони судна повинні бути встановлені заходи з охорони, що підлягають застосуванню в районах обмеженого доступу, які можуть уключати встановлення районів обмеженого доступу, що примикають до місць доступу:
A	1
B	2
C	3
D	Не використовуються

<u>Запитання 23</u>	Для якого рівня охорони у плані охорони судна повинні бути встановлені заходи з охорони, що підлягають застосуванню в районах обмеженого доступу, які можуть уключати виділення додаткового персоналу для охорони й обходу місць обмеженого доступу:
A	1
B	2
C	3
D	Не використовуються

<u>Запитання 24</u>	Визначення вразливих місць споруд, систем захисту персоналу, процесів або інших областей, де можливий інцидент, пов'язаний з охороною може не включати розгляд:
A	Доступу до портового засобу й суден, ошвартованих у портовому засобі, з боку води й з боку берега
B	Заходів із захисту устаткування радіозв'язку й інших видів зв'язку, портових і комунальних служб, зокрема комп'ютерних систем і мереж
C	Відомості про відповідальну особу, зокрема інформацію для зв'язку з нею у будь-який час доби
D	Існуючих угод з приватними охоронними організаціями, що надають послуги з охорони на воді й на березі

<u>Запитання 25</u>	Хто є відповідальним за підготовку плану охорони портового засобу:
A	Договірний Уряд або його власник
B	Капітан порту (портового засобу)
C	Офіцер охорони портового засобу
D	Інша довірена особа (організація)

<u>Запитання 26</u>	Плани охорони портового засобу обов'язково повинні містити:
A	Роль і структура служби охорони портового засобу
B	Докладні відомості про службу охорони портового засобу
C	Процедури й практику захисту конфіденційної інформації з питань охорони, що зберігається в друкованій або електронній формі
D	Процедури з подання й оцінки доповідей про можливе порушення заходів з охорони або проблеми, пов'язані з охороною

<u>Запитання 27</u>	Для якого рівня охорони у плані охорони портового засобу повинні бути зазначені контрольні пункти, в яких можуть уживатися такі заходи з охорони як перевірка особи всіх людей, що бажають пройти на територію портового засобу з причини, пов'язаної з судном
A	1
B	2
C	3
D	Інший

<u>Запитання 28</u>	Для якого рівня охорони в плані охорони портового засобу повинні бути встановлені додаткові заходи з охорони, які можуть уключати обмеження кількості місць доступу на територію портового засобу й визначення тих із них, які повинні бути закриті
A	1
B	2
C	3
D	Інший

<u>Запитання 29</u>	Для якого рівня охорони портовий засіб повинен дотримуватися вказівок, що поступили від тих, хто вживає відповідних заходів у випадку виникнення інциденту, пов'язаного з охороною, або його загрози, та прийняти заходи можуть уключати управління рухом суден стосовно всього портового засобу або його частини:
A	1
B	2
C	3
D	Інший

<u>Запитання 30</u>	До районів обмеженого доступу в межах портового засобу можуть НЕ ВХОДИТИ
A	Місця в'їзду та стоянки транспортних засобів
B	Ділянки води, що безпосередньо примикають до судна
C	Ділянки завантаження, вивантаження або складування вантажу чи запасів
D	Місця посадки й висадки, зони очікування та обробки пасажирів і суднового персоналу
<u>Запитання 31</u>	Поправки до плану охорони портового засобу, що стосуються конкретних змін, які можуть корінним чином змінити прийнятий підхід до забезпечення охорони портового засобу, схвалюються
A	Договірним Урядом або від його імені
B	Страховою компанією (наприклад, Lloyd)
C	Капітаном порту (портового засобу)
D	Офіцером охорони портового засобу

<u>Запитання 32</u>	З яким інтервалом Договірні уряди надають Міжнародній морській організації переглянутий та доповнений перелік, у якому містяться усі ухвалені плани безпеки портової споруди для портових споруд, які розташовані у межах їх території, разом з даними про зону або зони, охоплені таким планом безпеки портової споруди
A	1
B	2
C	5
D	10

<u>Запитання 33</u>	Обов'язки та зобов'язання офіцера безпеки компанії включають, проте не обмежуються цим, наступне:
A	Всі вказані обов'язки
B	Надання рекомендацій щодо рівня загроз, на які ймовірно може наражатись судно, за використання відповідних оцінювань безпеки та іншу відповідну інформацію.
C	Забезпечення проведення оцінювань безпеки судна
D	Організація відповідних тренувань персоналу, який відповідає за безпеку судна

<u>Запитання 34</u>	Обов'язки та зобов'язання офіцера безпеки компанії включають, проте не обмежуються цим, наступне:
A	Організація початкових та наступних перевірок судна адміністрацією або визнаною організацією з безпеки
B	Забезпечення того, щоб впродовж внутрішніх перевірок, періодичних переглядів, інспекцій безпеки та перевірок відповідності належним чином виявлялися та усувалися будь-які недоліки та невідповідності
C	Всі вказані обов'язки
D	Забезпечення відповідності між вимогами безпеки та вимогами охорони

<u>Запитання 35</u>	Хто з офіційних осіб повинен забезпечити ефективну координацію та імплементацію планів безпеки судна, беручи участь у практичних тренувальних заходах, які проводяться з відповідними інтервалами, враховуючи настанову, передбачену Міжнародним кодексом безпеки суден та портових споруд
A	Офіцер безпеки судна
B	Офіцер безпеки компанії
C	Офіцер безпеки портової споруди
D	Інша офіційна особа

3.2.2. Модуль 1. Теорія захисту інформаційних ресурсів обмеженого доступу.

Здобувачі, які проходять випробування, повинні володіти знаннями та навичками розв'язання завдань за наступними темами:

<u>Запитання 1</u>	Модель матриці доступів HRU використовується для аналізу
A	системи захисту, що реалізує дискреційну політику безпеки
B	системи захисту, що реалізує мандатну політику безпеки
C	за однаковими алгоритмами системи захисту, що реалізує дискреційну або мандатну політику безпеки
D	за різними алгоритмами системи захисту, що реалізує дискреційну або мандатну політику безпеки

<u>Запитання 2</u>	В моделі матриці доступів HRU система захисту представляється
A	системою правил переходу системи з одного стану в інший вигляду if (умова, що не є обов'язковою) then (послідовність примітивних операторів)
B	кінцевим автоматом, що функціонує згідно із певними правилами переходу системи з одного стану в інший вигляду if (умова, що не є обов'язковою) then (послідовність примітивних операторів)
C	системою правил переходу системи з одного стану в інший вигляду if (умова, що є обов'язковою) then (послідовність примітивних або складених операторів)
D	кінцевим автоматом, що функціонує згідно із певними правилами переходу системи з одного стану в інший вигляду if (умова, що є обов'язковою) then (послідовність примітивних або складених операторів)

<u>Запитання 3</u>	В моделі матриці доступів HRU функціонування системи розглядається
A	як послідовність станів системи
B	як послідовність виконуваних операторів
C	тільки з точки зору змін в матриці доступів
D	як послідовність виконуваних правил

<u>Запитання 4</u>	В моделі матриці доступів HRU примітивними операторами є
A	«внести право», «видалити право», «створити суб'єкт», «створити об'єкт», «видалити суб'єкт», «видалити об'єкт»
B	«брати», «давати», «створити», «видалити»
C	read, write, reset
D	read, write, append, execute

<u>Запитання 5</u>	В моделі матриці доступів HRU перехід системи в новий стан відбувається
A	тільки при виконанні примітивного оператора
B	тільки при виконанні команди
C	при виконанні примітивного оператора або команди, в якій є дійсною хоча б одна умова
D	при виконанні примітивного оператора або команди, в якій є дійсними всі умови

<u>Запитання 6</u>	В моделі матриці доступів HRU система називається моноопераційною, якщо
A	система правил, за якою функціонує кінцевий автомат, містить лише одне правило
B	всі команди мають однакові умови виконання
C	всі команди при різних умовах виконують однакові дії
D	кожна команда виконує один примітивний оператор

<u>Запитання 7</u>	Алгоритм, який перевіряє чи є вихідний (початковий) стан моноопераційної системи безпечним для даного права на моделі матриці доступів HR
A	існує і передбачає перебір тільки тих послідовностей, які містять оператор «внести» і хоча б один оператор «створити суб'єкт»
B	існує і передбачає перебір тільки тих послідовностей, які містять оператор «внести» і максимум один оператор «створити суб'єкт»
C	існує і передбачає тотальний перебір всіх послідовностей команд з перевіркою кінцевого стану кожної з них на відсутність витоку даного права
D	не існує

<u>Запитання 8</u>	Алгоритм, який перевіряє чи є вихідний (початковий) стан довільної системи безпечним для даного права на моделі матриці доступів HR
A	існує і передбачає перебір тільки тих послідовностей, які містять оператор «внести» і хоча б один оператор «створити суб'єкт»
B	існує і передбачає перебір тільки тих послідовностей, які містять оператор «внести»
C	існує і передбачає тотальний перебір всіх послідовностей команд з перевіркою кінцевого стану кожної з них на відсутність витоку даного права
D	не існує

<u>Запитання 9</u>	Алгоритм, який перевіряє чи є вихідний (початковий) стан системи безпечним для даного права існує на моделі матриці доступів HR, якщо
A	система не містить операції «створити»
B	система не містить операції «видалити» і має тільки команди, умови яких складаються не більше, ніж з одного речення
C	система має скінченну множину суб'єктів
D	в усіх перелічених випадках

<u>Запитання 10</u>	Модель розповсюдження прав доступу Take-Grant використовується для аналізу
A	системи захисту, що реалізує дискреційну політику безпеки
B	системи захисту, що реалізує мандатну політику безпеки
C	системи захисту, що реалізує дискреційну політику безпеки, в класичному варіанті моделі і системи захисту, що реалізує дискреційну або мандатну політику безпеки, в розширеному варіанті моделі
D	за різними алгоритмами системи захисту, що реалізує дискреційну або мандатну політику безпеки

<u>Запитання 11</u>	В моделі розповсюдження прав доступу Take-Grant система захисту представляється
A	системою правил переходу системи з одного стану в інший вигляду if (умова, що не є обов'язковою) then (послідовність примітивних операторів)
B	графом доступів і системою правил його перетворення
C	сукупністю властивостей поточного стану системи і сукупністю прав доступу кожного суб'єкта до кожного об'єкта
D	сукупністю об'єктів, що мають право обробляти інформацію високого рівня доступу, сукупністю об'єктів, що мають право обробляти інформацію низького рівня доступу, і системою інформаційних потоків між об'єктами

<u>Запитання 12</u>	В моделі розповсюдження прав доступу Take-Grant функціонування системи розглядається
A	як послідовність графів доступу
B	як послідовність виконуваних правил
C	як послідовність виконуваних операторів
D	як сукупність послідовностей отримання санкціонованого і несанкціонованого доступу

<u>Запитання 13</u>	В класичній моделі розповсюдження прав доступу Take-Grant система правил перетворення графів доступу містить де-юре правила
A	«внести право», «видалити право», «створити суб'єкт», «створити об'єкт», «видалити суб'єкт», «видалити об'єкт»
B	«брати», «давати», «створити», «видалити»
C	read, write, reset
D	read, write, append, execute

<u>Запитання 14</u>	В класичній моделі розповсюдження прав доступу Take-Grant розглядаються
A	два права доступу (read, write) і шість правил де-факто перетворення графа доступів (post, spy, find, pass і два додаткових правила)
B	два права доступу (take, grant) і чотири правила де-юре перетворення графа доступу (take, grant, create, remove)
C	три права доступу (read, write, reset) і чотири правила де-факто перетворення графа доступів (post, spy, find, pass)
D	два права доступу (read, write) і чотири правила де-юре перетворення графа доступу (take, grant, create, remove)

<u>Запитання 15</u>	В моделі розповсюдження прав доступу Take-Grant при аналізі функціонування системи головна увага приділяється
A	визначенню умов, при яких в системі можливе розповсюдження прав доступу способом викрадення прав доступу
B	визначенню умов, при яких в системі не можливе розповсюдження прав доступу способом викрадення прав доступу
C	визначенню умов, при яких в системі не можливе розповсюдження прав доступу способом санкціонованого отримання прав доступу
D	визначенню умов, при яких в системі можливе розповсюдження прав доступу способами санкціонованого отримання прав доступу і викрадення прав доступу

<u>Запитання 16</u>	В моделі розповсюдження прав доступу Take-Grant при санкціонованому отриманні прав доступу
A	при передачі прав доступу кооперація суб'єктів системи, що приймають участь в цьому процесі, не можлива
B	при передачі прав доступу кооперація суб'єктів системи, що приймають участь в цьому процесі, можлива при заданих обмеженнях на кількість суб'єктів
C	при передачі прав доступу кооперація суб'єктів системи, що приймають участь в цьому процесі, можлива без обмежень
D	при передачі прав доступу кооперація суб'єктів системи, що приймають участь в цьому процесі, можлива при заданих обмеженнях на склад суб'єктів

<u>Запитання 17</u>	В моделі розповсюдження прав доступу Take-Grant санкціоноване отримання права доступу α суб'єктом x в тому випадку, коли граф доступів G_0 містить тільки вершини суб'єкти, можливе тоді і тільки тоді,
A	коли існує непорожня множина суб'єктів, кожен з яких може надати об'єкту право α , і суб'єкт x з'єднаний tg -шляхом з кожним таким суб'єктом
B	коли існує непорожня множина суб'єктів, кожен з яких може надати об'єкту право α , і жоден із суб'єктів системи не може видалити право α
C	коли існує множина суб'єктів, кожен з яких може надати об'єкту права, що у сукупності складають право α , і суб'єкт x з'єднаний tg -шляхом з кожним таким суб'єктом
D	коли існує непорожня множина об'єктів, кожен з яких може надати суб'єкту право α , і жоден із суб'єктів системи не може видалити право α

<u>Запитання 18</u>	В моделі розповсюдження прав доступу Take-Grant санкціоноване отримання права доступу α суб'єктом x у випадку довільного графу доступів G_0 можливе тоді і тільки тоді
A	коли існує непорожня множина суб'єктів, кожен з яких може надати об'єкту право α , і суб'єкт x з'єднаний tg -шляхом з кожним таким суб'єктом
B	коли існує непорожня множина об'єктів, кожен з яких може надати суб'єкту право α , і жоден із суб'єктів системи не може видалити право α
C	коли існують: - множина об'єктів, $s_i, i = \overline{1, m}$, кожен з яких може надавати права γ_i , що у сукупності складають право $\alpha = \bigcup_{i=1}^m \gamma_i$; - множина вершин-суб'єктів x'_i , з'єднаних з x початковими прольотами мосту; - множина вершин-суб'єктів s'_i , з'єднаних з s_i кінцевими прольотами мосту; - острови для кожної пари (x'_i, s'_i) , між якими наявні мости, причому x'_i і s'_i належать різним островам
D	коли існує множина суб'єктів, кожен з яких може надати об'єкту права, що у сукупності складають право α , і суб'єкт x з'єднаний tg -шляхом з кожним таким суб'єктом

<u>Запитання 19</u>	В моделі розповсюдження прав доступу Take-Grant несанкціоноване отримання права доступу α суб'єктом x у випадку довільного графу доступів G_0 можливе тоді і тільки тоді
A	коли: - існує множина об'єктів, $s_i, i = \overline{1, m}$, кожен з яких може надавати права γ_i , що у сукупності складають право $\alpha = \bigcup_{i=1}^m \gamma_i$; - за початковим графом доступів суб'єкт x може отримати права доступу α
B	коли: - існує множина об'єктів, $s_i, i = \overline{1, m}$, кожен з яких може надавати права γ_i , що у сукупності складають право $\alpha = \bigcup_{i=1}^m \gamma_i$; - за початковим графом доступів суб'єкт x не може отримати права доступу α , але існує така послідовність перетворень початкового графа доступів, що від s_i права доступу γ_i отримують інші об'єкти, з'єднані з x tg -шляхами
C	коли існують: - множина об'єктів, $s_i, i = \overline{1, m}$ кожен з яких може надавати права γ_i , що у сукупності складають право $\alpha = \bigcup_{i=1}^m \gamma_i$; - множина вершин-суб'єктів x'_i , з'єднаних з x початковими прольотами мосту; - множина вершин-суб'єктів s'_i , з'єднаних з s_i кінцевими прольотами мосту; - острови для кожної пари (x'_i, s'_i) , між якими наявні мости, причому x'_i і s'_i належать різним островам
D	коли: - існує множина об'єктів, $s_i, i = \overline{1, m}$, кожен з яких може надавати право доступу α ; - за початковим графом доступів суб'єкт x не може отримати права доступу α , але існує така послідовність перетворень початкового графа доступів, що від s_i право доступу α отримують інші об'єкти, хоча б один з яких з'єднаний з x tg -шляхом

<u>Запитання 20</u>	В розширеній моделі розповсюдження прав доступу Take-Grant розглядаються
A	два права доступу (read, write) і шість правил де-факто перетворення графа доступів (post, spy, find, pass і два додаткових правила)
B	два права доступу (take, grant) і чотири правила де-юре перетворення графа доступів (take, grant, create, remove)
C	три права доступу (read, write, reset) і чотири правила де-факто перетворення графа доступів (post, spy, find, pass)
D	два права доступу (read, write) і чотири правила де-юре перетворення графа доступів (take, grant, create, remove)

<u>Запитання 21</u>	Визначити вартість розповсюдження прав доступу або інформації можна
A	за класичною моделлю Take-Grant
B	за розширеною моделлю Take-Grant
C	за моделлю матриці доступів HRU
D	за всіма переліченими моделями

<u>Запитання 22</u>	Визначити ймовірність розповсюдження прав доступу або інформації можна
A	за класичною моделлю Take-Grant
B	за розширеною моделлю Take-Grant
C	за моделлю матриці доступів HRU
D	за всіма переліченими моделями

<u>Запитання 23</u>	При визначенні вартості або ймовірності розповсюдження прав доступу чи інформації за розширеною моделлю розповсюдження прав доступу Take-Grant враховують, що шляхам найменшої вартості
A	відповідає найбільша ймовірність
B	відповідає найменша ймовірність
C	відповідає середня ймовірність
D	відповідає найбільша або найменша ймовірність в залежності від прийнятої моделі порушника

<u>Запитання 24</u>	При визначенні вартості або ймовірності розповсюдження прав доступу чи інформації за розширеною моделлю розповсюдження прав доступу Take-Grant вартість шляху розповсюдження може визначатися
A	як сума вартостей пройдених дуг
B	як сума вартостей правил де-юре, що спрацювали
C	як сума вартостей правил де-факто, що спрацювали
D	в залежності від обраного підходу як сума вартостей пройдених дуг або як сума вартостей правил де-юре і де-факто, що спрацювали

<u>Запитання 25</u>	При визначенні вартості або ймовірності розповсюдження прав доступу чи інформації за розширеною моделлю розповсюдження прав доступу Take-Grant вартість правила може
A	бути константою
B	залежати від специфіки правила
C	залежати від кількості учасників при застосуванні правила або від ступеня необхідної взаємодії об'єктів
D	усі відповіді вірні

<u>Запитання 26</u>	В реальних системах суб'єкти найчастіше використовують права
A	take, grant
B	create, remove
C	read, write
D	усі відповіді вірні

<u>Запитання 27</u>	Класична модель Белла-Лападула призначена для аналізу
A	системи захисту, що реалізує дискреційну політику безпеки
B	системи захисту, що реалізує мандатну політику безпеки
C	за однаковими алгоритмами системи захисту, що реалізує дискреційну або мандатну політику безпеки
D	за різними алгоритмами системи захисту, що реалізує дискреційну або мандатну політику безпеки

<u>Запитання 28</u>	За моделлю Белла-Лападула безпечність системи визначається за допомогою
A	властивості простої безпеки ss
B	властивості «*»
C	властивості дискретної безпеки ds
D	усіх трьох властивостей

<u>Запитання 29</u>	За моделлю Белла-Лападула система вважається безпечною, якщо вона
A	в певний термін часу володіє хоча б однією з властивостей ss, *, ds
B	одночасно володіє властивостями ss і ds
C	одночасно володіє властивостями ss, *, ds
D	має властивість «*»

<u>Запитання 30</u>	За базовою теоремою безпеки система вважається безпечною, якщо
A	початковий стан системи є безпечним і множина дій системи має властивості ss, *, ds одночасно
B	незалежно від початкового стану множина дій системи має властивості ss, *, ds одночасно
C	її можна певною послідовністю дій привести до безпечного стану
D	початковий стан системи є безпечним

<u>Запитання 31</u>	При визначенні безпечності за підходом Read-Write в моделі системи Белла-Лападула
A	система вважається безпечною для початкового безпечного стану тоді і тільки тоді, коли вона має властивості ss і * для будь-якого початкового стану
B	система вважається безпечною для початкового безпечного стану тоді і тільки тоді, коли вона має властивості ss і ds для будь-якого початкового стану
C	суб'єкт може стати каналом витоку інформації зверху до низу
D	усі відповіді вірні

<u>Запитання 32</u>	При визначенні безпечності за підходом Transaction в моделі системи Белла-Лападула
A	система вважається безпечною, якщо її функція переходу має властивість ss
B	система є безпечною для початкового безпечного стану, її функція переходу безпечна
C	система є безпечною для будь-якого початкового стану, якщо її функція переходу безпечна
D	система вважається безпечною, якщо її функція переходу має властивість *

<u>Запитання 33</u>	При визначенні безпечності за підходом Transaction в моделі системи Белла-Лападула можна розглядати випадки,
A	коли всі суб'єкти можуть змінювати рівні безпеки
B	ніхто не може змінювати рівні безпеки
C	тільки системний адміністратор може змінювати рівні безпеки
D	усі відповіді вірні

<u>Запитання 34</u>	При визначенні безпечності за підходом Transaction в моделі системи Белла-Лападула на функцію переходів
A	накладається одна додаткова умова: за один крок роботи системи вноситься серія змін тільки в один з параметрів, а інші параметри залишаються незмінними
B	накладається одна додаткова умова: за один крок роботи системи вносяться тільки однакові зміни в окремі параметри, а інші параметри залишаються незмінними
C	накладається одна додаткова умова: за один крок роботи системи вноситься тільки одна зміна в один з параметрів, а інші параметри залишаються незмінними
D	додаткові умови не накладаються

<u>Запитання 35</u>	Моделі Low-Water-Mark призначена для аналізу
A	системи захисту, що реалізує дискреційну політику безпеки
B	системи захисту, що реалізує мандатну політику безпеки
C	за однаковими алгоритмами системи захисту, що реалізує дискреційну або мандатну політику безпеки
D	за різними алгоритмами системи захисту, що реалізує дискреційну або мандатну політику безпеки

<u>Запитання 36</u>	Згідно з моделлю Low-Water-Mark при безпечному функціонуванні системи за запитом суб'єкта на запис в об'єкт
A	йому надається доступ, якщо рівень секретності об'єкта відповідає рівню доступу суб'єкта
B	йому завжди надається доступ, і рівень секретності об'єкта при цьому залишається незмінним
C	йому завжди надається доступ, але в результаті виконання операції write рівень секретності об'єкта встановлюється рівним рівню доступу суб'єкта і, якщо рівень секретності об'єкта знижується, то вся інформація в об'єкті стирається
D	йому надається доступ, якщо різниця між рівнем секретності об'єкта і рівнем доступу суб'єкта не перевищує задану величину

<u>Запитання 37</u>	Моделі інформаційних потоків призначена для аналізу
A	системи захисту, що реалізує дискреційну політику безпеки
B	системи захисту, що реалізує мандатну політику безпеки
C	за однаковими алгоритмами системи захисту, що реалізує дискреційну або мандатну політику безпеки
D	за різними алгоритмами системи захисту, що реалізує дискреційну або мандатну політику безпеки

<u>Запитання 38</u>	Безпека інформаційних потоків може бути визначена на основі наступних підходів
A	інформаційного невтручання, інформаційного невиведення
B	інформаційної стабільності
C	інформаційної незалежності
D	усі відповіді вірні

<u>Запитання 39</u>	Згідно з моделлю інформаційних потоків система безпечна з точки зору інформаційного невиведення, якщо
A	в ній відсутні інформаційні потоки від низькорівневих до високорівневих об'єктів
B	в ній відсутні інформаційні потоки від високорівневих до низькорівневих об'єктів
C	низькорівневі об'єкти не мають змоги накопичувати нову інформацію про значення параметрів високорівневих об'єктів
D	низькорівневі об'єкти не мають змоги отримувати інформацію про попередні значення параметрів високорівневих об'єктів

<u>Запитання 40</u>	Згідно з моделлю інформаційних потоків система безпечна з точки зору інформаційного невтручання, якщо
A	в ній відсутні інформаційні потоки від низькорівневих до високорівневих об'єктів
B	в ній відсутні інформаційні потоки від високорівневих до низькорівневих об'єктів
C	низькорівневі об'єкти не мають змоги накопичувати нову інформацію про значення параметрів високорівневих об'єктів
D	низькорівневі об'єкти не мають змоги отримувати інформацію про попередні значення параметрів високорівневих об'єктів

<u>Запитання 41</u>	Автоматна модель системи захисту GM призначена для аналізу
A	системи захисту, що реалізує дискреційну політику безпеки
B	системи захисту, що реалізує мандатну політику безпеки
C	за однаковими алгоритмами системи захисту, що реалізує дискреційну або мандатну політику безпеки
D	за різними алгоритмами системи захисту, що реалізує дискреційну або мандатну політику безпеки

<u>Запитання 42</u>	В автоматній моделі GM система захисту представляється
A	детермінованим автоматом, на вхід якого надходять команди користувачів, для кожного з яких задана функція виходів, яка визначає, що кожен з них «бачить» на пристрої виводу у відповідному стані системи
B	кінцевим автоматом, що функціонує згідно із певними правилами переходу системи з одного стану в інший вигляду if (умова, що не є обов'язковою) then (послідовність примітивних операторів)
C	системою правил переходу системи з одного стану в інший вигляду if (умова, що є обов'язковою) then (послідовність примітивних або складених операторів)
D	кінцевим автоматом, що функціонує згідно із певними правилами переходу системи з одного стану в інший вигляду if (умова, що є обов'язковою) then (послідовність примітивних або складених операторів)

<u>Запитання 43</u>	В автоматній моделі GM використовуються
A	чотири об'єкта – високорівневі і низькорівневі порти входу та виходу
B	два об'єкта - порти входу та виходу
C	п'ять об'єктів – високорівневі і низькорівневі порти входу та виходу і порт управління
D	об'єкти у будь-якій кількості

<u>Запитання 44</u>	В автоматній моделі GM функціонування системи представляється
A	як послідовність станів системи
B	як послідовність подій (high-in, high-out, low-in, low-out) кожна з яких має власну ймовірність
C	як послідовність виконуваних операторів
D	як послідовність виконуваних правил

<u>Запитання 45</u>	В автоматній моделі GM система має властивість інформаційного невтручання, якщо
A	$p(\text{low-out}_t \text{high-in}_s, \text{low-out}_s) = p(\text{high-out}_t \text{high-out}_s)$, де $s, t=0, 1, 2$ і $s < t$, p - ймовірність
B	$p(\text{low-out}_t \text{high-in}_s, \text{low-out}_s) = p(\text{low-out}_t \text{low-out}_s)$, де $s, t=0, 1, 2$ і $s > t$, p - ймовірність
C	$p(\text{low-out}_t \text{high-in}_s, \text{low-out}_s) = p(\text{low-out}_t \text{low-out}_s)$, де $s, t=0, 1, 2$ і $s < t$, p - ймовірність
D	$p(\text{high-out}_t \text{low-in}_s, \text{low-out}_s) = p(\text{high-out}_t \text{high-out}_s)$, де $s, t=0, 1, 2$ і $s < t$, p - ймовірність

<u>Запитання 46</u>	В автоматній моделі GM система з вихідною функцією $out(u, l)$, значення якої генеруються для користувача u в залежності від вхідної історії (послідовності команд користувачів) l , має властивість інформаційного невтручання, якщо
A	виконується нерівність $out(u, l) < out(u, l^*)$, де $l^* \in l$ з відкинутими командами користувачів, чий рівень безпеки вищий, ніж у u
B	виконується нерівність $out(u, l) > out(u, l^*)$, де $l^* \in l$ з відкинутими командами користувачів, чий рівень безпеки вищий, ніж у u
C	виконується рівність $out(u, l) = out(u, l^*)$, де $l^* \in l$ з відкинутими командами користувачів, чий рівень безпеки нижчий, ніж у u
D	виконується рівність $out(u, l) = out(u, l^*)$, де $l^* \in l$ з відкинутими командами користувачів, чий рівень безпеки вищий, ніж у u

<u>Запитання 47</u>	Домен безпеки - це
A	сукупність об'єктів, до яких дозволено доступ конкретному суб'єкту
B	сукупність об'єктів системи, що мають найвищий рівень безпеки
C	сукупність суб'єктів системи, що мають найвищий рівень безпеки
D	сукупність об'єктів і суб'єктів системи, що мають найвищий рівень безпеки, і зв'язків між ними

<u>Запитання 48</u>	Суб'єкт доступу - це
A	користувачі системи
B	персонал, що забезпечує захист інформації в системі
C	активні програми і процеси
D	особа, що надає права доступу

<u>Запитання 49</u>	При аналізі захисту автоматизованих систем рівні доступу поділяються на
A	рівень конфіденційності, рівень цілісності, рівень доступності, рівень спостереженості
B	рівень носіїв інформації, рівень засобів взаємодії з носіями інформації, рівень представлення інформації, рівень змісту інформації
C	фізичний рівень, каналний рівень, мережний рівень, транспортний рівень, сеансів рівень, рівень відображення, прикладний рівень
D	початковий рівень, впевнений користувач, досвідчений користувач, програміст, адміністратор мережі

<u>Запитання 50</u>	Основними поняттями моделі контролю цілісності Кларка-Вілсона є
A	множина об'єктів легального доступу, множина об'єктів обмеженого доступу, множина легітимних користувачів, множина дозволених процедур перетворення даних, множина дозволених перетворень процедур перетворення даних
B	транзакції, користувачі, аудит подій, контроль об'єктів, розмежування функцій, автентифікація користувачів, мінімізація привілеїв, шість правил перетворення даних
C	множина контрольованих елементів даних, множина неконтрольованих елементів даних, множина процедур контролю цілісності, множина процедур перетворення, дев'ять правил, що визначають взаємовідношення елементів даних і процедур
D	дані, що не підлягають захисту; дані, що підлягають захисту; «чорний список», «білий список»; вільно доступні дії; дії, на які слід отримувати дозвіл; правила, що регламентують процедури отримання доступу користувачами і правила, що регламентують процедури присвоєння об'єктам певного рівня секретності

3.3. Розділ третій

Розділ третій кваліфікаційного екзамену, на здобуття ступеня вищої освіти магістр складається з завдань дисципліни «Моделювання та оптимізації об'єктів і процесів захисту інформації».

Мета вивчення дисципліни - оволодіння теоретичними методами і практичними методиками моделювання та оптимізації процесів в системах технічного захисту інформації.

Предметом навчальної дисципліни є методологія моделювання та оптимізації комплексних систем захисту інформації та їх складових.

<u>Запитання 1</u>	Метод моделювання при якому система описується за допомогою набору алгебраїчних, диференціальних, логічних рівнянь, що задають зв'язок між різними (зазвичай – числовими) характеристиками системи, а також параметрами навколишнього середовища називається:
A	імітаційне моделювання;
B	аналітичне моделювання;
C	фізичне моделювання;
D	натурне моделювання.

<u>Запитання 2</u>	Метод моделювання при якому активно використовується генератор випадкових чисел, на основі результатів роботи якого виникають певні події в системі, процеси взаємодії у якій (тобто процеси роботи системи) описуються набором алгебраїчних, диференціальних, логічних рівнянь називається:
A	імітаційне моделювання;
B	аналітичне моделювання;
C	фізичне моделювання;
D	натурне моделювання.

<u>Запитання 3</u>	Метод моделювання при якому у вигляді реально існуючої моделі, створеної із матеріальних компонентів, відтворюється об'єкт моделювання чи його частина (залежно від предметної галузі) називається:
A	імітаційне моделювання;
B	аналітичне моделювання;
C	фізичне моделювання;
D	натурне моделювання.

<u>Запитання 4</u>	При аналітичному моделюванні усталений (стаціонарний) стан системи у найбільш загальному випадку описується за допомогою:
A	набору алгебраїчних рівнянь;
B	набору алгебраїчних та диференціальних рівнянь;
C	набору диференціальних рівнянь;
D	текстового аналітичного опису компонентів системи.

<u>Запитання 5</u>	При аналітичному моделюванні перехідний (динамічний) стан системи у найбільш загальному випадку описується за допомогою:
A	набору алгебраїчних рівнянь;
B	набору алгебраїчних та диференціальних рівнянь;
C	набору диференціальних рівнянь;
D	текстового аналітичного опису компонентів системи.

<u>Запитання 6</u>	При аналітичному моделюванні динамічних систем вид розв'язку диференціального рівняння (чи системи таких рівнянь) залежить:
A	тільки, і тільки від структури (виду) самого диференціального рівняння;
B	від початкових умов диференціального рівняння та інших факторів;
C	від значення числових параметрів (коефіцієнтів) диференціального рівняння та інших факторів;
D	тільки, і тільки від граничних умов диференціального рівняння.

Запитання 7	Який метод не застосовується при вирішенні задач однокритеріальної оптимізації:
A	графічний метод розв'язку задач лінійного програмування;
B	симплекс-метод;
C	знаходження та аналіз критичних точок цільової функції;
D	метод бульбашки.

Запитання 8	Який підхід не використовується при вирішенні задач багатокритеріальної оптимізації:
A	розробка лексикографічного порядку окремих критеріїв;
B	перехід до однокритеріальної задачі на основі застосування міркувань адитивної корисності (розрахунком зваженої суми частинних критеріїв один з одним);
C	перехід до однокритеріальної задачі на основі застосування міркувань мультиплікативної корисності (розрахунком зваженого добутку частинних критеріїв один з одним);
D	перехід до однокритеріальної задачі на основі застосування міркувань дивергентної корисності (розрахунком зваженої частки від ділення частинних критеріїв один на один).

Запитання 9	Якщо у матричній моделі розподіленої атаки на відмову в обслуговуванні (DDoS) матриця $A = (a_{ij})$ задає кількість запитів, відправлених з i -того атакуючого комп'ютера на j -тий обслуговуючий пристрій атакованого кластеру, то чому буде дорівнювати число $\sum_{i=1}^m a_{ij}$:
A	загальній кількості запитів, надісланих з i -того атакуючого комп'ютера на кластер в цілому;
B	загальній кількості запитів, що надійшли на j -тий обслуговуючий пристрій кластеру;
C	загальній кількості запитів, що були відправлені усіма атакуючими комп'ютерами;
D	загальній кількості запитів, що надійшли на усі обслуговуючі пристрої кластеру в цілому.

Запитання 10	Якщо у матричній моделі розподіленої атаки на відмову в обслуговуванні (DDoS) матриця $A = (a_{ij})$ задає кількість запитів, відправлених з i -того атакуючого комп'ютера на j -тий обслуговуючий пристрій атакованого кластеру, то чому буде дорівнювати число $\sum_{j=1}^n a_{ij}$:
A	загальній кількості запитів, надісланих з i -того атакуючого комп'ютера на кластер в цілому;
B	загальній кількості запитів, що надійшли на j -тий обслуговуючий пристрій кластеру;
C	загальній кількості запитів, що були відправлені усіма атакуючими комп'ютерами;
D	загальній кількості запитів, що надійшли на усі обслуговуючі пристрої кластеру в цілому.

Запитання 11	Якщо у матричній моделі розподіленої атаки на відмову в обслуговуванні (DDoS) матриця $A = (a_{ij})$ задає кількість запитів, відправлених з i -того атакуючого комп'ютера на j -тий обслуговуючий пристрій атакованого кластеру, то чому буде дорівнювати число $\sum_{i=1}^m \sum_{j=1}^n a_{ij}$:
A	загальній кількості запитів, надісланих з i -того атакуючого комп'ютера на кластер в цілому;
B	загальній кількості запитів, що надійшли на j -тий обслуговуючий пристрій кластеру;
C	загальній кількості запитів, що були відправлені усіма атакуючими комп'ютерами;
D	загальній кількості запитів, що були відправлені з i -того атакуючого комп'ютера на j -тий обслуговуючий пристрій кластеру.

<u>Запитання 12</u>	Якщо у матричній моделі розподіленої атаки на відмову в обслуговуванні (DDoS) матриця $A = (a_{ij})$ задає кількість запитів, відправлених з i -того атакуючого комп'ютера на j -тий обслуговуючий пристрій атакованого кластеру, а $T = (t_i)$ – матриця-рядок кількостей операцій t_i , необхідних для обробки одного запиту від i -того атакуючого пристрою (мається на увазі, що на різних атакуючих комп'ютерах можуть бути встановлені різні версії атакуючого програмного забезпечення), то добуток $P = T \cdot A$:
A	рівний кількості операцій p , необхідних для обробки кластером усіх відправлених на нього запитів;
B	рівний матриці-рядку кількостей операцій p_j , що необхідно виконати кожному j -тому обслуговуючому пристрою атакованого кластеру для обробки усіх запитів, що на цей пристрій надійшли;
C	рівний матриці-стовпцю кількостей операцій p_j , що були виконані i -тим атакуючим комп'ютером;
D	не існує, а визначений зміст має добуток $A \cdot T$.

<u>Запитання 13</u>	Якщо у матричній моделі розподіленої атаки на відмову в обслуговуванні (DDoS) матриця $A = (a_{ij})$ задає кількість запитів, відправлених з i -того атакуючого комп'ютера на j -тий обслуговуючий пристрій атакованого кластеру, а $T = (t_i)$ – матриця-рядок кількостей операцій t_i , необхідних для обробки одного запиту від i -того атакуючого пристрою (мається на увазі, що на різних атакуючих комп'ютерах можуть бути встановлені різні версії атакуючого програмного забезпечення), то добуток $P = A \cdot T$:
A	рівний кількості операцій p , необхідних для обробки кластером усіх відправлених на нього запитів;
B	рівний матриці-рядку кількостей операцій p_j , що необхідно виконати кожному j -тому обслуговуючому пристрою атакованого кластеру для обробки усіх запитів, що на цей пристрій надійшли;
C	рівний матриці-стовпцю кількостей операцій p_j , що були виконані i -тим атакуючим комп'ютером;
D	не існує, а визначений зміст має добуток $T \cdot A$.

<u>Запитання 14</u>	Якщо у матричній моделі розподіленої атаки на відмову в обслуговуванні (DDoS) матриця $A = (a_{ij})$ задає кількість запитів, відправлених з i -того атакуючого комп'ютера на j -тий обслуговуючий пристрій атакованого кластеру, а $T = (t_i)$ – матриця-рядок кількостей операцій t_i , необхідних для обробки одного запиту від i -того атакуючого пристрою (мається на увазі, що на різних атакуючих комп'ютерах можуть бути встановлені різні версії атакуючого програмного забезпечення), то для добутку $P = T \cdot A$ сума $\sum_{j=1}^n p_j$ буде рівною:
A	кількості операцій p , необхідних для обробки кластером усіх відправлених на нього запитів;
B	кількості операцій p_j , що необхідно виконати j -тому обслуговуючому пристрою атакованого кластеру для обробки усіх запитів, що на цей пристрій надійшли;
C	кількості операцій p_j , що були виконані i -тим атакуючим комп'ютером;
D	вказаний добуток матриць не існує, а визначений зміст має добуток $A \cdot T$.

<u>Запитання 15</u>	Вкажіть тип графу, що відповідає моделі системи захисту інформації:	
A	Орієнтований граф;	
B	Неорієнтований граф;	
C	Мішаний граф;	
D	Не всюди зв'язний граф.	

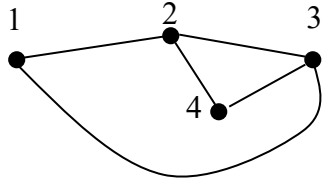
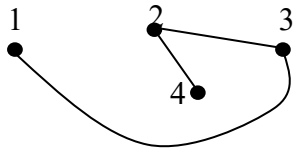
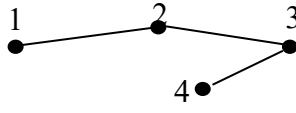
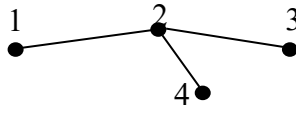
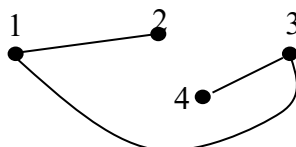
<u>Запитання 16</u>	У графівій моделі системи захисту інформації, наведений на рисунку, матриця суміжності матиме вид:	
A	$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix};$	
B	$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix};$	
C	$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix};$	
D	$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$	

<u>Запитання 17</u>	У графівій моделі системи захисту інформації, наведений на рисунку, матриця інцидентності матиме вид (тут «1» означає те ж саме, що « ± 1 »):	
A	$\begin{pmatrix} +1 & 0 & 0 & 0 & 1 \\ +1 & +1 & 1 & 0 & 0 \\ 0 & +1 & 0 & +1 & 1 \\ 0 & 0 & 1 & +1 & 0 \end{pmatrix};$	
B	$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix};$	
C	$\begin{pmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix};$	
D	$\begin{pmatrix} +1 & 0 & 0 & 0 & 1 \\ -1 & +1 & 1 & 0 & 0 \\ 0 & -1 & 0 & -1 & 1 \\ 0 & 0 & 1 & +1 & 0 \end{pmatrix}.$	

<u>Запитання 18</u>	У графівій моделі системи захисту інформації, наведений на рисунку, матриця суміжності матиме вид:	
A	$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix};$	
B	$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix};$	
C	$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix};$	
D	$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$	

<u>Запитання 19</u>	Вкажіть тип графу, що відповідає моделі системи захисту інформації:	
A	Орієнтований граф;	
B	Неорієнтований граф;	
C	Мішаний граф;	
D	Не всюди зв'язний граф.	

<u>Запитання 20</u>	Графова модель системи захисту інформації наведена на рисунку, причому матриця суміжності містить ваги відповідних ребер. Виберіть екстремальне (що відповідає мінімуму) дерево даного графу:	 $\begin{pmatrix} 0 & 2 & 7 & 0 \\ 2 & 0 & 3 & 5 \\ 7 & 3 & 0 & 10 \\ 0 & 5 & 10 & 0 \end{pmatrix}$
A		
B		
C		
D		

Запитання 21	Графова модель системи захисту інформації наведена на рисунку, причому матриця суміжності містить ваги відповідних ребер. Виберіть екстремальне (що відповідає мінімуму) дерево даного графу:	 $\begin{pmatrix} 0 & 5 & 2 & 0 \\ 5 & 0 & 1 & 2 \\ 2 & 1 & 0 & 3 \\ 0 & 2 & 3 & 0 \end{pmatrix}$
A		
B		
C		
D		

Запитання 22	Марковським називається процес:
A	у якому наступний стан об'єкта залежить тільки від історії переходу об'єкта у поточний стан;
B	у якому наступний стан об'єкта залежить тільки від поточного стану об'єкта;
C	у якому наступний стан об'єкта залежить як від поточного стану об'єкта, так і від історії переходу об'єкта у поточний стан;
D	у якому послідовність переходів між станами є детермінованим процесом.

Запитання 23	У системі масового обслуговування реалізується процес:
A	у якому наступний стан об'єкта залежить тільки від історії переходу об'єкта у поточний стан;
B	у якому наступний стан об'єкта залежить тільки від поточного стану об'єкта;
C	у якому наступний стан об'єкта залежить як від поточного стану об'єкта, так і від історії переходу об'єкта у поточний стан;
D	у якому послідовність переходів між станами є детермінованим процесом.

Запитання 24	Оберіть не існуючий тип системи масового обслуговування:
A	із втратами (тобто з відмовами), без черги;
B	із втратами (тобто з відмовами), зі скінченною чергою;
C	із втратами (тобто з відмовами), з нескінченною чергою;
D	із очікуванням та нескінченною чергою.

Запитання 25	Виконати повне дослідження системи масового обслуговування означає знайти:
A	часові залежності ймовірностей усіх її допустимих станів;
B	значення ймовірностей усіх її допустимих станів у стаціонарному режимі;
C	і описати вербально усі її допустимі стани;
D	значення інтенсивностей, що відповідають усім допустимим переходам між станами системи.

Запитання 26	Шуканими величинами у спрощеному варіанті системи рівнянь Колмогорова, що описує систему масового обслуговування, а саме, коли усі похідні замінені нулями, шуканими величинами є:
A	часові залежності ймовірностей усіх її допустимих станів;
B	значення ймовірностей усіх її допустимих станів у стаціонарному режимі;
C	символьні назви усіх допустимих станів;
D	значення інтенсивностей, що відповідають усім допустимим переходам між станами системи.

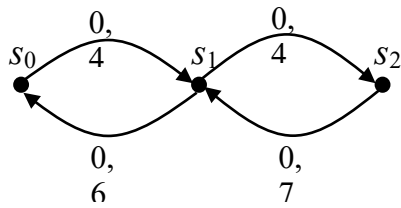
Запитання 27	Для системи масового обслуговування, зображеної графом, оберіть правильний запис системи рівнянь Колмогорова для стаціонарного режиму (без урахування умови нормування):	
A	$\begin{cases} -0,4p_0 + 0,6p_1 = 0 \\ 0,4p_0 - p_1 + 0,7p_2 = 0; \\ 0,4p_1 - 0,7p_2 = 0 \end{cases}$	
B	$\begin{cases} -0,4p_0 + 0,6p_1 = \frac{dp_0}{dt}; \\ 0,4p_0 - p_1 + 0,7p_2 = \frac{dp_1}{dt} \\ 0,4p_1 - 0,7p_2 = \frac{dp_2}{dt} \end{cases}$	
C	$\begin{cases} -0,4p_0 + 0,6p_1 = p_0 \\ 0,4p_0 - p_1 + 0,7p_2 = p_1; \\ 0,4p_1 - 0,7p_2 = p_2 \end{cases}$	
D	$\begin{cases} -0,4p_0 + 0,6p_1 = p_2 \\ 0,4p_0 - p_1 + 0,7p_2 = p_1 \cdot \\ 0,4p_1 - 0,7p_2 = p_0 \end{cases}$	

Запитання 28	Для системи масового обслуговування, зображеної графом, оберіть правильний запис повної системи рівнянь Колмогорова (без урахування умови нормування):	
A	$\begin{cases} -0,4p_0 + 0,6p_1 = 0 \\ 0,4p_0 - p_1 + 0,7p_2 = 0; \\ 0,4p_1 - 0,7p_2 = 0 \end{cases}$	
B	$\begin{cases} -0,4p_0 + 0,6p_1 = \frac{dp_0}{dt} \\ 0,4p_0 - p_1 + 0,7p_2 = \frac{dp_1}{dt}; \\ 0,4p_1 - 0,7p_2 = \frac{dp_2}{dt} \end{cases}$	
C	$\begin{cases} -0,4p_0 + 0,6p_1 = p_0 \\ 0,4p_0 - p_1 + 0,7p_2 = p_1; \\ 0,4p_1 - 0,7p_2 = p_2 \end{cases}$	
D	$\begin{cases} -0,4p_0 + 0,6p_1 = p_2 \\ 0,4p_0 - p_1 + 0,7p_2 = p_1 \cdot \\ 0,4p_1 - 0,7p_2 = p_0 \end{cases}$	

Запитання 29	Для системи масового обслуговування, зображеної графом, розв'яжіть систему рівнянь Колмогорова для стаціонарного режиму (включіть до неї умову нормування та виключіть зайві рівняння):	
A	$\begin{cases} p_0 = \frac{4}{43} \\ p_1 = \frac{17}{43} \\ p_2 = \frac{22}{43} \end{cases}$	
B	$\begin{cases} p_0 = \frac{2}{43} \\ p_1 = \frac{18}{43} \\ p_2 = \frac{25}{43} \end{cases}$	
C	$\begin{cases} p_0 = 0,535 \\ p_1 = 0,257 \\ p_2 = 0,208 \end{cases}$	
D	$\begin{cases} p_0 = \frac{21}{43} \\ p_1 = \frac{14}{43} \\ p_2 = \frac{8}{43} \end{cases}$	

Запитання 30	Чи можна за даним графом системи масового обслуговування встановити кількість обслуговуючих пристроїв у ній (тут s_0 – вільний стан):	
A	так, у ній 1 обслуговуючий пристрій;	
B	так, у ній 2 обслуговуючих пристроїв;	
C	так, у ній 3 обслуговуючих пристроїв;	
D	ні, на графі приведено замало інформації для відповіді на поставлене питання.	

Запитання 31	Оберіть правильне твердження про систему масового обслуговування на основі її графу (тут s_0 – вільний стан):	
A	це система масового обслуговування без добровільних відмов у обслуговуванні;	
B	усі запити, що направляються до цієї системи масового обслуговування після проходження певного інтервалу часу обов'язково обробляються;	
C	інтенсивність добровільних відмов складає 0,1 запитів/од. часу;	
D	серед попередніх пунктів правильних тверджень немає.	

Запитання 32	Визначте тип системи масового обслуговування на основі її графу:	
A	система масового обслуговування без відмов;	
B	система масового обслуговування із чергою довжиною 1;	
D	система масового обслуговування без добровільних відмов від обслуговування.	

Запитання 33	Процес визначення функціональної залежності, яка найкраще відповідає експериментальним даним називається:
A	інтерполяція;
B	екстраполяція;
C	апроксимація;
D	регресія.

Запитання 34	Процес встановлення зв'язку (впливу) однієї величини (або кількох величин) на іншу називається:
A	інтерполяція;
B	екстраполяція;
C	апроксимація;
D	регресія.

Запитання 35	Дослідження впливу однієї величини на іншу, встановлення їх зв'язку називається:
A	лінійною регресією;
B	нелінійною регресією;
C	одновимірною (парною) регресією;
D	багатовимірною (множинною) регресією.

Запитання 36	Дослідження впливу двох заданих величин на третю, встановлення їх зв'язку називається:
A	лінійною регресією;
B	нелінійною регресією;
C	одновимірною (парною) регресією;
D	багатовимірною (множинною) регресією.

Запитання 37	За умови, що зв'язок між двома величинами описується формулою $y = ax + b$, сам зв'язок найбільш повно можна назвати:
A	лінійною регресією;
B	нелінійною регресією;
C	одновимірною (парною) регресією;
D	багатовимірною (множинною) регресією.

Запитання 38	За умови, що зв'язок між двома величинами описується формулою $y = ax^2 + bx + c$, сам зв'язок найбільш повно можна назвати:
A	лінійною регресією;
B	нелінійною регресією;
C	одновимірною (парною) регресією;
D	багатовимірною (множинною) регресією.

Запитання 39	Для визначення коефіцієнтів рівняння лінійної регресії застосовують:
A	метод найменших квадратів;
B	симплекс-метод;
C	метод градієнтного спуску;
D	принцип максимальної правдоподібності.

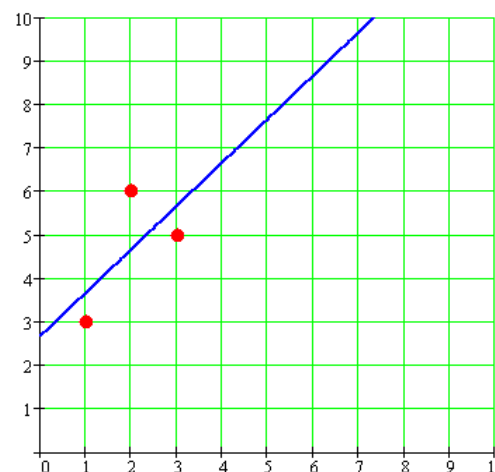
Запитання 40	Для якої кількості експериментальних точок при побудові лінійної регресії не доцільно застосовувати метод найменших квадратів:
A	10^6 , через дуже велику їх кількість;
B	3, через дуже малу їх кількість;
C	2;
D	метод найменших квадратів є найбільш простим методом для визначення коефіцієнтів рівняння лінійної регресії при будь-яких обсягах експериментальних даних.

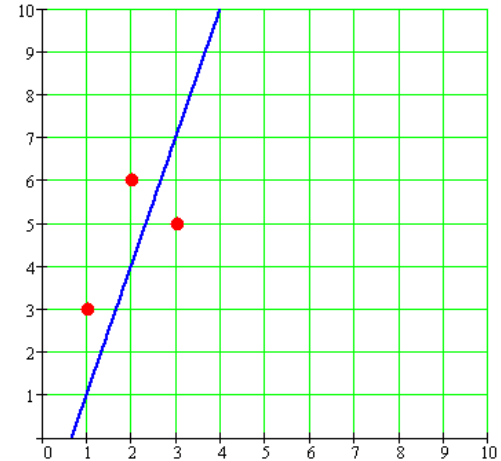
<u>Запитання 41</u>	Розрахуйте коефіцієнт a у рівнянні лінійної регресії $y = ax + b$ для наступного набору експериментальних даних:			
	x	1	2	3
	y	3	6	5
A	1;			
B	8/3;			
C	8,3;			
D	11/3.			

<u>Запитання 42</u>	Розрахуйте коефіцієнт b у рівнянні лінійної регресії $y = ax + b$ для наступного набору експериментальних даних:			
	x	1	2	3
	y	3	6	5
A	1;			
B	8/3;			
C	8,3;			
D	11/3.			

<u>Запитання 43</u>	Розрахуйте значення залежної величини y , що відповідає значенню незалежної величини $x = 1$, на основі рівняння лінійної регресії (порівняйте з експериментальним значенням $y = 3$), яку слід встановити, користуючись наступним набором експериментальних даних:			
	x	1	2	3
	y	3	6	5
A	1;			
B	$8/3$;			
C	8,3;			
D	$11/3$.			

Запитання 44	На основі чисельних розрахунків встановити, чи відповідає пряма на рисунку рівнянню лінійної регресії для трьох відмічених експериментальних точок:
A	так;
B	ні, вона повинна утворювати менший кут з віссю Ox ;
C	ні, вона повинна утворювати більший кут з віссю Ox ;
D	на основі даних рисунку не можливо встановити рівняння лінійної регресії.



Запитання 45	На основі чисельних розрахунків встановити, чи відповідає пряма на рисунку рівнянню лінійної регресії для трьох відмічених експериментальних точок:	
A	так;	
B	ні, вона повинна утворювати менший кут з віссю Ох;	
C	ні, вона повинна утворювати більший кут з віссю Ох;	
D	на основі даних рисунку не можливо встановити рівняння лінійної регресії.	

Запитання 46	Оберіть правильну назву для рівняння $y = a_0 + a_1x_1 + a_2x_2$, що встановлює зв'язок між двома незалежними змінними та однією залежною:
A	рівняння тривимірної лінійної регресії;
B	рівняння багатовимірної (множинної) лінійної регресії;
C	рівняння тривимірної нелінійної регресії;
D	рівняння багатовимірної (множинної) нелінійної регресії.

Запитання 47	Оберіть правильну назву для рівняння $y = a_0 + a_1x_1 + a_2x_2 + a_3x_1x_2$, що встановлює зв'язок між двома незалежними змінними та однією залежною:
A	рівняння тривимірної лінійної регресії;
B	рівняння багатовимірної (множинної) лінійної регресії;
C	рівняння тривимірної нелінійної регресії;
D	рівняння багатовимірної (множинної) нелінійної регресії.

Запитання 48	Чи можна використовувати метод найменших квадратів для визначення коефіцієнтів степеневих залежностей порядку квадратичної та більше:
A	можна, але трудомісткість розв'язку отриманої системи лінійних алгебраїчних рівнянь сильно збільшується з підвищенням величини степеня нелінійної регресії;
B	можна, причому трудомісткість розв'язку отриманої системи лінійних алгебраїчних рівнянь несуттєво збільшується з підвищенням величини степеня нелінійної регресії;
C	це принципово залежить від значення степеня нелінійної регресії;
D	ні, слід застосувати інший метод.

Запитання 49	Оберіть формулу для знаходження набору коефіцієнтів рівняння множинної лінійної регресії (тут X – регресійна матриця, Y – матриця значень залежної величини, T – символ транспонування):
A	$A = (X^T Y Y)^{-1} X^T Y$;
B	$A = (X^T Y)^{-1} X^T$;
C	$A = (X^T X)^{-1} X^T$;
D	$A = (X^T X)^{-1} X^T Y$.

Запитання 50	Виберіть неправильне твердження про регресійну матрицю, що використовується при множинній лінійній регресії:
A	розмірність регресійної матриці залежить від кількості наявних експериментальних точок та кількості вхідних параметрів (незалежних змінних);
B	перший рядок регресійної матриці утворений лише з одиниць;
C	усі елементи першого стовпця регресійної матриці дорівнюють одиниці;
D	при обчисленні матриці коефіцієнтів рівняння множинної регресії регресійна матриця в тому числі двічі використовується у транспонованому вигляді.

4. Список основної літератури

1. ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва.
2. НД ТЗІ 1.1-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення.
3. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
4. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
5. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу ТЗІ. Основні положення.
6. НД ТЗІ 1.4-001-00 Типове положення про службу захисту інформації в автоматизованій системі.
7. НД ТЗІ 1.4-002-08 Радіолокатори нелінійні. Класифікація. Рекомендовані методи та засоби випробувань.
8. НД ТЗІ 1.5-001-00 Радіовиявлювачі. Класифікація. Загальні положення.
9. НД ТЗІ 1.5-002-12 Класифікатор засобів технічного захисту інформації.
10. НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації.
11. НД ТЗІ 1.6-005-13 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці”
12. НД ТЗІ 2.1-002-07 Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу ТЗІ. Основні положення.
13. НД ТЗІ 2.3-001-01 Радіовиявлювачі вимірювальні. Методи та засоби випробувань.
14. НД ТЗІ 2.3-002-01 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби пасивного приховування мовної інформації. Нелінійні атенюатори та загороджувальні фільтри. Методика випробувань.
15. НД ТЗІ 2.3-003-01 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби активного приховування мовної інформації. Генератори спеціальних сигналів. Методика випробувань.
16. НД ТЗІ 2.3-004-01 Радіовиявлювачі індикаторні. Методи та засоби випробувань.
17. НД ТЗІ 2.3-005-01 Радіовиявлювачі панорамні. Методи та засоби випробувань.
18. НД ТЗІ 2.3-006-01 Радіовиявлювачі аналізувальні. Методи та засоби випробувань.
19. НД ТЗІ 2.5-006-99 Класифікатор засобів копіювально-розмножувальної техніки.
20. НД ТЗІ 2.6-001-11 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах.
21. НД ТЗІ 2.7-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт.
22. НД ТЗІ 2.7-002-99 Методичні вказівки з використання засобів копіювально-розмножувальної техніки.

23. НД ТЗІ 2.7-009-09 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.
24. НД ТЗІ 2.7-010-09 Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу
25. НД ТЗІ 2.7-011-12 Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки «Методики виявлення закладних пристроїв».
26. НД ТЗІ 2.7-013-16 Методичні вказівки з виконання зіставлення результатів оцінювання засобів захисту інформації від несанкціонованого доступу на відповідність вимогам ISO/IEC 15408 з вимогами НД ТЗІ 2.5-004-99
27. НД ТЗІ 3.1-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексів технічного захисту інформації. Перед проектні роботи.
28. НД ТЗІ 3.3-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.
29. НД ТЗІ 3.6-001-00 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.
30. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (Зі зміною № 1).
31. НД ТЗІ 3.7-002-99 Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова).
32. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
33. НД ТЗІ 4.7-001-01 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби визначення наявності та віддаленості місця контактного підключення засобів технічної розвідки. Рекомендації щодо розроблення методів випробувань.
34. Наказ Держспецзв'язку №023 (ДСК) від 19.06.2015 р. зі змінами наказ № 01т від 23.01.2023 р.
35. Бюлетень 28 Інформаційно-аналітичний бюлетень. Системи і засоби технічних розвідок та їх носії. Випуск 28 за 2022 рік
36. Кара-Мурза С. Маніпуляція свідомістю. – «ЕКСМО-Прес», 2001
37. Exposure of Enemy Set-Ups. Електронний ресурс. Режим доступу: <https://drive.google.com/file/d/16t59k0G381jlasvlZM5i49MZ2wTnwsyA/view>
38. Intelligence Targets Abroad. Електронний ресурс. Режим доступу: <https://drive.google.com/file/d/1dWB8ak89PeNiQppP7IYNqc7FIO6TZmGM/view>
39. Political Intelligence from USSR Territory. Електронний ресурс. Режим доступу: <https://drive.google.com/file/d/1XxulRAGcXO4XIFW-YrNhi57uzAx3dGwB/view>
40. Communication with Agents. Електронний ресурс. Режим доступу: <https://drive.google.com/file/d/1NQPERpdFYjCkrQEO-mIcmDVk5PMDQzmm/view>
41. Acquisition and Training of Agent Recruiters. Електронний ресурс. Режим доступу: <https://drive.google.com/file/d/1EesGYnEONyKHuApCNtCcDOm84ZxnLeRG/view>

42. Use of Soviet Cultural Committee. Електронний ресурс. Режим доступу: https://drive.google.com/file/d/1kbcWaaaEbxz_lIFXHg9BRDtZKfo-xD1e/view
43. Зачепило В.С. Схорона державної таємниці: навч. посіб. / В.С. Зачепило, З.А. Шандра, І.Р. Опірський, І.Я. Тишик, Л.В. Мороз. – Львів: Видавництво Львівської політехніки, 2015. – 168 с.
44. Закон України. Про перевезення небезпечних вантажів. Закон України від 06.04.2000 № 1644-III. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/1644-14#Text>
45. Закон України. Про страхування. Закон України від 18.11.2021 № 1909-IX. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/1909-20#Text>
46. Закон України. Про транспорт. Закон України від 10.11.1994 № 232/94-BPP. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/232/94-%D0%B2%D1%80#Text>
47. Кодекс України. Водний кодекс України. Кодекс від 06.06.1995 № 213/95-BP. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/213/95-%D0%B2%D1%80#Text>
48. Кодекс України. Кодекс торговельного мореплавства України. Кодекс від 23.05.1995 № 176/95-BP. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/176/95-%D0%B2%D1%80#Text>
49. Кодекс України. Кодекс торговельного мореплавства України. Кодекс від 23.05.1995 № 176/95-BP [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/176/95-%D0%B2%D1%80#Text>
50. Міжнародна конвенція по запобіганню забрудненню з суден (з поправками). [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/896_009#Text
51. Міжнародна конвенція про безпечні контейнери [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/995_013#Text
52. Міжнародна конвенція про вантажну марку (з поправками). [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/896_007#Text
53. Міжнародна конвенція про охорону людського життя на морі 1974 року (СОЛАС-74). <https://marad.gov.ua/ua/npa/mizhnarodna-konvenciya-pro-ohoronu-lyudskogo-zhittya-na-mori-1974-roku-solas-74>
54. Міжнародна конвенція про підготовку і дипломування моряків та несення вахти (з поправками). [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/995_053#Text
55. Міжнародна конвенція про пошук і рятування на морі. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/995_138#Text
56. Міжнародна конвенція щодо втручання у відкритому морі у випадках аварій, які призводять до забруднення нафтою (з поправками). [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/995_049#Text
57. Міжнародна конвенція. Експлуатаційна угода Міжнародної організації морського супутникового зв'язку (ІНМАРСАТ). [Електронний ресурс]. – Режим доступу: <http://consultant.parus.ua/?doc=00VYA2BF2F&abz=1LG29>
58. Міжнародна конвенція. Конвенція про боротьбу з незаконними актами, спрямованими проти безпеки морського судноплавства. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/995_220#Text
59. Міжнародна конвенція. Конвенція про Міжнародну організацію морського супутникового зв'язку (ІНМАРСАТ) [Електронний ресурс]. – Режим доступу: <http://consultant.parus.ua/?doc=00VY976843>
60. Міжнародна конвенція. Поправки до Міжнародної конвенції про пошук і рятування на морі 1979 року, які були прийняті Комітетом з безпеки на морі Міжнародної морської

організації 18 травня 1998 року (Резолюція КБМ.70 (69)). [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/896_001-98#Text

61. Міжнародні правила запобігання зіткненню суден у морі. https://zakon.rada.gov.ua/laws/show/995_220#Text

62. Наказ Мінінфраструктури. Про затвердження Змін до Положення про порядок підготовки та подання інформації про вантаж для його безпечного морського перевезення. Наказ від 26.06.2013 № 425. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/z1177-13#Text>

63. Наказ Мінінфраструктури. Про затвердження Положення про морських лоцманів. Наказ, Положення, Форма типового документа від 08.05.2013 № 292. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/z0920-13#Text>

64. Наказ Мінтранс України Про затвердження Положення про систему управління безпекою судноплавства на морському і річковому транспорті. Положення, від 20.11.2003 № 904. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/z1193-03#Text>

65. Наказ Мінтранс України. Про Головну державну інспекцію України з безпеки судноплавства. Наказ від 21.03.2002 № 185 [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/rada/show/v0185361-02#Text>

66. Наказ Мінтранс України. Про Головну державну інспекцію України з безпеки судноплавства. Наказ від 21.03.2002 № 185. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/rada/show/v0185361-02#Text>

67. Наказ Мінтранс України. Про затвердження Інструкції про огляд суден, які здійснюють плавання (експлуатуються) на внутрішніх водних шляхах України. Інструкція від 19.04.2001 № 225. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/z0400-01#Text>

68. Наказ Мінтранс України. Про затвердження Положення про державних річкових лоцманів. Наказ, Положення, Форма типового документа від 14.01.2002 № 11. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/z0091-02#Text>

69. Наказ Мінтранс України. Про затвердження Положення про порядок підготовки та подання інформації про вантаж для його безпечного морського перевезення. Наказ, Положення, Форма типового документа від 14.12.1998 № 497. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/z0848-98#Text>

70. Наказ Мінтранс України. Про затвердження Правил безпечної експлуатації баз для стоянки маломірних (малих) суден. Наказ, Правила, Форма типового документа від 16.07.2004 № 642. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/z0915-04#Text>.

71. Постанова Кабінету Міністрів України. Про вдосконалення технічного, класифікаційного і судноплавного нагляду на морському і внутрішньому водному транспорті. Положення від 08.06.1998 № 814. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/814-98-%D0%BF#Text>

72. Постанова Кабінету Міністрів України. Про внесення зміни до Порядку здійснення нагляду за забезпеченням безпеки руху на транспорті та визнання такими, що втратили чинність, деяких постанов Кабінету. Перелік від 29.02.2012 № 159. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/159-2012-%D0%BF#Text>

73. Розпорядження Кабінету Міністрів України Про схвалення Національної транспортної стратегії України на період до 2030 року Стратегія від 30.05.2018 № 430-р. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/430-2018-%D1%80#Text>

74. Стан безпеки судноплавства та аварійності на водному транспорті в Україні (у тому числі і за її межами, але із українськими суднами), включаючи маломірні (малі) судна, за січень – червень 2022 року з наростаючим підсумком [Електронний ресурс]. – Режим доступу: https://marad.gov.ua/storage/app/sites/1/uploaded-files/Zvit_2022.pdf

75. Балобанов А.О. Діяльність Європейського Союзу з правового забезпечення безпеки мореплавання. – Одеса: Вид-во ОНМУ, 2003. – 227с.
76. Іванов Д.А. Історія правового регулювання використання радіозв'язку для пошуку та рятування на морі // Актуальні проблеми держави і права: Зб. наук. пр. – Одеса: Юрид. л-ра, 2005. – Вип. 26. – С. 246-254.
77. Україна в міжнародних відносинах. Боротьба із злочинністю та взаємна правова допомога (Книга перша) / Зб. докум. (укр.. і рос. мовами). – Юрінком. – Київ, 1996.
78. Липинский В.Н., Качан В.Д., Аксенов Н.Ф. Глобальна морська система зв'язку під час лиха та для забезпечення безпеки За заг. ред.. В.В. Пономаренко. - Одеса: Морський тренажерний центр. - – 2002. – 525 с.
79. Лукшин І.В. Протиправні дії, що посягають на свободу мореплавання / / Право і політика. - 2000. - № 6.
80. Ромашев Ю.С., Корбут Л.В. Основи боротьби з актами тероризму та піратства на морі. // Альманах "Організована злочинність, тероризм та корупція". - 2003. - № 2.
81. Блінцов В.С. Підводно-технічні засоби і технології обстеження морських кабелів зв'язку.// Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні К.,1998 . – С. 109-110
82. Модель технічних розвідок (ТР-2030). – К. : ДССЗІ України, 2015
83. Модель технічних розвідок (ТР-2030). Бюлетень 28 Інформаційно-аналітичний бюлетень. Системи і засоби технічних розвідок та їх носії. Випуск 28 за 2022 рік
84. Закон України. Про державну таємницю / Редакція від 13.02.2020 – Режим доступу: <https://zakon.rada.gov.ua/laws/show/3855-12>
85. Закон України. Про захист інформації в інформаційно-телекомунікаційних системах / Редакція від 19.04.2014 – Режим доступу: <https://zakon.rada.gov.ua/laws/show/80/94-вр>
86. Закон України. Про захист персональних даних / Редакція від 20.03.2020. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2297-17>
87. Закон України. Про інформацію / Редакція від 21.12.2019 – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2657-12>
88. Закон України. Про національну безпеку України / Редакція від 15.03.2020 – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2469-19>
89. НД ТЗІ 1.1-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення.
90. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
91. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі
92. НД ТЗІ 1.6-005-13 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці"
93. НД ТЗІ 2.3-003-01 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби активного приховування мовної інформації. Генератори спеціальних сигналів. Методика випробувань.
94. НД ТЗІ 2.7-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт.
95. НД ТЗІ 2.7-009-09 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.
96. НД ТЗІ 2.7-010-09 Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу
97. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (Зі зміною № 1).

98. НД ТЗІ 3.7-002-99 Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова).

99. Наказ Адміністрації Держспецзв'язку від 06 жовтня 2021 року № 601 Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури (зі змінами). [Електронний ресурс]. – Режим доступу: <https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601>

100. Наказ Адміністрації Держспецзв'язку Про внесення змін до Положення про державну експертизу у сфері технічного захисту інформації. Наказ від 19.08.2020 № 483. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/z0995-20#Text>

101. Наказ Адміністрації Держспецзв'язку від 15.01.2021 № 23 "Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури" [Електронний ресурс]. – Режим доступу: <https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-15-01-2021-23-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-kategorizaciyi-ob-yektiv-kritichnoyi-infrastrukturi>

102. Наказ Адміністрації Держспецзв'язку від 29.05.2023 № 463 «Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами». [Електронний ресурс]. – Режим доступу: <https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-29-05-2023-463-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-zabezpechennya-kiberzakhistu-avtomatizovanikh-sistem-upravlinnya-tehnologichnimi-procesami>

103. Наказ Держспецзв'язку №023 (ДСК) від 19.06.2015 р. зі змінами наказ № 01т від 23.01.2023 р.

104. Наказ Служби безпеки України. Про затвердження Зводу відомостей, що становлять державну таємницю. Наказ від 23.12.2020 № 383. Режим доступу: <https://zakon.rada.gov.ua/laws/show/z0052-21#Text>

105. Наказ Служби безпеки України. Про затвердження Змін до розділу II Зводу відомостей, що становлять державну таємницю. Наказ від 17.02.2023 № 63 Режим доступу: <https://zakon.rada.gov.ua/laws/show/z0337-23#Text>

106. Перелік нормативно-методичних документів в галузі захисту інформації. Товариство з обмеженою відповідальністю «НІКС» NicS / Облікові документи для секретного діловодства. – Режим доступу: <https://sites.google.com/a/nics.com.ua/price/>

107. Кавун С. В. Інформаційна безпека. Навчальний посібник. Ч. 2 / С. В. Кавун, В. В. Носов, О. В. Манжай. – Харків: Вид. ХНЕУ, 2008. – 196 с.

108. Захист інформації в автоматизованих системах управління [Текст]: навч. посібник/Уклад. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.

109. Яремчук Ю. Є. Комплексні системи захисту інформації. Навчальний посібник / Ю.Є. Яремчук, П.В. Павловський, В.С. Катаєв, В.В. Сінюгін / Видавництво ВНТУ. Режим доступу: https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi/index.html

5. Критерії та норми оцінювання

Підсумкове оцінювання результатів навчання в Університеті здійснюється за єдиною 100-бальною шкалою. Оцінка здобувача освіти відповідає відношенню встановленого при оцінюванні рівня сформованості професійних і загальних компетентностей до запланованих результатів навчання.

Довідник з розподілу оцінок / Reference book on ratings	
Оцінка за 100-бальною шкалою університету / Grade according to 100-points scale of University	Оцінка за шкалою ЄКТС / Grade according to ECTS scale
90-100 (творчий рівень)/(creative level)	A (відмінно) / (excellent)
82 – 89 (високий рівень)/(high level)	B (дуже добре) / (very good)
74 – 81 (добрий рівень)/(good level)	C (добре) / (good)
64 – 73 (середній рівень)/(average level)	D (посередньо) / (average)
60 – 63 (задовільний рівень)/(satisfactory level)	E (достатньо) / (satisfactory)
35 – 59 (низький рівень)/(low level)	FX (незадовільно з можливістю повторного складання) / (unsatisfactory with the possibility to repass the exam)
1 – 34 (незадовільний рівень)/(unsatisfactory level)	F (незадовільно з обов'язковим повторним вивченням) / (unsatisfactory with the compulsory repeating of the course)

Критерієм успішного проходження студентом оцінювання є досягнення ним мінімальних порогових рівнів оцінок за кожним запланованим результатом навчання освітнього компонента та мінімального порогового рівня оцінки за освітнім компонентом загалом; □

Мінімальний пороговий рівень оцінки з освітнього компоненту є єдиним в Університеті, не залежить від форм і методів оцінювання та становить 60 балів від максимально можливої кількості балів;



НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
КОРАБЛЕБУДУВАННЯ
ІМ. АДМІРАЛА МАКАРОВА

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
АВТОМАТИКИ І ЕЛЕКТРОТЕХНІКИ



« _ » грудня 20 року

ДЕРЖАВНИЙ КВАЛІФІКАЦІЙНИЙ ЕКЗАМЕН

**ДРУГОГО РІВНЯ ВИЩОЇ ОСВІТИ
ЗА ОСВІТНЬО-ПРОФЕСІЙНОЮ ПРОГРАМОЮ**

«СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ, АВТОМАТИЗАЦІЯ ЇЇ ОБРОБКИ»

спеціальність F5 «Кібербезпека та захист інформації»
галузь знань F «Інформаційні технології»

Освітня кваліфікація – Магістр з кібербезпеки та захисту інформації

Професійна кваліфікація – Провідний фахівець сфери захисту інформації

студента групи _____

(П.І.Б.)

Варіант _____

БЛАНК ВІДПОВІДЕЙ*

№	A	B	C	D	E	№	A	B	C	D	E	№	A	B	C	D	E	№	A	B	C	D	E	№	A	B	C	D	E
1.						11.						21.						31.						41.					
2.						12.						22.						32.						42.					
3.						13.						23.						33.						43.					
4.						14.						24.						34.						44.					
5.						15.						25.						35.						45.					
6.						16.						26.						36.						46.					
7.						17.						27.						37.						47.					
8.						18.						28.						38.						48.					
9.						19.						29.						39.						49.					
10.						20.						30.						40.						50.					

*Місце для виправлення помилкової відповіді***

№	A	B	C	D	E

№	A	B	C	D	E

№	A	B	C	D	E

Підпис студента _____ /

Підпис секретаря _____ / (Макарчук О.М.)

* Відповіді до всіх завдань позначати X;

** Виправлення необхідно робити в спеціально відведеній частині бланка

ТАБЛИЦЯ БАЛІВ

№	Кількість балів	№	Кількість балів	№	Кількість балів	№	Кількість балів	№	Кількість балів
1.		11.		21.		31.		41.	
2.		12.		22.		32.		42.	
3.		13.		23.		33.		43.	
4.		14.		24.		34.		44.	
5.		15.		25.		35.		45.	
6.		16.		26.		36.		46.	
7.		17.		27.		37.		47.	
8.		18.		28.		38.		48.	
9.		19.		29.		39.		49.	
10.		20.		30.		40.		50.	

Загальна кількість набраних балів _____

ПІДСУМКОВА ОЦІНКА

Підсумкова оцінка за 100-бальною шкалою	Підсумкова оцінка за шкалою ECTS

Голова ДЕК _____ Нужний С.М.

Члени ДЕК: _____ Козирсв С.С.

_____ Турти М.В.

_____ Сірівчук А.С.

Секретар _____ Макарчук О.М.