Міністерство освіти і науки України
Харківський національний університет імені В.Н. Каразіна

Програма атестаційного екзамену

за спеціальністю 125-кібербезпека

перший (бакалаврський) рівень

Затверджено на засіданні Вченої ради факультету комп'ютерних наук
Протокол № від . .2022 р.

Голова Вченої ради Лазурик В.Т.

м. Харків 2022 р.

І. Перелік питань за темами.

Тема №1. Теорія чисел

1. Прості числа і "основна" теорема арифметики. Канонічне подання раціональних чисел. Решето Ератосфена для пошуку простих чисел. Взаємно прості числа. Теорема Чезаро.
2. Ланцюгові дроби. Розкладання чисел в ланцюгові дроби. Скінченні та нескінченні ланцюгові дроби та їх зв'язок із раціональними та ірраціональними числами.
3. Обчислення придатних дробів. Застосування алгоритму Евкліда для обчислення придатних дробів. Властивості придатних дробів. Основні рекурентні співвідношення.
4. Формули Біне. Послідовності чисел Фібоначчі та чисел Люка, їх властивості та зв'язок із придатними дробами. Щільність послідовностей чисел та пар чисел.
5. Визначення і прості властивості порівнянь. Кільце лишків. Повна та приведена система вирахувань. Визначення та основні властивості.
6. Теорема Ейлера і теорема Ферма. Порівняння першого степеня, визначення та основні властивості. Вирішення порівняння із застосуванням функції Ейлера.
7. Китайська теорема про лишки. Вирішення системи порівнянь. Схема розподілу секрету із застосуванням китайської теореми про лишки.
8. Алгоритм обміну ключами Діффі-Хеллмана. Алгоритм шифрування з відкритими ключами RSA. Алгоритм цифрового підпису RSA.

Тема №2. Теорія груп, полів, кілець

1. Дайте абстрактне визначення та наведіть основні властивості групи. Поясніть на прикладі властивість комутативності групи. Дайте абстрактне визначення підгрупи, наведіть приклади.

2. Дайте абстрактне визначення та наведіть основні властивості векторного простору над кінцевим полем. Що таке базис векторного простору та його розмірність?

3. Дайте абстрактне визначення та наведіть основні властивості кільця. Поясніть на прикладі властивість комутативності кільця.

4. Дайте абстрактне визначення та наведіть основні властивості поля. Що таке поле Галуа? Наведіть приклади. Дайте визначення таких понять як підполе та розширення поля.

5. Дайте визначення незвідного многочлена. Що таке приведений многочлен?

6. Дайте визначення порядку точки еліптичної кривої. За якими формулами обчислюються операції подвоєння та додавання точок еліптичної кривої у простому полі характеристики $p > 3$?

7. Дайте визначення та наведіть основні властивості примітивних елементів кінцевого поля. Що таке примітивний многочлен?

Тема №3. Прикладна криптологія

1. В чому сутність основних положень щодо управління ключами. Стани ключа та переходи між станами. Захист ключів криптографічними, фізичними засобами та організаційними засобами?

2. Визначення, властивості та застосування ВП та ПВП. В чому сутність методик тестування ВП та ПВП з використанням FIPS 140-1 та NIST STS?

3. Які основні задачі криптоаналізу відносно симетричних криптосистем та при яких вхідних даних вони можуть вирішуватись?

4. В чому сутність та відмінності ЕЦП з додатком та відновленням повідомлення? Які основні вимоги висуваються до ЕЦП з додатком та з відновленням повідомлення?

5. Основні підходи до побудування БСШ. В чому сутність підходу до побудування БСШ на основі СПН структур та які БСШ побудовані на основі SPN структур і їх властивості?

6. В чому сутність вимог коректності та повноти криптографічного протоколу? В чому сутність та які можливості криптографічного протоколу з нульовим розголошенням?

7. Які основні задачі криптоаналізу відносно асиметричних криптосистем та при яких вхідних даних вони можуть вирішуватись? Модель крипто аналітика та які його практичні та потенційні можливості?

8. Дайте характеристику та обґрунтуйте вимоги до загальних параметрів та ключової пари для крипто перетворення в групі точок еліптичної кривої ?

9. Умови та приклади реалізації криптосистем з безумовним рівнем стійкості. Особливості реалізації обчислювальної та ймовірної стійкості крипто перетворень?

10. Класифікація та сутність криптографічних перетворень і їх застосування для надання послуг безпеки інформації?

Тема №4. Теорія автоматичного управління.

1. Математичний опис лінійних динамічних систем (ЛДС). Визначення передаточної функції лінійної системи.

2. Типові елементарні сигнали для дослідження ЛДС. Динамічні та частотні характеристики ЛДС. Годограф амплитудно-фазової характеристики ЛДС.

3. Стійкість ЛДС. Алгебраїчний критерій стійкості, частотні критерії стійкості Найквіста і Михайлова.

4. Основні показники якості управління в ЛДС. Статичні та астатичні системи. Робастність ЛДС.

Тема №5. Системи технічного захисту інформації

1. Технічні канали витоку інформації.
2. Структура і класифікація радіоканалів витоку інформації.
3. Електричні і візуально-оптичні канали витоку інформації. Заходи технічного захисту.
4. Класифікація матеріально-речових каналів витоку інформації. Джерела та носії інформації.

Тема №6. Захист інформації в інформаційних і комунікаційних системах

1. Проаналізуйте і надайте характеристику забезпечення безпеки засобами СУБД.
2. Проаналізуйте і надайте характеристику засобам та методам захисту, яки використовуються в СУБД Microsoft Access.
3. Проаналізуйте і надайте характеристику основних методів і засобів захисту від шкідливого програмного забезпечення.
4. Проаналізуйте і надайте пояснення, що таке комп'ютерне піратство? Надайте характеристику основних способів боротьби з комп'ютерним піратством.
6. Назвіть, охарактеризуйте та порівняйте основні захисні механізми універсальних і захищених операційних систем (наприклад, MS Windows і Linux).
7. Чи достатніми є три базові права доступу до файлів для реалізації в ОС Linux необхідної політики безпеки? Які права по відношенню до файлів і каталогів необхідно мати для копіювання файлу?
8. Які ви знаєте заходи по організації захищених мереж з використанням технології VPN? Охарактеризуйте можливі для використання при цьому безпечні протоколи.
9. Сутність захисту локальних мереж за допомогою міжмережевих екранів. Міжмережева політика, типова архітектура та компоненти при реалізації екранування мереж.
10. Які ви знаєте типові уразливості інформаційно-телекомунікаційних систем та методи підвищення їх захищеності. Приведіть приклади криптографічних методів і засобів їх реалізації.

Тема №7. Комплексні системи захисту інформації

1. Правові основи створення КСЗІ. Визначення КСЗІ. В яких випадках створюються КСЗІ. Склад КСЗІ та характеристика складових.
2. Етапи створення КСЗІ. Сутність етапів.
3. Обстеження інформаційно-телекомунікаційної системи. Середовища функціонування інформаційно-телекомунікаційної системи (складові середовища).
4. У яких випадках розроблюється технічне завдання (ТЗ) на створення КСЗІ. Що є вихідними даними для створення ТЗ на КСЗІ. Функціональний профіль захищеності (ФПЗ) інформації. Визначення ФПЗ. Семантика профілю.

5. Політика безпеки інформації (ПБІ) – як етап створення КСЗІ. Чим визначається зміст ПБІ. Склад документу "Політика безпеки інформації".

6. Розкрити зміст визначенням, термінам та словосполученням: «виток інформації», «порушення цілісності інформації в системі», «блокування та знищення інформації в системі», «технічний захист інформації», «криптографічний захист інформації», «комплексна система захисту інформації».

7. Перерахувати дії, що містить комплексний підхід до побудови систем захисту інформації. Принципи створення комплексної системи захисту інформації.

8. Призначення та основні завдання Держспецз’вязку щодо захисту інформації.

9. Види та типи схем в КСЗІ згідно вимог ЄСКД. Зміст основних стандартів щодо захисту інформації.

Тема №8. Компоненти складних комп'ютерних мереж

1. Модель взаємодії відкритих систем.
2. Основні принципи багатоканального зв'язку. Часове, частотне і кодове розділення сигналів абонентів.
3. Системи передачі даних плезіохронної і синхронної цифровій ієрархії.
4. Системи мобільного зв'язку: стандарти AMPS, GSM, CDMA.
5. Мережі мобільного зв'язку третього покоління (3G).
6. Транкінгові системи. Протокол TETRA.

Тема №9. Основи теорії передачі інформації

1. Сучасний стан і перспективи розвитку систем передачі інформації. Основні визначення систем електрозв’язку.

2. Пропускна спроможність фізичних каналів передачі інформації. Геометричний спосіб визначення.

3. Види фізичних ліній зв’язку. Дротові та бездротові лінії. Способи розповсюдження радіохвиль. Хвильові характеристики металічних ліній зв’язку.

4. Одиниця виміру потужності дБ. Одиниця виміру потужності відносно еталонного рівня дБм. Обчислення рівнів потужності, посилення та втрат.

5. Види уявлення сигналів. Дискретизація сигналів за часом. Теорема Котельникова. Квантування сигналів за рівнем. Теорема Шеннона о RD(DR)-функціях. Обчислення помилок дискретизації і квантування.

6. Двійкова симетрична модель незалежних помилок у дискретних каналах. Біноміальний закон розподілу помилок. Амплитудно-імпульсна модуляція. Дельта модуляція. Імпульсно-кодова модуляція. Спектральні характеристики імпульсно-кодової модуляції.

7. Модель простого сигнала АМ-2 з пасивною паузою. Модель простого сигнала ЧМ-2. Формування та обробка. Модель простого сигнала ФМ-2. Формування та обробка.

8. Маніпуляційний код Грея. Правило отримання та декодування.

Тема №10. Стеганографія

1. Дайте визначення низькорівневих властивостей зорової системи людини та приклади їхнього використання в стеганографії. Які методи приховування даних у просторовій області нерухомих зображень Ви знаєте?
2. Дайте визначення пропускної здатності каналів передачі прихованих повідомлень (стеганографічних каналів). Як зазвичай пов'язана пропускна здатність, ймовірність правильного вилучення інформації на приймальній стороні та величина внесених похибок в контейнер, що був використаний при вбудовуванні інформаційних повідомлень?
3. Дайте визначення складних дискретних сигналів. Наведіть правило формування складних сигналів Уолша-Адамара. Які відомі Вам методи стеганографічного приховування застосовують ці сигнали?
4. Дайте визначення теоретично недешифрованих секретних систем в термінах теоретико-інформаційного підходу К. Шеннона. За аналогією дайте визначення теоретично недетектованих стеганографічних систем.
5. Наведіть структурну схему та математичну модель стеганографічної системи. Поясніть функціонування стеганографічної системи за її структурною схемою, дайте визначення та поясніть функціональне призначення структурних елементів стеганосистеми.
6. Поясність сутність методу фазового кодуванні при стеганографічному перетворенні із аудіоконтейнерами.
7. Поясність сутність семантичних методів лінгвістичної стеганографії. Наведіть як приклад деякі словосполучення або фрази, що можуть бути використані для приховування інформації. Які основні переваги та недоліки сематичних методів?
8. Які основні галузі використання стеганографічних систем Ви знаєте? Що таке «цифрові водяні знаки», де вони використовується і які головні відмінності від інших прикладів використання стегосистем?
9. Які особливості слуху людини використовують в стеганографії? Який стеганографічний метод використовує властивість слухової системи людини, що полягає в слабкій чутливості до незначних змін луна-сигналів? Поясніть сутність методу та основні фізичні властивості.

Тема №11. Управління інформаційною безпекою

1. Загальна характеристика міжнародних стандартів в галузі управління інформаційною безпекою. Процесна модель управління інформаційною безпекою.
2. Концепція створення системи управління інформаційною безпекою. Принципи забезпечення безпеки інформації в інформаційних системах.
3. Концепція створення системи управління інформаційною безпекою. Мета забезпечення безпеки інформації в інформаційних системах. Суб'єкти та об'єкти захисту. Методи протидії загрозам інформаційною безпеки.

4. Мета та методи проведення державної експертизи КСЗІ. Загальні положення щодо організація проведення експертизи (суб'єкти та об'єкти експертизи, взаємодія Організатора та Замовника експертизи, строки проведення експертизи, порядок надання та розгляду заяв на проведення експертизи тощо).

5. Етапи проведення державної експертизи КСЗІ та засобів захисту інформації. Призначення та сутність етапів. Зміст робіт, що виконуються на відповідних етапах.

6. Комплекс технічного захисту інформації (КТЗІ). Визначення, в яких випадках створюється. Етапи створення та їх характеристика.

7. Принципи забезпечення безпеки інформації в АС.

8. Призначення етапу створення КСЗІ: Розробка проекту КСЗІ. Стадії проектування (створення) КСЗІ ІТС. Документи, що розробляються при проектуванні КСЗІ.

9. Призначення етапів створення КСЗІ: Попередні випробування, Дослідна експлуатація КСЗІ.

10. Призначення етапів створення КСЗІ: введення КСЗІ в дію; оцінка захищеності інформації.

Тема №12. Нормативно-правове забезпечення інформаційної безпеки

1. Організаційно-правові заходи щодо охорони державної таємниці. За яких умов організаціям надається дозвіл на провадження діяльності, пов'язаної з державною таємницею.

2. Порядок надання допуску до державної таємниці. Кому надається допуск. Що передбачає надання допуску до державної таємниці.

3. Класифікація інформації з обмеженим доступом. Особливості захисту інформації з обмеженим доступом.

4. Відповідальність за порушення законодавства про державну таємницю.

5. Вимоги законодавства до забезпечення захисту відкритої інформації в системі.

6. Банківська таємниця та система її охорони. Шляхи збереження банком банківської таємниці. Які відомості відносяться до банківської таємниці. В яких випадках може бути розкрита банківська таємниця.

7. Правові основи ліцензування господарської діяльності в Україні. Принципи державної політики в сфері ліцензування. Які роботи в галузі КЗІ та ТЗІ підлягають ліцензуванню.

8. Вимоги, що висуваються до суб'єктів господарювання для провадження господарської діяльності. Кваліфікаційні, організаційні, технологічні, особливі вимоги.

9. Персональні дані (ПД). Що відноситься до персональних даних. Правові основи захисту ПД. Основні визначення: персональні дані; база персональних даних; обробка персональних даних; суб'єкти персональних даних.

10. Загальні вимоги правових актів щодо обробки персональних даних.

ІІ. Загальні критерії оцінювання знань.

Бали	Оцінка за національною шкалою	Вимоги
(90-100)	відмінно	Тверде засвоєння теоретичного матеріалу, глибокі та вичерпні знання змісту програмного матеріалу по суті питання, розуміння сутності та взаємозв'язку розглянутих процесів і явищ, тверде знання основних положень суміжних питань. Уміння самостійно використовувати математичний апарат для аналізу та вирішення практичних завдань, робити правильні висновки з отриманих результатів. Логічність і грамотність викладення. Відсутність помилок і неточних формулювань.
(70-89**)**	добре	Тверді і досить повні знання теоретичного матеріалу по суті питання, правильне розуміння сутності та взаємозв'язку розглянутих процесів і явищ, розуміння основних положень суміжних питань. Уміння самостійно застосовувати математичний апарат до вирішення практичних завдань. Окремі неточності у формулах, графіках, логікі та мові відповіді, що не ставлять під сумнів принципову вірність відповіді. Логічність і зрозумілість викладення. Бали 80-89 : Відсутність значних помилок, допустимі 1-3 неточності. Бали 70-79 : Не більше як 4 припущені неточностей при відсутності помилок або одна значна помилка і 1-2 неточності
(50-69**)**	задовільно	Тверді у основі та загалом задовільні знання і розуміння теоретичного матеріалу по суті питання, зрозумілість викладення. Правильні конкретні відповіді на поставлені питання за наявності кількох помилок і неточностей при висвітленні окремих положень. Уміння застосовувати теоретичні знання до вирішення основних практичних завдань, які не потребують самостійного застосування складного математичного апарату або творчого підходу до інформаційних технологій. Бали 60-69: припущення тільки однієї, однак грубої, помилки або тільки двох суттєвих помилок. Бали 50-59 : не більше однієї грубої помилки при 1-2 значних помилках або не більше 4 значних

		помилок за відсутності грубих.
(0-49)	незадовільно	Недостатнє розуміння суті розглянутих процесів і явищ, наявність кількох грубих помилок або значної кількості суттєвих помилок у відповіді. Невміння зрозуміло викладати відповіді на питання. Невміння застосовувати знання при вирішенні практичних завдань.

Затверджено на засіданні кафедри безпеки інформаційних систем і технологій факультету комп'ютерних наук. Протокол № від . .2021.

Завідувач кафедри безпеки інформаційних систем і технологій

д.т.н, доцент С.Г. Рассомахін