

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Одеська національна академія зв'язку ім. О.С. Попова

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ  
РАДІО, ТЕЛЕБАЧЕННЯ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

**ЗАТВЕРДЖУЮ**

Ректор ОНАЗ ім. О.С. Попова

\_\_\_\_\_ проф. П.П. Воробієнко

«\_\_\_» \_\_\_\_\_ 2017 р.

## **ПРОГРАМА**

**вступних випробувань для осіб,  
що мають ступінь бакалавра  
та виявили бажання продовжити навчання  
для здобуття ступеня магістра**

Ступінь: Магістр

Галузь знань: 12 «Інформаційні технології»

Спеціальність: **125 «Кібербезпека»**

Одеса 2017

Програма вступних випробувань для осіб, що здобули ступінь бакалавра та проходять вступні випробування для подальшого навчання на здобуття ступеня магістра за відповідною спеціальністю 125 «Кібербезпека».

Програму розроблено кафедрою Інформаційної безпеки та передачі даних

Директор  
ННІ Радіо, телебачення  
та інформаційної безпеки

Є.В. Васіліу

Програма розглянута та схвалена  
на засіданні приймальної комісії,

протокол № \_\_\_\_\_ від «\_\_\_\_\_» \_\_\_\_\_ 2017 р.

Відповідальний секретар  
приймальної комісії

В.Ю. Кумиш

## ПЕРЕДМОВА

Мета вступного іспиту полягає в комплексній перевірці знань абітурієнтів, отриманих ними в результаті вивчення циклу дисциплін, передбачених освітньо-професійною програмою та навчальними планами відповідного напрямку підготовки *6.170101 – Безпека інформаційних і комунікаційних систем* та *6.170102 – Системи технічного захисту інформації*. Студент повинен продемонструвати фундаментальні та професійно-орієнтовані уміння та знання щодо узагальненого об'єкта дослідження і здатність вирішувати типові професійні завдання, передбачені для відповідних посад.

Фаховий вступний іспит базується на матеріалах з дисциплін „Інформаційні технології”, „Прикладна криптологія”, „Криптографія та стеганографія”, „Безпека інформаційних та комунікаційних систем”, „Захист інформації в інформаційно-комунікаційних системах”, „Теорія інформації та кодування”, „Комплексні системи захисту інформації: Проектування, впровадження, супровід”, „Методи та засоби технічного захисту інформації”.

## МЕТА ІСПИТУ

Визначення рівня підготовки абітурієнтів з метою проведення конкурсного відбору для навчання в Одеській національній академії зв'язку ім. О. С. Попова (далі: Академія) за відповідною спеціальністю.

## ФОРМА ФАХОВОГО ВСТУПНОГО ВИПРОБУВАННЯ

Згідно з чинними «Правилами прийому до Одеської національної академії зв'язку ім. О. С. Попова у 2017р.», для охочих продовжити навчання за ступенем магістра на основі базової вищої освіти передбачено обов'язкове складання комплексного вступного іспиту з фахових дисциплін. Нижче наведена структура даного іспиту та навчальні матеріали, які рекомендовані для опрацювання в ході підготовки до нього. Іспит складається з п'яти питань (Додатки 1-2).

1. Абітурієнт відповідає на запитання, що зазначені в екзаменаційному білеті. Питання взято з відповідних навчальних програм дисциплін „Інформаційні технології”, „Прикладна криптологія”, „Захист інформацій в інформаційно-комунікаційних системах”, „Теорія інформації та кодування”, „Комплексні системи захисту інформації: Проектування, впровадження, супровід” відповідно до програми підготовки бакалаврів напрямку 6.170101 – Безпека інформаційних і комунікаційних систем та навчальних програм дисциплін „Інформаційні технології”, „Безпека інформаційних та комунікаційних систем”, „Криптографія та стеганографія”, „Теорія інформації та кодування”, „Методи та засоби технічного захисту інформації” відповідно до програм підготовки бакалаврів напрямку 6.170102 – Системи технічного захисту інформації.

Фахове вступне випробування проводиться на підставі білетів, які містять п'ять питань з перелічених дисциплін. У кожному питанні є теоретична та практична складова. Час на підготовку відповідей – 3 академічних години. Сумарна оцінка розраховується як середня арифметична з п'яти окремих оцінок.

2. Перелік запитань, покладених в основу вступного іспиту з фахових дисциплін, наведено в Додатках 1-2 та представлено у відповідному розділі на сайті Академії ([www.onat.edu.ua](http://www.onat.edu.ua)).

3. При оцінюванні знань абітурієнта під час вступного іспиту з фахових дисциплін відповідно до чинних «Правил прийому до Одеської національної академії зв'язку ім. О. С. Попова у 2017р.» використовується 100-бальна система оцінки, за якою оцінка «відмінно» відповідає 90-100 балам, оцінка «добре» – 74-89 балам, оцінка «задовільно» – 60-73 балам, при отриманні менш ніж 60 балів абітурієнт отримує оцінку «незадовільно».

## КРИТЕРІЇ ОЦІНЮВАННЯ

При оцінюванні знань вступників вихідними критеріями є такі:

- оцінку **«відмінно»** (90-100 балів) абітурієнт отримує, якщо він, працюючи над відповідями в межах встановленого для підготовки часу, правильно виразив власну думку, що не суперечить теоретичному матеріалу з відповідної дисципліни; не зробив жодної помилки при формулюванні відповідей; зв'язано, логічно, тематично адекватно і зрозуміло побудував свої відповіді, а також може невимушено, без жодних складнощів, вільно дати пояснення представнику комісії під час іспиту (реагувати на пропозиції та запитання, ставити запитання в разі виникнення непорозуміння щодо отриманого завдання або зазначеного в білеті запитання);

- оцінку **«добре»** (74-89 балів) абітурієнт отримує, якщо він, працюючи над відповідями в межах встановленого для виконання часу, виразив власну думку, що не суперечить теоретичному матеріалу з відповідної дисципліни; зробив незначні помилки при формулюванні відповідей; не завжди зв'язано, логічно, тематично адекватно і зрозуміло побудував свої відповіді, але певною мірою може невимушено, без жодних складнощів, вільно дати пояснення представнику комісії під час іспиту (реагувати на пропозиції та запитання, ставити запитання в разі виникнення непорозуміння щодо отриманого завдання або зазначеного в білеті запитання);

- оцінку **«задовільно»** (60-73 бали) абітурієнт отримує, якщо він, працюючи над відповідями в межах встановленого для виконання часу, намагався виразити власну думку, що не суперечить теоретичному матеріалу з відповідної дисципліни; зробив певною мірою некритичні помилки при формулюванні відповідей; не завжди зв'язано, логічно, тематично адекватно і зрозуміло побудував свої відповіді, але певною мірою може дати пояснення своїх відповідей на запитання представнику комісії під час іспиту (реагувати на пропозиції та запитання, ставити запитання в разі виникнення непорозуміння щодо отриманого завдання або зазначеного в білеті запитання);

- оцінку **«незадовільно»** (менше 60 балів) абітурієнт отримує, якщо він не може дати відповіді в межах встановленого для виконання часу; припускає грубі помилки у відповідях, які не відповідають змісту теоретичного матеріалу з відповідної дисципліни та не дає представнику комісії відповідей на жодне з додаткових запитань.

## Перелік запитань до вступних випробувань для осіб, що виявили бажання продовжити навчання для здобуття ступеня магістра

### За спеціальністю: 125 «Кибербезпека»

(спеціалізацією: Безпека інформаційних і комунікаційних систем)

#### Інформаційні технології

1. Скласти схему алгоритму та програму обчислення значення  $Y$ :

$$Y = \begin{cases} \operatorname{tg}^3 (cx^2 + 0.2x), & \text{якщо } x < 0 \\ \ln |c^2 - 1|, & \text{якщо } x = 0 \\ \frac{\cos^3 (c + x)}{2 + x^4}, & \text{якщо } x > 0 \end{cases}$$

при  $c = 2.86$ . Значення  $x$  ввести з клавіатури.

2. Скласти схему алгоритму та програму обчислення значення суми:

$$S = \sum_{k=1}^{10} \frac{x^{4k+1}}{(4k+1)!};$$

Значення  $x$  ввести з клавіатури.

3. Скласти схему алгоритму та програму обчислення значення суми:

$$S = \sum_{k=1}^{11} \frac{x^{2(k+1)}}{(k+1)!};$$

Значення  $x$  ввести з клавіатури.

4. Скласти схему алгоритму та програму обчислення значення суми:

$$S = \sum_{k=1}^{10} \frac{x^{2k}}{(k+1)!};$$

Значення  $x$  ввести з клавіатури.

5. Скласти схему алгоритму та програму обчислення значення суми:

$$S = \sum_{k=1}^{12} \frac{x^{2k+1}}{k!};$$

Значення  $x$  ввести з клавіатури.

6. Скласти схему алгоритму та програму обчислення значення суми:

$$S = \sum_{k=1}^7 \frac{(-1)^k \cdot x^{2k}}{(2k+3)!};$$

Значення  $x$  ввести з клавіатури.

7. Скласти схему алгоритму та програму обчислення значення добутку:

$$p = \prod_{i=1}^n (3i - 1).$$

Значення  $n$  ввести з клавіатури.

8. Скласти схему алгоритму та програму обчислення значення суми:

$$S = \sum_{k=1}^7 \frac{(2x)^k}{(2k)!};$$

Значення  $x$  ввести з клавіатури.

9. Скласти схему алгоритму та програму обчислення значення суми:

$$S = \sum_{k=1}^{11} \frac{x^{3k+1}}{(3k+1)!};$$

Значення  $x$  ввести з клавіатури.

10. Скласти схему алгоритму та програму обчислення значення суми:

$$S = \sum_{k=1}^7 \frac{x^{2k+1}}{(2k+1)!};$$

Значення  $x$  ввести з клавіатури.

11. Скласти схему алгоритму та програму обчислення значення суми:

$$K = \sum_{i=1}^{11} \frac{x^{2i}}{(2i)!};$$

Значення  $x$  ввести з клавіатури.

12. Скласти схему алгоритму та програму табулювання функції  $y=\sin(x)$ , де  $x \in [2, 4]$  і змінюється з кроком  $h=0,5$ .

13. Скласти схему алгоритму та програму табулювання функції  $y=\sin(x)$ , де  $x \in [2, 4]$  і змінюється з кроком  $h=0,5$ .

14. Скласти схему алгоритму та програму табулювання функції  $y=x^2 + 0,8x$ , де  $x \in [-2, 2]$  і змінюється з кроком  $h=0,5$ .

15. Скласти схему алгоритму та програму табулювання функції  $y=x^3+x^2+0,5$ , де  $x \in [-4,4]$  і змінюється з кроком  $h=0,5$ .

16. Скласти схему алгоритму та програму табулювання функції  $y=x^2+0,5x+3$ , де  $x \in [-3, 3]$  і змінюється з кроком  $h=0,5$ .

17. Скласти схему алгоритму та програму табулювання функції  $y$ :

$$y = \begin{cases} \sqrt{p + \sin^2 x}, & \text{якщо } x < 0 \\ e^{p^2+p}, & \text{якщо } x = 0 \\ \frac{3 \cdot x + \sin^2 p}{x^3}, & \text{якщо } x > 0 \end{cases}$$

при  $p=2,36$ . Значення  $x \in [-2, 2]$  і змінюється з кроком  $h=0,2$ .

18. Скласти схему алгоритму та програму табулювання функції  $y=x^3+x^2+0,8x+4$ , де  $x \in [-1, 1]$  і змінюється з кроком  $h=0,5$ .

19. Скласти схему алгоритму та програму табулювання функції  $y=x^3+x^2+0,8x+4$ , де  $x \in [-1, 1]$  і змінюється з кроком  $h=0,5$ .

20. Скласти схему алгоритму та програму введення масиву з 15 цілих чисел та виведення найменшого елемента масиву.

21. Скласти схему алгоритму та програму введення масиву з 10 цілих чисел та виведення найбільшого елемента масиву.

22. Скласти схему алгоритму та програму, що вводять з клавіатури послідовність з 8-ми чисел та знаходить її найбільший елемент.

23. Обчислити елементи квадратної матриці  $D$  за формулою:

$$d_{ij} = 2^{1-j} (|i - 4| + 2 \cdot |3,5 - j - 1,2|) (6 - 4j^2),$$

де  $i=1, \dots, n$ ;  $j=1, \dots, n$ ;  $n=6$ .

З матриці  $D$  отримати вектор сум елементів рядків. Обчислення виконати з використанням підпрограм.

24. Обчислити суму:

$$S = \sum_{i=1}^{\infty} \frac{1}{2^i}$$

Для усіх доданків більших заданої похибки  $\epsilon$ . Значення  $\epsilon=0,0001$  ввести з клавіатури.

25. Скласти схему алгоритму та програму, що вводять з клавіатури матрицю дійсних чисел розміром  $5 \times 5$  та знаходить кількість від'ємних чисел.

26. Скласти схему алгоритму та програму обчислення таблиці значень опору ланцюга  $R(t)$  за формулою:

$$R = \begin{cases} \cos^2(At) + \sqrt{t^2 + 1}, & t \leq 1; \\ \ln(t^2 + |t - 3|), & t > 1 \end{cases};$$

$t$  - змінюється від 0 до 2 із кроком 0,2. Значення  $A=3$  ввести з клавіатури.

27. Обчислити суму:

$$S = \sum_{i=1}^n \frac{i}{i+1} \prod_{k=i}^{n+1} \frac{i}{k+i}.$$

28. Скласти схему алгоритму та програму обчислення значення  $Y$ :

$$Y = \begin{cases} \operatorname{tg}^3 (cx^2 + 0.2x), & \text{якщо } x < 0 \\ \ln |c^2 - 1|, & \text{якщо } x = 0 \\ \frac{\cos^3 (c + x)}{2 + x^4}, & \text{якщо } x > 0 \end{cases}$$

при  $c=2.86$ . Значення  $x$  ввести з клавіатури.

29. Скласти схему алгоритму та програму обчислення значення суми:

$$S = \sum_{k=1}^{10} \frac{x^{4k+1}}{(4k+1)};$$

Значення  $x$  ввести з клавіатури.

30. Скласти схему алгоритму та програму обчислення значення суми:

$$S = \sum_{k=1}^{11} \frac{x^{2(k+1)}}{(k+1)!};$$

Значення  $x$  ввести з клавіатури.

31. Скласти схему алгоритму та програму обчислення значення суми:

$$S = \sum_{k=1}^{10} \frac{x^{2k}}{(k+1)!};$$

Значення  $x$  ввести з клавіатури.

32. Скласти схему алгоритму та програму обчислення значення суми:

$$S = \sum_{k=1}^{12} \frac{x^{2k+1}}{k!};$$

Значення  $x$  ввести з клавіатури.

33. Скласти схему алгоритму та програму обчислення значення суми:

$$S = \sum_{k=1}^7 \frac{(-1)^k \cdot x^{2k}}{(2k+3)!};$$

Значення  $x$  ввести з клавіатури.

34. Скласти схему алгоритму та програму обчислення значення суми:

$$s = \sum_{k=1}^6 \frac{x^k \cdot (k+3)}{(x^2 + 2 \cdot k)}.$$

Значення  $x$  ввести з клавіатури.

35. Скласти схему алгоритму та програму обчислення значення добутку:

Значення  $n$  ввести з клавіатури.

36. Скласти схему алгоритму та програму обчислення значення суми:

$$p = \prod_{i=1}^n (3i-1).$$

$$S = \sum_{k=1}^7 \frac{(2x)^k}{(2k)!};$$

Значення  $x$  ввести з клавіатури.

37. Скласти схему алгоритму та програму обчислення значення суми:

$$S = \sum_{k=1}^7 \frac{x^{2k+1}}{(2k+1)!};$$

Значення  $x$  ввести з клавіатури.

38. Скласти схему алгоритму та програму обчислення значення суми:

$$K = \sum_{i=1}^{11} \frac{x^{2i}}{(2i)!};$$

Значення  $x$  ввести з клавіатури.



39. Скласти схему алгоритму та програму табулювання функції  $y=\sin(x)$ , де  $x \in [2, 4]$  і змінюється з кроком  $h=0,5$ .
40. Скласти схему алгоритму та програму табулювання функції  $y=x^2 + 0,8x$ , де  $x \in [-2, 2]$  і змінюється з кроком  $h=0,5$ .
41. Скласти схему алгоритму та програму табулювання функції  $y=x^3+x^2+0,5$ , де  $x \in [-4,4]$  і змінюється з кроком  $h=0,5$ .
42. Скласти схему алгоритму та програму табулювання функції  $y=x^2+0,5x+3$ , де  $x \in [-3, 3]$  і змінюється з кроком  $h=0,5$ .
43. Скласти схему алгоритму та програму табулювання функції  $y=x^3+x^2+0,8x+4$ , де  $x \in [-1, 1]$  і змінюється з кроком  $h=0,5$ .
44. Скласти схему алгоритму та програму табулювання функції  $y=x^3+x^2+0,8x+4$ , де  $x \in [-1, 1]$  і змінюється з кроком  $h=0,5$ .
45. Скласти схему алгоритму та програму, що вводить з клавіатури послідовність з 6-ти цілих чисел та знаходить кількість п'ятірок у цій послідовності.

### Теорія інформації та кодування

1. Запишіть номер правильної, на Ваш погляд, відповіді:

Кількість символів алфавіту складає  $N = 32$ . Чому дорівнює ентропія повідомлення?

- 1) 4                      2) 5                      3) 6

Обґрунтуйте відповідь.

2. Запишіть номер правильної, на Ваш погляд, відповіді:

Яка із систем з багатократною передачею має кращу здатність виправляти помилки:

- 1) з мажоритарним прийомом;  
2) з мажоритарним посимвольним прийомом;

Обґрунтуйте відповідь.

3. Запишіть номер правильної, на Ваш погляд, відповіді:

Мінімальна кодова відстань  $d_0=5$ . Чому дорівнює кратність виправлення помилки?

- 1) 2      2) 3                      3) 4

Обґрунтуйте відповідь.

4. Запишіть номер правильної, на Ваш погляд, відповіді:

У системі передачі даних з інформаційним зворотнім зв'язком (ізз) оцінка якості прийнятого повідомлення приймачем прямого каналу виробляється на:

- 1) передавальній стороні прямого каналу;  
2) приймальній стороні прямого каналу;  
3) як на передавальній так й на приймальній сторонах прямого каналу.

Обґрунтуйте відповідь.

5. Запишіть номер правильної, на Ваш погляд, відповіді:

У системі передачі даних з вирішальним зворотнім зв'язком та очікуванням (взз-оч) чергова передача блоку інформації здійснюється лише після:

- 1) одержання сигналу підтвердження зворотнім зв'язком;  
2) одержання сигналу перезапиту зворотнім зв'язком;  
3) одержання будь-якого сигналу зворотнім зв'язком.

Обґрунтуйте відповідь.

6. Запишіть номер правильної, на Ваш погляд, відповіді:

Зворотній зв'язок у системах передачі даних необхідний для:

- 1) збільшення швидкості модуляції у каналі зв'язку;  
2) розширення функціональних можливостей апаратури;  
3) адаптації до зміни параметрів каналу зв'язку.

Обґрунтуйте відповідь.

7. Запишіть номер правильної, на Ваш погляд, відповіді:

У системі без зворотного зв'язку в основному використовується режим завадостійкого коду:

- 1) з виявленням помилок;  
2) з виправленням помилок;  
3) у комбінованому режимі.

Обґрунтуйте відповідь.

8. Запишіть номер правильної, на Ваш погляд, відповіді:

Ефективність системи передачі із зворотним зв'язком і виявленням помилок знижується при:

- 1) групуванні помилок в каналі;  
2) незалежному потоці помилок в каналі.

Обґрунтуйте відповідь.

9. Запишіть номер правильної, на Ваш погляд, відповіді:

У якому каналі передачі даних кратність появи помилок більша:

- 1) у каналі з групуванням помилок;
- 2) у каналі незалежними помилками.

Обґрунтуйте відповідь.

10. Імовірність прийому помилкової комбінації (комбінації, що містить хоча б одну помилку)  $p(\geq 1, n)$  довжиною  $n=12$  елементів з імовірністю помилки  $p_{\text{пом}}=0,00001$  складає:

1.  $1,20 \cdot 10^{-4}$ ;
2.  $1,19 \cdot 10^{-6}$ ;
3.  $1,19 \cdot 10^{-2}$ .

Обґрунтуйте відповідь.

11. Запишіть номера правильних, на Ваш погляд, відповідей:

Що відбувається в каналі при збільшенні коефіцієнту групування помилок  $\alpha$ :

- 1) кратність появи помилок в кодовій комбінації зменшується;
- 2) кратність появи помилок в кодовій комбінації збільшується;
- 3) вірогідність спотворення кодової комбінації зменшується;
- 4) вірогідність спотворення кодової комбінації збільшується;
- 5) число запитів в системі із зворотним зв'язком не міняється.

Обґрунтуйте відповідь.

12. Встановити відповідність відповідей у вигляді комбінації цифр та літер:

Імовірність помилки кодової комбінації  $p_{\text{пом } k}$  для каналу з незалежними помилками і при їхньому пакетуванні можна розрахувати за допомогою формули:

Формула Канал  
 1  $P_{\text{пом } l} \cong n p_{\text{пом}}$  А З незалежним розподілом помилок

2  $P_{\text{пом } l} = \sum_{t=1}^n C_n^t p_{\text{пом}}^t (1 - p_{\text{пом}})^{n-t}$  В З пакетуванням помилок

3  $P_{\text{пом } l} \cong n^{1-\alpha} p_{\text{пом}}$

1 2 3.

Обґрунтуйте відповідь.

13. Імовірність прийому помилкової комбінації (комбінації, що містить хоча б одну помилку)  $p(\geq 1, n)$  довжиною  $n=12$  елементів з імовірністю помилки  $p_{\text{пом}}=0,001$  складає:

- 1)  $1,19 \cdot 10^{-4}$
- 2)  $1,19 \cdot 10^{-6}$
- 3)  $1,20 \cdot 10^{-2}$

14. Запишіть номер правильної, на Ваш погляд, відповіді:

Кількість символів алфавіту складає  $N = 64$ . Чому дорівнює ентропія повідомлення?

- 1) 4
- 2) 5
- 3) 6

Обґрунтуйте відповідь.

15. Запишіть номер правильної, на Ваш погляд, відповіді:

Систем з багатократною передачею ( $S=5$ ) та мажоритарним поелементним прийомом гарантує кратність виправлення помилок у кодовому блоку  $k = 8$ :

- 1) 3;
- 2) 2;
- 3) 5.

Обґрунтуйте відповідь.

16. Запишіть номер правильної, на Ваш погляд, відповіді:

Мінімальна кодова відстань  $d_0=7$ . Чому дорівнює кратність виправлення помилок?

- 1) 2
- 2) 3
- 3) 4

Обґрунтуйте відповідь.

17. Запишіть номер правильної, на Ваш погляд, відповіді:

Ефективна швидкість передачі  $R$  у системі передачі даних з повним інформаційним зворотнім зв'язком (ізз)

- 1)  $>0,5$ ;
- 2)  $\leq 0,5$ ;
- 3)  $<0,5$ .

Обґрунтуйте відповідь.

18. Запишіть номер правильної, на Ваш погляд, відповіді:

У системі передачі даних з вирішальним зворотнім зв'язком та очікуванням (взз-оч) повторна передача блоку інформації здійснюється лише після:

- 1) одержання сигналу підтвердження зворотнім зв'язком;
- 2) одержання сигналу перезапиту зворотнім зв'язком;
- 3) одержання будь-якого сигналу зворотнім зв'язком.

Обґрунтуйте відповідь.

19. Запишіть номер правильної, на Ваш погляд, відповіді:

Зворотній зв'язок у системах передачі даних необхідний для:

- 1) збільшення швидкості модуляції у каналі зв'язку;
- 2) розширення функціональних можливостей апаратури;
- 3) адаптації до зміни параметрів каналу зв'язку.

Обґрунтуйте відповідь.

20. Запишіть номер правильної, на Ваш погляд, відповіді:

У системі без зворотного зв'язку в основному використовується режим завадостійкого коду:

- 1) з виявленням помилок;
- 2) з виправленням помилок;
- 3) у комбінованому режимі.

Обґрунтуйте відповідь.

21. Запишіть номер правильної, на Ваш погляд, відповіді:

Ефективність системи передачі із зворотним зв'язком і виявленням помилок знижується при:

- 1) групуванні помилок в каналі;
- 2) незалежному потоці помилок в каналі

Обґрунтуйте відповідь.

22. Запишіть номер правильної, на Ваш погляд, відповіді:

У якому каналі передачі даних кратність появи помилок більша:

- 1) у каналі з групуванням помилок;
- 2) у каналі незалежними помилками.

Обґрунтуйте відповідь.

23. Імовірність прийому помилкової комбінації (комбінації, що містить хочаб одну помилку)  $p(\geq 1, n)$  довжиною  $n=8$  елементів з імовірністю помилки  $p_{\text{пом}}=0,001$  складає:

1.  $1,19 \cdot 10^{-4}$
2.  $1,19 \cdot 10^{-6}$
3.  $8,00 \cdot 10^{-2}$

Обґрунтуйте відповідь.

24. Запишіть номери правильних, на Ваш погляд, відповідей:

Що відбувається в каналі при зменшенні коефіцієнту групування помилок  $\alpha$ :

- 1) кратність появи помилок в кодовій комбінації зменшується;
- 2) кратність появи помилок в кодовій комбінації збільшується;
- 3) вірогідність спотворення кодової комбінації зменшується;
- 4) вірогідність спотворення кодової комбінації збільшується;
- 5) число запитів в системі із зворотним зв'язком збільшується.

Обґрунтуйте відповідь.

25. Запишіть номер правильної, на Ваш погляд, відповіді:

Кількість символів алфавіту складає  $N = 16$ . Чому дорівнює ентропія повідомлення?

- 1) 4
- 2) 5
- 3) 6

Обґрунтуйте відповідь.

26. Запишіть номер правильної, на Ваш погляд, відповіді:

Яка із систем з багатократною передачею має кращу здатність виправляти помилки:

- 1) з мажоритарним поелементним прийомом;
- 2) з мажоритарним посимвольним прийомом;

Обґрунтуйте відповідь.

27. Запишіть номер правильної, на Ваш погляд, відповіді:

Мінімальна кодова відстань  $d_0=6$ . Чому дорівнює кратність виправлення помилки?

- 1) 2
- 2) 3
- 3) 4

Обґрунтуйте відповідь.

28. Запишіть номер правильної, на Ваш погляд, відповіді:

У системі передачі даних з інформаційним зворотнім зв'язком (ізз) оцінка якості прийнятого повідомлення приймачем прямого каналу виробляється на:

- 1) передавальній стороні прямого каналу;
- 2) приймальній стороні прямого каналу;
- 3) як на передавальній так й на приймальній сторонах прямого каналу.

Обґрунтуйте відповідь.

29. Запишіть номер правильної, на Ваш погляд, відповіді:

У системі передачі даних з вирішальним зворотнім зв'язком та очікуванням (взз-оч) чергова передача блоку інформації здійснюється лише після:

- 1) одержання сигналу підтвердження зворотнім зв'язком;
- 2) одержання сигналу перезапиту зворотнім зв'язком;
- 3) одержання будь-якого сигналу зворотнім зв'язком.

Обґрунтуйте відповідь.

30. Запишіть номери правильних, на Ваш погляд, відповідей:

Зворотній зв'язок у системах передачі даних необхідний для:

- 1) Формування сигналу зворотного зв'язку;
- 2) розширення функціональних можливостей апаратури;
- 3) адаптації до зміни параметрів каналу зв'язку.

Обґрунтуйте відповідь.

31. Запишіть номер правильної, на Ваш погляд, відповіді:

Ефективність системи передачі із зворотним зв'язком і виявленням помилок знижується при:

- 1) групуванні помилок в каналі;
- 2) незалежному потоці помилок в каналі

Обґрунтуйте відповідь.

32. Запишіть номер правильної, на Ваш погляд, відповіді:

У якому каналі передачі даних кратність появи помилок менша:

- 1) у каналі з групуванням помилок;
- 2) у каналі незалежними помилками

Обґрунтуйте відповідь.

33. Імовірність прийому помилкової комбінації (комбінації, що містить хоча б одну помилку)  $p(\geq 1, n)$  довжиною  $n=7$  елементів з імовірністю помилки  $p_{\text{ном}}=0,01$  складає:

- 1)  $1,19 \cdot 10^{-4}$
- 2)  $1,19 \cdot 10^{-6}$
- 3)  $7,00 \cdot 10^{-1}$

Обґрунтуйте відповідь.

34. Запишіть номери правильних, на Ваш погляд, відповідей:

Що відбувається при збільшенні у каналі коефіцієнту групування помилок  $\alpha$  :

- 1) кратність появи помилок в кодовій комбінації зменшується;
- 2) кратність появи помилок в кодовій комбінації збільшується;
- 3) вірогідність спотворення кодової комбінації зменшується;
- 4) вірогідність спотворення кодової комбінації збільшується;
- 5) число запитів в системі із зворотного зв'язку зменшується.

Обґрунтуйте відповідь.

35. Запишіть номер правильної, на Ваш погляд, відповіді:

Кількість символів алфавіту складає  $N = 128$ . Чому дорівнює ентропія повідомлення?

- 1) 4                    2) 5                    3) 7

Обґрунтуйте відповідь.

36. Запишіть номер правильної, на Ваш погляд, відповіді:

Яка із систем з багатократною передачею має кращу здатність виправляти помилки:

- 1) з мажоритарним поелементним прийомом;  
2) з мажоритарним посимвольним прийомом;

Обґрунтуйте відповідь.

37. Запишіть номер правильної, на Ваш погляд, відповіді:

Мінімальна кодова відстань  $d_0 = 9$ . Чому дорівнює кратність виправлення помилки?

- 1) 2    2) 3    3) 4

Обґрунтуйте відповідь.

38. Запишіть номер правильної, на Ваш погляд, відповіді:

У системі передачі даних з інформаційним зворотнім зв'язком (ізз) оцінка якості прийнятого повідомлення приймачем прямого каналу виробляється на:

- 1) передавальній стороні прямого каналу;  
2) приймальній стороні прямого каналу;  
3) як на передавальній так й на приймальній сторонах прямого каналу.

Обґрунтуйте відповідь.

39. Запишіть номер правильної, на Ваш погляд, відповіді:

У системі передачі даних з вирішальним зворотнім зв'язком та очікуванням (ВЗЗ-ОЧ) чергова передача блоку інформації здійснюється лише після:

- 1) одержання сигналу підтвердження зворотнім зв'язком;  
2) одержання сигналу перезапиту зворотнім зв'язком;  
3) одержання будь-якого сигналу зворотнім зв'язком.

Обґрунтуйте відповідь.

40. Запишіть номер правильної, на Ваш погляд, відповіді:

Зворотній зв'язок у системах передачі даних необхідний для:

- 1) збільшення швидкості модуляції у каналі зв'язку;  
2) розширення функціональних можливостей апаратури;  
3) адаптації до зміни параметрів каналу зв'язку.

Обґрунтуйте відповідь.

41. Запишіть номер правильної, на Ваш погляд, відповіді:

Кількість символів алфавіту складає  $N = 16$ . Чому дорівнює ентропія повідомлення?

- 1) 4                    2) 5                    3) 6

Обґрунтуйте відповідь.

42. Запишіть номер правильної, на Ваш погляд, відповіді:

Яка із систем з багатократною передачею має кращу здатність виправляти помилки:

- 1) з мажоритарним поелементним прийомом;  
2) з мажоритарним посимвольним прийомом;

Обґрунтуйте відповідь.

43. Запишіть номер правильної, на Ваш погляд, відповіді:

Мінімальна кодова відстань  $d_0 = 10$ . Чому дорівнює кратність виправлення помилки?

- 1) 2    2) 3                    3) 4

Обґрунтуйте відповідь.

44. Запишіть номер правильної, на Ваш погляд, відповіді:

У системі передачі даних з інформаційним зворотнім зв'язком (ізз) оцінка якості прийнятого повідомлення приймачем прямого каналу виробляється на:

- 1) передавальній стороні прямого каналу;  
2) приймальній стороні прямого каналу;  
3) як на передавальній так й на приймальній сторонах прямого каналу.

Обґрунтуйте відповідь.

45. Запишіть номер правильної, на Ваш погляд, відповіді:

У системі передачі даних з вирішальним зворотнім зв'язком та очікуванням (ВЗЗ-ОЧ) чергова передача блоку інформації здійснюється лише після:

- 1) одержання сигналу підтвердження зворотнім зв'язком;  
2) одержання сигналу перезапиту зворотнім зв'язком;  
3) одержання будь-якого сигналу зворотнім зв'язком.

Обґрунтуйте відповідь.

## Захист інформації в інформаційно-комунікаційних системах

- 1) Перерахувати заходи для підвищення захищеності останньої милі за технологією ADSL.
- 2) Написати правила брандмауера для ОС Linux, які відкривають 23 порт і 22 порт (і який сервіс, на вашу думку, працює через дані порти).
- 3) Який протокол авторизації і алгоритм шифрування використовується в rppp.
- 4) Який протокол авторизації та алгоритм шифрування використовується в WEP.
- 5) Які кроки треба зробити для забезпечення захисту інфокомунікаційної системи банку (коротко, пункти).
- 6) Перерахувати заходи для підвищення захищеності останньої милі за технологією DOCSIS.
- 7) Написати правила брандмауера Cisco, які відкривають 21 порт і 25 порт (і який сервіс, на вашу думку, працює через дані порти).
- 8) Який протокол авторизації та алгоритм шифрування використовується в rppoe.
- 9) Який протокол авторизації та алгоритм шифрування використовується в WPA.
- 10) Які кроки треба зробити для забезпечення захисту мережевої інфраструктури середнього підприємства (коротко, пункти).
- 11) Перерахувати заходи для підвищення захищеності останньої милі за технологією WIFI.
- 12) Написати правила брандмауера Cisco, які відкривають 139 порт і 138 порт (і який сервіс, на вашу думку, працює через дані порти).
- 13) Який протокол авторизації та алгоритм шифрування використовується в l2tp.
- 14) Який протокол авторизації та алгоритм шифрування використовується в WPA-2.
- 15) Перерахувати заходи для підвищення захищеності останньої милі за технологією Ethernet.
- 16) Який протокол авторизації та алгоритм шифрування використовується в ipsec.
- 17) Який протокол авторизації та алгоритм шифрування використовується в WEP.
- 18) Які кроки треба зробити для підвищення захисту інформації в SDH, PDH.
- 19) Перерахувати заходи підвищення захищеності останньої милі за технологією WiMAX.
- 20) Написати правила брандмауера для ОС Linux, які закривають 22 порт і 23 порт (і який, на вашу думку, сервіс працює через дані порти).
- 21) Який протокол авторизації та алгоритм шифрування використовується в rppp.
- 22) Який протокол авторизації та алгоритм шифрування використовується в WPA-2.
- 23) Які кроки треба зробити для підвищення захисту інформації в телефонних мережах зв'язку.
- 24) Засоби підвищення захищеності останньої милі за технологією PRI, E1.
- 25) Який протокол авторизації та алгоритм шифрування використовується в rppoe.
- 26) Який протокол авторизації та алгоритм шифрування використовується в WPA-2.
- 27) Які кроки треба зробити для підвищення захисту інформації в мережах дата центрів.
- 29) Перерахувати заходи підвищення захищеності останньої милі за технологією SDH.
- 30) Написати правила брандмауера для ОС Linux, які відкривають 137 порт, і правила, котрі закривають 21 порт на обладнанні CISCO (і який сервіс працює, на вашу думку, через дані порти).
- 31) Який протокол авторизації та алгоритм шифрування використовується в WPA.
- 32) Які кроки потрібні для підвищення захисту інформації в віртуальних машинах 1 типу.
- 33) Перерахувати заходи підвищення захищеності останньої милі за технологією PDH.
- 34) Написати правила брандмауера для ОС Linux, які закривають 445 порт, і правила, котрі закривають 21 порт на обладнанні CISCO (і який сервіс працює, на вашу думку, через дані порти).
- 35) Який протокол авторизації та алгоритм шифрування використовується в rppoe.
- 36) Які кроки треба зробити для підвищення захисту інформації в BGP.
- 37) Перерахувати заходи підвищення захищеності технології WDM.
- 38) Який протокол авторизації та алгоритм шифрування використовується в OSPF.
- 39) Які засоби застосувати для забезпечення захисту доступу до комп'ютерного мережі та обладнання середнього підприємства (коротко, пункти).
- 45) Перерахувати заходи підвищення захищеності протоколу RIP.
- 46) Який протокол авторизації та алгоритм шифрування використовується в ipsec.
- 47) Який протокол авторизації та алгоритм шифрування використовується в DWDM.
- 48) Які кроки треба зробити для підвищення захисту інформації в DOCSIS v.2.
- 49) Який протокол авторизації та алгоритм шифрування використовується в статичній маршрутизації.
- 50) Які кроки треба зробити для підвищення захисту інформації в віртуальних машинах 2 типу.



26. Створити сеансовий ключ за допомогою алгоритму Діффі-Хелмана за умовами: просте число  $P=1019$ , мантиса  $d=59$ , секретні ключі абонентів  $x_1=116$ ,  $x_2=217$ .
27. Створити сеансовий ключ за допомогою алгоритму Діффі-Хелмана за умовами: просте число  $P=1019$ , мантиса  $d=61$ , секретні ключі абонентів  $x_1=117$ ,  $x_2=216$ .
28. Створити сеансовий ключ за допомогою алгоритму Діффі-Хелмана за умовами: просте число  $P=1019$ , мантиса  $d=67$ , секретні ключі абонентів  $x_1=118$ ,  $x_2=215$ .
29. Вирахувати секретний ключ RSA за умовами: прості числа  $p=19$ ,  $q=23$  відкритий ключ  $d=\{57,99,329\}$  (обрати один правильний з 3-х).
30. Вирахувати секретний ключ RSA за умовами: прості числа  $p=19$ ,  $q=29$  відкритий ключ  $d=\{49,65,123\}$  (обрати один правильний з 3-х).
31. Вирахувати секретний ключ RSA за умовами: прості числа  $p=19$ ,  $q=31$  відкритий ключ  $d=\{49,111,255\}$  (обрати один правильний з 3-х).
32. Вирахувати секретний ключ RSA за умовами: прості числа  $p=19$ ,  $q=37$  відкритий ключ  $d=\{65,87,201\}$  (обрати один правильний з 3-х).
33. Вирахувати секретний ключ RSA за умовами: прості числа  $p=19$ ,  $q=41$  відкритий ключ  $d=\{55,111,221\}$  (обрати один правильний з 3-х).
34. Вирахувати секретний ключ RSA за умовами: прості числа  $p=19$ ,  $q=43$  відкритий ключ  $d=\{93,155,217\}$  (обрати один правильний з 3-х).
35. Вирахувати секретний ключ RSA за умовами: прості числа  $p=19$ ,  $q=47$  відкритий ключ  $d=\{51,133,161\}$  (обрати один правильний з 3-х).
36. Вирахувати секретний ключ RSA за умовами: прості числа  $p=19$ ,  $q=53$  відкритий ключ  $d=\{55,93,247\}$  (обрати один правильний з 3-х).
37. Вирахувати секретний ключ RSA за умовами: прості числа  $p=19$ ,  $q=59$  відкритий ключ  $d=\{69,91,145\}$  (обрати один правильний з 3-х).
38. Вирахувати секретний ключ RSA за умовами: прості числа  $p=19$ ,  $q=61$  відкритий ключ  $d=\{85,119,333\}$  (обрати один правильний з 3-х).
39. Вирахувати секретний ключ RSA за умовами: прості числа  $p=19$ ,  $q=67$  відкритий ключ  $d=\{51,65,231\}$  (обрати один правильний з 3-х).
40. Розрахувати ключі шифру Ель-Гамалю і зашифрувати повідомлення  $M=101$  за умовами: просте число  $p=587$  мантиса  $w=41$  секретний ключ  $x=35$  випадковий параметр  $k=79$ .
41. Розрахувати ключі шифру Ель-Гамалю і зашифрувати повідомлення  $M=101$  за умовами: просте число  $p=563$  мантиса  $w=41$  секретний ключ  $x=35$  випадковий параметр  $k=67$ .
42. Розрахувати ключі шифру Ель-Гамалю і зашифрувати повідомлення  $M=101$  за умовами: просте число  $p=503$  мантиса  $w=31$  секретний ключ  $x=35$  випадковий параметр  $k=59$ .
43. Розрахувати ключі шифру Ель-Гамалю і зашифрувати повідомлення  $M=101$  за умовами: просте число  $p=479$  мантиса  $w=43$  секретний ключ  $x=35$  випадковий параметр  $k=53$ .
44. Розрахувати ключі шифру Ель-Гамалю і зашифрувати повідомлення  $M=101$  за умовами: просте число  $p=467$  мантиса  $w=31$  секретний ключ  $x=35$  випадковий параметр  $k=61$ .
45. Розрахувати ключі шифру Ель-Гамалю і зашифрувати повідомлення  $M=101$  за умовами: просте число  $p=383$  мантиса  $w=47$  секретний ключ  $x=35$  випадковий параметр  $k=43$ .
46. Розрахувати ключі шифру Ель-Гамалю і зашифрувати повідомлення  $M=101$  за умовами: просте число  $p=587$  мантиса  $w=37$  секретний ключ  $x=35$  випадковий параметр  $k=69$ .
47. Розрахувати ключі шифру Ель-Гамалю і зашифрувати повідомлення  $M=101$  за умовами: просте число  $p=563$  мантиса  $w=43$  секретний ключ  $x=35$  випадковий параметр  $k=61$ .
48. Розрахувати ключі шифру Ель-Гамалю і зашифрувати повідомлення  $M=101$  за умовами: просте число  $p=503$  мантиса  $w=37$  секретний ключ  $x=35$  випадковий параметр  $k=53$ .
49. Розрахувати ключі шифру Ель-Гамалю і зашифрувати повідомлення  $M=101$  за умовами: просте число  $p=479$  мантиса  $w=47$  секретний ключ  $x=35$  випадковий параметр  $k=59$ .
50. Розрахувати ключі шифру Ель-Гамалю і зашифрувати повідомлення  $M=101$  за умовами: просте число  $p=467$  мантиса  $w=37$  секретний ключ  $x=35$  випадковий параметр  $k=67$ .



## Комплексні системи захисту інформації: Проектування, впровадження, супровід

1. Основи, напрямки та етапи побудови систем захисту інформації.
2. Нормативно-правові акти України щодо створення комплексної системи захисту інформації.
3. Положення про службу захисту інформації в інформаційно-телекомунікаційних системах.
4. Порядок проведення робіт із створення комплексної системи захисту інформації.
5. Функції служби захисту інформації під час створення комплексної системи захисту інформації.
6. Функції служби захисту інформації під час експлуатації комплексної системи захисту інформації.
7. Структура та зміст Плану захисту інформації в інформаційно-телекомунікаційних системах.
8. Основні етапи створення комплексної системи захисту інформації.
9. Формування загальних вимог до комплексної системи захисту інформації в інформаційно-телекомунікаційних системах.
10. Обґрунтування необхідності створення комплексної системи захисту інформації.
11. Порядок проведення категоріювання інформаційно-телекомунікаційної системи.
12. Обстеження середовищ функціонування інформаційно-телекомунікаційної системи.
13. Розробка моделі порушника безпеки інформації в інформаційно-телекомунікаційних системах.
14. Модель загроз для інформації в інформаційно-телекомунікаційних системах.
15. Формування завдання на створення комплексної системи захисту інформації в інформаційно-телекомунікаційних системах.
16. Розробка політики безпеки інформації в інформаційно-телекомунікаційних системах.
17. Розробка технічного завдання на створення комплексної системи захисту інформації.
18. Які проектні рішення обґрунтовуються і приймаються при розробці проекту.
19. Що включається в робочу і експлуатаційну документацію на етапі розробки робочого проекту.
20. Які документи повинен містити проект КСЗІ при об'єднанні робочого і технічного проекту.
21. Які ставляться завдання на етапі підготовки КСЗІ до введення в дію.
22. Що повинно бути враховано в Інструкції про порядок обробки в ІТС службової інформації.
23. Що повинні визначати посадові інструкції. З яких розділів складається посадова інструкція співробітника КСЗІ.
24. Які інструкції повинні бути розроблені для засобів криптографічного захисту й за яких умов вони не потрібні.
25. Які заходи захисту від ПЕМВН (побічні електромагнітні випромінювання і наведення) здійснюються в приміщеннях, де встановлені технічні засоби ІТС.
26. Які заходи є метою пусконаладжувальних робіт.
27. Які відомості містить програма випробувань КСЗІ в ІТС.
28. Які повинна містити розділи програма випробувань.
29. Що включає в себе перевірка впроваджених в ІТС заходів захисту інформації від несанкціонованого доступу.
30. Що включає в себе перевірка впроваджених в ІТС заходів антивірусного захисту інформації.
31. Що включає в себе перевірка порядку поводження з носіями інформації.
32. Що включає в себе перевірка підготовленості персоналу та інших організаційних заходів.
33. Які заходи здійснюються при дослідній експлуатації КСЗІ.
34. Які вказівки розробляються при дослідній експлуатації КСЗІ.
35. З яких розділів складається акт завершення дослідної експлуатації КСЗІ.
36. Яка мета наукової і науково-технічної експертизи.
37. Які види державної експертизи КСЗІ в ІТС.
38. Які вимоги до експертного висновку.
39. Який порядок організації і проведення експертизи.
40. Який порядок надання Експертного висновку та Атестату на засіб ТЗІ.
41. Який порядок проведення експертиз КСЗІ державними органами.
42. Які реєстри формує і веде Адміністрація Держспецзв'язку.
43. Які роботи виконуються персоналом під час супроводу КСЗІ.
44. Які є заходи по роботі з кадрами в Календарному плані робіт із захисту інформації в ІТС.
45. Які функції повинна виконувати служба захисту інформації в ІТС в процесі супроводу КСЗІ.
46. Що входить до складу супровідної документації КСЗІ згідно з вимогами НД ТЗІ.
47. Які функції покладаються на адміністратора безпеки під час супроводу КСЗІ.
48. Які функції покладаються на системного адміністратора під час супроводу КСЗІ.
49. Які обов'язки лежать на користувачах при супроводі КСЗІ.
50. Які питання перевіряються під час планових та позапланових перевірок.

**Перелік запитань до вступних випробувань для осіб, що виявили бажання продовжити навчання для здобуття ступеня магістра**

**За спеціальністю: 125 «Кібербезпека»**

(спеціалізацією: Системи технічного захисту інформації, автоматизація її обробки)

**Інформаційні технології**

1. Скласти схему алгоритму та програму обчислення значення  $Y$ :

$$Y = \begin{cases} \operatorname{tg}^3 (cx^2 + 0.2x), & \text{якщо } x < 0 \\ \ln |c^2 - 1|, & \text{якщо } x = 0 \\ \frac{\cos^3 (c + x)}{2 + x^4}, & \text{якщо } x > 0 \end{cases}$$

при  $c = 2.86$ . Значення  $x$  ввести з клавіатури.

2. Скласти схему алгоритму та програму обчислення значення суми:

$$S = \sum_{k=1}^{10} \frac{x^{4k+1}}{(4k+1)!};$$

Значення  $x$  ввести з клавіатури.

3. Скласти схему алгоритму та програму обчислення значення суми:

$$S = \sum_{k=1}^{11} \frac{x^{2(k+1)}}{(k+1)!};$$

Значення  $x$  ввести з клавіатури.

4. Скласти схему алгоритму та програму обчислення значення суми:

$$S = \sum_{k=1}^{10} \frac{x^{2k}}{(k+1)!};$$

Значення  $x$  ввести з клавіатури.

5. Скласти схему алгоритму та програму обчислення значення суми:

$$S = \sum_{k=1}^{12} \frac{x^{2k+1}}{k!};$$

Значення  $x$  ввести з клавіатури.

6. Скласти схему алгоритму та програму обчислення значення суми:

$$S = \sum_{k=1}^7 \frac{(-1)^k \cdot x^{2k}}{(2k+3)!};$$

Значення  $x$  ввести з клавіатури.

7. Скласти схему алгоритму та програму обчислення значення добутку:

$$p = \prod_{i=1}^n (3i - 1).$$

Значення  $n$  ввести з клавіатури.

8. Скласти схему алгоритму та програму обчислення значення суми:

$$S = \sum_{k=1}^7 \frac{(2x)^k}{(2k)!};$$

Значення  $x$  ввести з клавіатури.

9. Скласти схему алгоритму та програму обчислення значення суми:

$$S = \sum_{k=1}^{11} \frac{x^{3k+1}}{(3k+1)!};$$

Значення  $x$  ввести з клавіатури.

10. Скласти схему алгоритму та програму обчислення значення суми:

$$S = \sum_{k=1}^7 \frac{x^{2k+1}}{(2k+1)!};$$

Значення  $x$  ввести з клавіатури.

11. Скласти схему алгоритму та програму обчислення значення суми:

$$K = \sum_{i=1}^{11} \frac{x^{2i}}{(2i)!};$$

Значення  $x$  ввести з клавіатури.

12. Скласти схему алгоритму та програму табулювання функції  $y=\sin(x)$ , де  $x \in [2, 4]$  і змінюється з кроком  $h=0,5$ .

13. Скласти схему алгоритму та програму табулювання функції  $y=\sin(x)$ , де  $x \in [2, 4]$  і змінюється з кроком  $h=0,5$ .

14. Скласти схему алгоритму та програму табулювання функції  $y=x^2 + 0,8x$ , де  $x \in [-2, 2]$  і змінюється з кроком  $h=0,5$ .

15. Скласти схему алгоритму та програму табулювання функції  $y=x^3+x^2+0,5$ , де  $x \in [-4,4]$  і змінюється з кроком  $h=0,5$ .

16. Скласти схему алгоритму та програму табулювання функції  $y=x^2+0,5x+3$ , де  $x \in [-3, 3]$  і змінюється з кроком  $h=0,5$ .

17. Скласти схему алгоритму та програму табулювання функції  $y$ :

$$y = \begin{cases} \sqrt{p + \sin^2 x}, & \text{якщо } x < 0 \\ e^{p^2+p}, & \text{якщо } x = 0 \\ \frac{3 \cdot x + \sin^2 p}{x^3}, & \text{якщо } x > 0 \end{cases}$$

при  $p=2,36$ . Значення  $x \in [-2, 2]$  і змінюється з кроком  $h=0,2$ .

18. Скласти схему алгоритму та програму табулювання функції  $y=x^3+x^2+0,8x+4$ , де  $x \in [-1, 1]$  і змінюється з кроком  $h=0,5$ .

19. Скласти схему алгоритму та програму табулювання функції  $y=x^3+x^2+0,8x+4$ , де  $x \in [-1, 1]$  і змінюється з кроком  $h=0,5$ .

20. Скласти схему алгоритму та програму введення масиву з 15 цілих чисел та виведення найменшого елемента масиву.

21. Скласти схему алгоритму та програму введення масиву з 10 цілих чисел та виведення найбільшого елемента масиву.

22. Скласти схему алгоритму та програму, що вводить з клавіатури послідовність з 8-ми чисел та знаходить її найбільший елемент.

23. Обчислити елементи квадратної матриці  $D$  за формулою:

$$d_{ij} = 2^{1-j} (|i - 4| + 2 \cdot |3,5 - j - 1,2|) (6 - 4j^2),$$

де  $i=1, \dots, n$ ;  $j=1, \dots, n$ ;  $n=6$ .

З матриці  $D$  отримати вектор сум елементів рядків. Обчислення виконати з використанням підпрограм.

24. Обчислити суму:

$$S = \sum_{i=1}^{\infty} \frac{1}{2i}$$

Для усіх доданків більших заданої похибки  $\epsilon_{ps}$ . Значення  $\epsilon_{ps}=0,0001$  ввести з клавіатури.

25. Скласти схему алгоритму та програму, що вводить з клавіатури матрицю дійсних чисел розміром  $5 \times 5$  та знаходить кількість від'ємних чисел.

26. Скласти схему алгоритму та програму обчислення таблиці значень опору ланцюга  $R(t)$  за формулою:

$$R = \begin{cases} \cos^2(At) + \sqrt{t^2 + 1}, & t \leq 1 \\ \ln(t^2 + |t - 3|), & t > 1 \end{cases};$$

$t$  - змінюється від 0 до 2 із кроком 0,2. Значення  $A=3$  ввести з клавіатури.

27. Обчислити суму:

$$S = \sum_{i=1}^n \frac{i}{i+1} \prod_{k=i}^{n+1} \frac{i}{k+i}$$

28. Скласти схему алгоритму та програму обчислення значення  $Y$ :

$$Y = \begin{cases} \operatorname{tg}^3 (cx^2 + 0.2x), & \text{якщо } x < 0 \\ \ln |c^2 - 1|, & \text{якщо } x = 0 \\ \frac{\cos^3 (c + x)}{2 + x^4}, & \text{якщо } x > 0 \end{cases}$$

при  $c=2.86$ . Значення  $x$  ввести з клавіатури.

29. Скласти схему алгоритму та програму обчислення значення суми:

$$S = \sum_{k=1}^{10} \frac{x^{4k+1}}{(4k+1)!};$$

Значення  $x$  ввести з клавіатури.

30. Скласти схему алгоритму та програму обчислення значення суми:

$$S = \sum_{k=1}^{11} \frac{x^{2(k+1)}}{(k+1)!};$$

Значення  $x$  ввести з клавіатури.

31. Скласти схему алгоритму та програму обчислення значення суми:

$$S = \sum_{k=1}^{10} \frac{x^{2k}}{(k+1)!};$$

Значення  $x$  ввести з клавіатури.

32. Скласти схему алгоритму та програму обчислення значення суми:

$$S = \sum_{k=1}^{12} \frac{x^{2k+1}}{k!};$$

Значення  $x$  ввести з клавіатури.

33. Скласти схему алгоритму та програму обчислення значення суми:

$$S = \sum_{k=1}^7 \frac{(-1)^k \cdot x^{2k}}{(2k+3)!};$$

Значення  $x$  ввести з клавіатури.

34. Скласти схему алгоритму та програму обчислення значення суми:

$$s = \sum_{k=1}^6 \frac{x^k \cdot (k+3)}{(x^2 + 2 \cdot k)}.$$

Значення  $x$  ввести з клавіатури.

35. Скласти схему алгоритму та програму обчислення значення добутку:

$$p = \prod_{i=1}^n (3i-1).$$

Значення  $n$  ввести з клавіатури.

36. Скласти схему алгоритму та програму обчислення значення суми:

$$S = \sum_{k=1}^7 \frac{(2x)^k}{(2k)!};$$

Значення  $x$  ввести з клавіатури.

37. Скласти схему алгоритму та програму обчислення значення суми:

$$S = \sum_{k=1}^7 \frac{x^{2k+1}}{(2k+1)!};$$

Значення  $x$  ввести з клавіатури.

38. Скласти схему алгоритму та програму обчислення значення суми:

$$K = \sum_{i=1}^{11} \frac{x^{2i}}{(2i)!};$$

Значення  $x$  ввести з клавіатури.

39. Скласти схему алгоритму та програму табулювання функції  $y=\sin(x)$ , де  $x \in [2, 4]$  і змінюється з кроком  $h=0,5$ .
40. Скласти схему алгоритму та програму табулювання функції  $y=x^2 + 0,8x$ , де  $x \in [-2, 2]$  і змінюється з кроком  $h=0,5$ .
41. Скласти схему алгоритму та програму табулювання функції  $y=x^3+x^2+0,5$ , де  $x \in [-4,4]$  і змінюється з кроком  $h=0,5$ .
42. Скласти схему алгоритму та програму табулювання функції  $y=x^2+0,5x+3$ , де  $x \in [-3, 3]$  і змінюється з кроком  $h=0,5$ .
43. Скласти схему алгоритму та програму табулювання функції  $y=x^3+x^2+0,8x+4$ , де  $x \in [-1, 1]$  і змінюється з кроком  $h=0,5$ .
44. Скласти схему алгоритму та програму табулювання функції  $y=x^3+x^2+0,8x+4$ , де  $x \in [-1, 1]$  і змінюється з кроком  $h=0,5$ .
45. Скласти схему алгоритму та програму, що вводить з клавіатури послідовність з 6-ти цілих чисел та знаходить кількість п'ятірок у цій послідовності.

### Безпека інформаційних та комунікаційних систем

1. Визначення понять: механізм захисту, безпека ОС. Особливості, які дозволяють визначити питання забезпечення безпеки ОС.
2. Типові функціональні дефекти ОС, які можуть привести до створення каналів витоку даних.
3. Допоміжні засоби захисту (засоби моніторингу, профілактичного контролю та аудиту).
4. Контроль доступу до даних. Логічне управління доступом.
5. Довільне управління доступом та його недоліки.
6. Вимоги до забезпечення захисту інформації в інформаційній, телекомунікаційній та Централізована модель адміністрування механізмів захисту.
7. Захисні механізми ОС сімейства UNIX (побудова файлової системи і розмежування доступу до файлових об'єктів).
8. Недоліки захисних механізмів ОС сімейства UNIX.
9. Відмінності та подібність захисних механізмів ОС сімейства Windows від ОС сімейства UNIX.
10. Принципові недоліки захисних механізмів у ОС сімейства Windows.
11. Концепція реалізації розмежувальної політики доступу до ресурсів.
12. Механізм замкнутості програмного середовища.
13. Класифікація загроз та їх зв'язок з недоліками засобів захисту операційних систем.
14. Які основні можливості захисту надають інструменти безпеки ОС Windows NT.
15. Функції безпеки Windows NT.
16. Сервер автентифікації Kerberos.
17. Засоби мережевої безпеки Windows Server 2003.
18. Протоколи забезпечення безпеки. Протокол Kerberos
19. Протокол NTLM. Інтерактивний вхід в систему у відповідності з протоколом NTLM.
20. Протокол IPSec і його функції.
21. Структура протоколу IPSec.
22. Функції протоколів AH и ESP.
23. Функції протоколу IKE.
24. Протокол SSL/TLS. Захист даних за допомогою SSL/TLS.
25. Визначення реєстру Windows. Структура реєстру.
26. Функції безпеки Windows NT.
27. Локальна політика безпеки та її склад.
28. Перелічіть та опишіть основні типи загроз комп'ютерної системи згідно НД ТЗИ 2.5-004-99 «Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу.»
29. Протоколи забезпечення безпеки. Протокол Kerberos.
30. Протокол NTLM. Інтерактивний вхід в систему у відповідності з протоколом NTLM.
31. Структура протоколу IPSec.
32. Функції протоколів AH и ESP.
33. Функції протоколу IKE.
34. Протокол SSL/TLS. Захист даних за допомогою SSL/TLS.
35. Визначення реєстру Windows. Структура реєстру.
36. Функції безпеки Windows NT.
37. Локальна політика безпеки та її склад.
38. Перелічіть та опишіть основні типи загроз комп'ютерної системи згідно НД ТЗИ 2.5-004-99 «Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу.»
39. Протоколи забезпечення безпеки. Протокол Kerberos.
40. Протокол NTLM. Інтерактивний вхід в систему у відповідності з протоколом NTLM.
41. Визначення понять: механізм захисту, безпека ОС. Особливості, які дозволяють визначити питання забезпечення безпеки ОС.
42. Типові функціональні дефекти ОС, які можуть привести до створення каналів витоку даних.
43. Допоміжні засоби захисту (засоби моніторингу, профілактичного контролю та аудиту).
44. Контроль доступу до даних. Логічне управління доступом.
45. Довільне управління доступом та його недоліки.

**Криптографія та стеганографія**

1. Розшифрувати криптограму зашифровану шифром Віженера за допомогою ключового слова *криптографія*.

К Б Р Ї Ю У Х А И Л Х Ь П Ь Ш Ч Б Ъ С Б И Е Ъ Д Ц Л

2. Розшифрувати криптограму зашифровану шифром Гронсфеля за допомогою ключової послідовності 2709164835.

М Ч И Ш У Ф З Ш Г Щ К Ю Е Ь Л О Й Ф И Ч Р Л Ї Р Б Я М Ь Ю

3. Розшифрувати текст В Ш А С Ф Н И В А Р О Е И О Л З, зашифрований за допомогою «магічного квадрата».

|    |    |    |    |
|----|----|----|----|
| 16 | 3  | 2  | 13 |
| 5  | 10 | 11 | 8  |
| 9  | 6  | 7  | 12 |
| 4  | 15 | 14 | 1  |

4. Розшифруйте повідомлення О И Р М Е О С Ю В Т А Ь Л Г О П, отримане за допомогою «магічного квадрата».

|    |    |    |    |
|----|----|----|----|
| 16 | 3  | 2  | 13 |
| 5  | 10 | 11 | 8  |
| 9  | 6  | 7  | 12 |
| 4  | 15 | 14 | 1  |

5. Криптограма Т Ю А Е О О Г М Р Л И П О Ь С В отримана засобом подвійної перестановки. Ключем шифру слугує послідовність номерів стовпців 4132 і номерів рядків 3142 таблиці. Шифр текст вписувати порядково.

6. Розшифрувати криптограму П Ы Й У Щ И Э С С Е К Ъ Х Л Н, зашифровану шифром Гронсфеля за допомогою ключової послідовності 0,12,1,16,14,7,8,31.

7. Розшифрувати криптограму Д Х Т Ъ Р Ю О Г Л Д Л Щ С Ч Ж Щ У, зашифровану шифром Гронсфеля за допомогою ключової послідовності 2,7,1,8.

8. Розшифрувати криптограму П Д К З Ы В З Ч Ш Л Ы Й С Й за допомогою таблиці Трисеміуса розміром 4x8 для російського алфавіту. У якості ключа – слово БАНДЕРОЛЬ.

9. Розшифруйте повідомлення У И Р Д З Е Г Ю С Ж А О Е Я Н П, отримане за допомогою «магічного квадрата»

|    |    |    |    |
|----|----|----|----|
| 16 | 3  | 2  | 13 |
| 5  | 10 | 11 | 8  |
| 9  | 6  | 7  | 12 |
| 4  | 15 | 14 | 1  |

10. Розшифруйте текст П С О С Н С, отриманий за допомогою шифра Цезаря для російської мови.

11. Розшифрувати криптограму, зашифровану шифром Віженера за допомогою ключового слова *криптографія*.

К Б Р Ї Ю У Х А И Л Х Ь П Ь Ш Ч Б Ъ С Б И Е Ъ Д Ц Л

12. Розшифрувати криптограму, зашифровану шифром Гронсфеля за допомогою ключової послідовності 2709164835.

М Ч И Ш У Ф З Ш Г Щ К Ю Е Ь Л О Й Ф И Ч Р Л Ї Р Б Я М Ь Ю

13. Розшифрувати текст В Ш А С Ф Н И В А Р О Е И О Л З, зашифрований за допомогою «магічного квадрата».

|    |    |    |    |
|----|----|----|----|
| 16 | 3  | 2  | 13 |
| 5  | 10 | 11 | 8  |
| 9  | 6  | 7  | 12 |
| 4  | 15 | 14 | 1  |

14. Розшифруйте повідомлення О И Р М Е О С Ю В Т А Ь Л Г О П, отримане за допомогою «магічного квадрата».

|    |    |    |    |
|----|----|----|----|
| 16 | 3  | 2  | 13 |
| 5  | 10 | 11 | 8  |
| 9  | 6  | 7  | 12 |
| 4  | 15 | 14 | 1  |

15. Криптограма Т Ю А Е О О Г М Р Л И П О Ь С В отримана засобом подвійної перестановки. Ключем шифру виступає послідовність стовпців 4132 і номерів рядків 3142 таблиці. Шифртекст вписувати порядково.

16. Розшифрувати криптограму П Ы Й У Щ И Э С С Е К Ъ Х Л Н, зашифровану шифром Гронсфеля за допомогою ключової послідовності 0,12,1,16,14,7,8,31.

17. Розшифрувати криптограму Д Х Т Ъ Р Ю О Г Л Д Л Щ С Ч Ж Щ У, зашифровану шифром Гронсфеля за допомогою ключової послідовності 2,7,1,8.

18. Розшифрувати криптограму П Д К З Ы В З Ч Ш Л Ы Й С Й за допомогою таблиці Трисеміуса розміром 4x8 для російського алфавіту. В якості ключа – слово БАНДЕРОЛЬ.

19. Розшифруйте повідомлення УИРДЗЕГЮСЖАОЕЯНП, отримане за допомогою «магічного квадрата».

|    |    |    |    |
|----|----|----|----|
| 16 | 3  | 2  | 13 |
| 5  | 10 | 11 | 8  |
| 9  | 6  | 7  | 12 |
| 4  | 15 | 14 | 1  |

20. Розшифруйте текст ПСОСНС, отриманий за допомогою шифру Цезаря для російської мови.

21. Розшифрувати криптограму, зашифровану шифром Віженера за допомогою ключового слова *криптография*.

К Б Р Ы Ю У Х А И Л Х Ъ П Ъ Ш Ч Б Ъ С Б И Е Ъ Д Ц Л

22. Розшифрувати криптограму, зашифровану шифром Гронсфельда за допомогою ключової послідовності 2709164835.

М Ч И Ш У Ф З Ш Г Щ К Ю Е Ъ Л О Й Ф И Ч Р Л Ы Р Б Я М Ь Ю

23. Розшифрувати текст В Ш А С Ф Н И В А Р О Е И О Л З, зашифрований за допомогою «магічного квадрата».

|    |    |    |    |
|----|----|----|----|
| 16 | 3  | 2  | 13 |
| 5  | 10 | 11 | 8  |
| 9  | 6  | 7  | 12 |
| 4  | 15 | 14 | 1  |

24. Розшифруйте повідомлення О И Р М Е О С Ю В Т А Ь Л Г О П, отримане за допомогою «магічного квадрата».

|    |    |    |    |
|----|----|----|----|
| 16 | 3  | 2  | 13 |
| 5  | 10 | 11 | 8  |
| 9  | 6  | 7  | 12 |
| 4  | 15 | 14 | 1  |

25. Криптограма Т Ю А Е О О Г М Р Л И П О Ъ С В, отримана засобом подвійної перестановки. Ключем до шифру слугує послідовність номерів стовпців 4132 і номерів рядків 3142 таблиці. Шифртекст вписувати порядково.

26. Розшифрувати криптограму ПЪЙЫУЩИЭССЕКЪХЛН, зашифровану шифром Гронсфельда за допомогою ключової послідовності 0,12,1,16,14,7,8,31.

27. Розшифрувати криптограму ПДКЗЫВЗЧШЛЫЙСЙ за допомогою таблиці Трисеміуса розміром 4x8 для російського алфавіту. В якості ключа – слово БАНДЕРОЛЬ

28. Розшифруйте повідомлення УИРДЗЕГЮСЖАОЕЯНП, отримане за допомогою «магічного квадрата»

|    |    |    |    |
|----|----|----|----|
| 16 | 3  | 2  | 13 |
| 5  | 10 | 11 | 8  |
| 9  | 6  | 7  | 12 |
| 4  | 15 | 14 | 1  |

29. Розшифруйте тест ПСОСНС, отриманий за допомогою шифру Цезаря для російської мови.

30. Розшифрувати криптограму, зашифровану шифром Віженера за допомогою ключового слова *криптография*.

К Б Р Ы Ю У Х А И Л Х Ъ П Ъ Ш Ч Б Ъ С Б И Е Ъ Д Ц Л

31. Розшифрувати криптограму, зашифровану шифром Гронсфельда за допомогою ключової 2709164835.

М Ч И Ш У Ф З Ш Г Щ К Ю Е Ъ Л О Й Ф И Ч Р Л Ы Р Б Я М Ь Ю

32. Розшифрувати текст В Ш А С Ф Н И В А Р О Е И О Л З, зашифрований за допомогою «магічного квадрата»

|    |    |    |    |
|----|----|----|----|
| 16 | 3  | 2  | 13 |
| 5  | 10 | 11 | 8  |
| 9  | 6  | 7  | 12 |
| 4  | 15 | 14 | 1  |

33. Розшируйте повідомлення О И Р М Е О С Ю В Т А Ь Л Г О П, отримане за допомогою «магічного квадрата»

|    |    |    |    |
|----|----|----|----|
| 16 | 3  | 2  | 13 |
| 5  | 10 | 11 | 8  |
| 9  | 6  | 7  | 12 |
| 4  | 15 | 14 | 1  |

34. Криптограма Т Ю А Е О О Г М Р Л И П О Ъ С В, отримана засобом подвійної перестановки. Ключем до шифру слугує послідовність номерів стовпців 4132 і номерів рядків 3142 таблиці. Шифртекст вписувати порядково.

35. Розшифрувати криптограму ПЪЙЫУЩИЭССЕКЪХЛН, зашифровану шифром Гронсфельда за допомогою ключової послідовності 0,12,1,16,14,7,8,31.

36. Розшифрувати криптограму ДХТЬРЮОГЛДЛЩСЧЖЩУ, зашифровану шифром Гронсфельда за допомогою ключової послідовності 2,7,1,8.

37. Розшифрувати криптограму ПДКЗЫВЗЧШЛЫЙСЙ за допомогою таблиці Трисеміуса розміром 4x8 для російського алфавіту. В якості ключа – слово БАНДЕРОЛЬ.

38. Розшифрувати повідомлення УИРДЗЕГЮСЖАОЕЯНП, отримане за допомогою «магічного квадрата».

|    |    |    |    |
|----|----|----|----|
| 16 | 3  | 2  | 13 |
| 5  | 10 | 11 | 8  |
| 9  | 6  | 7  | 12 |
| 4  | 15 | 14 | 1  |

39. Розшифруйте текст ПСОСНС, отриманий за допомогою шифру Цезаря для російського руської мови.

40. Розшифрувати криптограму, зашифровану шифром Віженера за допомогою ключового слова *крипто-графія*.

К Б Р Ы Ю У Х А И Л Х Ь П Ь Ш Ч Б Ъ С Б И Е Ъ Д Ц Л

41. Розшифрувати криптограму, зашифровану шифром Гронсфельда за допомогою ключової послідовності 2709164835.

М Ч И Ш У Ф З Ш Г Щ К Ю Е Ь Л О Й Ф И Ч Р Л Ы Р Б Я М Ь Ю

42. Розшифрувати текст В Ш А С Ф Н И В А Р О Е И О Л З, зашифрований за допомогою «магічного квадрата».

|    |    |    |    |
|----|----|----|----|
| 16 | 3  | 2  | 13 |
| 5  | 10 | 11 | 8  |
| 9  | 6  | 7  | 12 |
| 4  | 15 | 14 | 1  |

43. Розшифруйте повідомлення О И Р М Е О С Ю В Т А Ь Л Г О П, отримане за допомогою «магічного квадрата»

|    |    |    |    |
|----|----|----|----|
| 16 | 3  | 2  | 13 |
| 5  | 10 | 11 | 8  |
| 9  | 6  | 7  | 12 |
| 4  | 15 | 14 | 1  |

44. Криптограма Т Ю А Е О О Г М Р Л И П О Б С В, отримана засобом подвійної перестановки. Ключем к шифру слугує послідовність номерів стовпців 4132 і номерів рядків 3142 таблиці. Шифртекст вписувати порядково.

### Теорія інформації та кодування

1. Запишіть номер правильної, на Ваш погляд, відповіді:

Кількість символів алфавіту складає  $N = 32$ . Чому дорівнює ентропія повідомлення?

- 1) 4      2) 5      3) 6

Обґрунтуйте відповідь.

2. Запишіть номер правильної, на Ваш погляд, відповіді:

Яка із систем з багатократною передачею має кращу здатність виправляти помилки:

- 1) з мажоритарним поелементним прийомом;  
2) з мажоритарним посимвольним прийомом;

Обґрунтуйте відповідь.

3. Запишіть номер правильної, на Ваш погляд, відповіді:

Мінімальна кодова відстань  $d_0=5$ . Чому дорівнює кратність виправлення помилки?

- 1) 2    2) 3      3) 4

Обґрунтуйте відповідь.

4. Запишіть номер правильної, на Ваш погляд, відповіді:

У системі передачі даних з інформаційним зворотнім зв'язком (ізз) оцінка якості прийнятого повідомлення приймачем прямого каналу виробляється на:

- 4) передавальній стороні прямого каналу;  
5) приймальній стороні прямого каналу;  
6) як на передавальній так й на приймальній сторонах прямого каналу.

Обґрунтуйте відповідь.

5. Запишіть номер правильної, на Ваш погляд, відповіді:

У системі передачі даних з вирішальним зворотнім зв'язком та очікуванням (взз-оч) чергова передача блоку інформації здійснюється лише після:

- 1) одержання сигналу підтвердження зворотнім зв'язком;  
2) одержання сигналу перезапиту зворотнім зв'язком;  
3) одержання будь-якого сигналу зворотнім зв'язком.

Обґрунтуйте відповідь.



6. Запишіть номер правильної, на Ваш погляд, відповіді:  
Зворотній зв'язок у системах передачі даних необхідний для:

- 3) збільшення швидкості модуляції у каналі зв'язку;
- 4) розширення функціональних можливостей апаратури;
- 3) адаптації до зміни параметрів каналу зв'язку.

Обґрунтуйте відповідь.

7. Запишіть номер правильної, на Ваш погляд, відповіді:  
У системі без зворотного зв'язку в основному використовується режим завадостійкого коду:

- 1) з виявленням помилок;
- 2) з виправленням помилок;
- 3) у комбінованому режимі.

Обґрунтуйте відповідь.

8. Запишіть номер правильної, на Ваш погляд, відповіді:  
Ефективність системи передачі із зворотним зв'язком і виявленням помилок знижується при:

- 1) групуванні помилок в каналі;
- 2) незалежному потоці помилок в каналі.

Обґрунтуйте відповідь.

9. Запишіть номер правильної, на Ваш погляд, відповіді:  
У якому каналі передачі даних кратність появи помилок більша:

- 1) у каналі з групуванням помилок;
- 2) у каналі незалежними помилками.

Обґрунтуйте відповідь.

10. Імовірність прийому помилкової комбінації (комбінації, що містить хоча б одну помилку)  $p(\geq 1, n)$  довжиною  $n=12$  елементів з імовірністю помилки  $p_{\text{пом}}=0,00001$  складає:

4.  $1,20 \cdot 10^{-4}$ ;
5.  $1,19 \cdot 10^{-6}$ ;
6.  $1,19 \cdot 10^{-2}$ .

Обґрунтуйте відповідь.

11. Запишіть номери правильних, на Ваш погляд, відповідей:  
Що відбувається в каналі при збільшенні коефіцієнту групування помилок  $\alpha$ :

- 6) кратність появи помилок в кодовій комбінації зменшується;
- 7) кратність появи помилок в кодовій комбінації збільшується;
- 8) вірогідність спотворення кодової комбінації зменшується;
- 9) вірогідність спотворення кодової комбінації збільшується;
- 10) число запитів в системі із зворотним зв'язком не міняється.

Обґрунтуйте відповідь.

12. Встановити відповідність відповідей у вигляді комбінації цифр та літер:  
Імовірність помилки кодової комбінації  $p_{\text{пом } k}$  для каналу з незалежними помилками і при їхньому пакетуванні можна розрахувати за допомогою формули:

|  |                                   |
|--|-----------------------------------|
| Формула                                      | Канал                             |
| 1 $P_{\text{пом } l} \cong n p_{\text{пом}}$ | A З незалежним розподілом помилок |

|  |                          |
|--|--------------------------|
| 2 $P_{\text{пом } l} = \sum_{t=1}^n C_n^t p_{\text{пом}}^t (1 - p_{\text{пом}})^{n-t}$ | B З пакетуванням помилок |
|--|--------------------------|

|   |  |
|---|--|
| 3 $P_{\text{пом } l} \cong n^{1-\alpha} p_{\text{пом}}$ |  |
|---|--|

1            2            3.  
Обґрунтуйте відповідь.

13. Імовірність прийому помилкової комбінації (комбінації, що містить хоча б одну помилку)  $p(\geq 1, n)$  довжиною  $n=12$  елементів з імовірністю помилки  $p_{\text{пом}}=0,001$  складає:

- 1)  $1,19 \cdot 10^{-4}$
- 2)  $1,19 \cdot 10^{-6}$
- 3)  $1,20 \cdot 10^{-2}$

14. Запишіть номер правильної, на Ваш погляд, відповіді:

Кількість символів алфавіту складає  $N = 64$ . Чому дорівнює ентропія повідомлення?

- 1) 4      2) 5      3) 6

Обґрунтуйте відповідь.

15. Запишіть номер правильної, на Ваш погляд, відповіді:

Систем з багатократною передачею ( $S=5$ ) та мажоритарним поелементним прийомом гарантує кратність виправлення помилок у кодовому блоку  $k = 8$ :

- 1) 3;  
2) 2;  
3) 5.

Обґрунтуйте відповідь.

16. Запишіть номер правильної, на Ваш погляд, відповіді:

Мінімальна кодова відстань  $d_0=7$ . Чому дорівнює кратність виправлення помилок?

- 1) 2    2) 3    3) 4

Обґрунтуйте відповідь.

17. Запишіть номер правильної, на Ваш погляд, відповіді:

Ефективна швидкість передачі  $R$  у системі передачі даних з повним інформаційним зворотнім зв'язком (ізз)

- 4)  $>0,5$ ;  
5)  $\leq 0,5$ ;  
6)  $<0,5$ .

Обґрунтуйте відповідь.

18. Запишіть номер правильної, на Ваш погляд, відповіді:

У системі передачі даних з вирішальним зворотнім зв'язком та очікуванням (взз-оч) повторна передача блоку інформації здійснюється лише після:

- 1) одержання сигналу підтвердження зворотнім зв'язком;  
2) одержання сигналу перезапиту зворотнім зв'язком;  
3) одержання будь-якого сигналу зворотнім зв'язком.

Обґрунтуйте відповідь.

19. Запишіть номер правильної, на Ваш погляд, відповіді:

Зворотній зв'язок у системах передачі даних необхідний для:

- 4) збільшення швидкості модуляції у каналі зв'язку;  
5) розширення функціональних можливостей апаратури;  
6) адаптації до зміни параметрів каналу зв'язку.

Обґрунтуйте відповідь.

20. Запишіть номер правильної, на Ваш погляд, відповіді:

У системі без зворотного зв'язку в основному використовується режим завадостійкого коду:

- 1) з виявленням помилок;  
2) з виправленням помилок;  
3) у комбінованому режимі.

Обґрунтуйте відповідь.

21. Запишіть номер правильної, на Ваш погляд, відповіді:

Ефективність системи передачі із зворотним зв'язком і виявленням помилок знижується при:

- 1) групуванні помилок в каналі;  
2) незалежному потоці помилок в каналі

Обґрунтуйте відповідь.

22. Запишіть номер правильної, на Ваш погляд, відповіді:

У якому каналі передачі даних кратність появи помилок більша:

- 1) у каналі з групуванням помилок;  
2) у каналі незалежними помилками.

Обґрунтуйте відповідь.

23. Імовірність прийому помилкової комбінації ( комбінації, що містить хочаб одну помилку)  $p(\geq 1, n)$  довжиною  $n=8$  елементів з імовірністю помилки  $p_{\text{пом}}=0,001$  складає:

4.  $1,19 * 10^{-4}$
5.  $1,19 * 10^{-6}$
6.  $8,00 * 10^{-2}$

Обґрунтуйте відповідь.

24. Запишіть номера правильних, на Ваш погляд, відповідей:

Що відбувається в каналі при зменшенні коефіцієнту групування помилок  $\alpha$  :

- 6) кратність появи помилок в кодовій комбінації зменшується;
- 7) кратність появи помилок в кодовій комбінації збільшується;
- 8) вірогідність спотворення кодової комбінації зменшується;
- 9) вірогідність спотворення кодової комбінації збільшується;
- 10) число запитів в системі із зворотним зв'язком збільшується.

Обґрунтуйте відповідь.

25. Запишіть номер правильної, на Ваш погляд, відповіді:

Кількість символів алфавіту складає  $N = 16$ . Чому дорівнює ентропія повідомлення?

- 1) 4
- 2) 5
- 3) 6

Обґрунтуйте відповідь.

26. Запишіть номер правильної, на Ваш погляд, відповіді:

Яка із систем з багатократною передачею має кращу здатність виправляти помилки:

- 1) з мажоритарним поелементним прийомом;
- 2) з мажоритарним посимвольним прийомом;

Обґрунтуйте відповідь.

27. Запишіть номер правильної, на Ваш погляд, відповіді:

Мінімальна кодова відстань  $d_0=6$ . Чому дорівнює кратність виправлення помилки?

- 1) 2
- 2) 3
- 3) 4

Обґрунтуйте відповідь.

28. Запишіть номер правильної, на Ваш погляд, відповіді:

У системі передачі даних з інформаційним зворотнім зв'язком (ізз) оцінка якості прийнятого повідомлення приймачем прямого каналу виробляється на:

- 4) передавальній стороні прямого каналу;
- 5) приймальної стороні прямого каналу;
- 6) як на передавальній так й на приймальної сторонах прямого каналу.

Обґрунтуйте відповідь.

29. Запишіть номер правильної, на Ваш погляд, відповіді:

У системі передачі даних з вирішальним зворотнім зв'язком та очікуванням (взз-оч) чергова передача блоку інформації здійснюється лише після:

- 4) одержання сигналу підтвердження зворотнім зв'язком;
- 5) одержання сигналу перезапиту зворотнім зв'язком;
- 6) одержання будь-якого сигналу зворотнім зв'язком.

Обґрунтуйте відповідь.

30. Запишіть номера правильних, на Ваш погляд, відповідей:

Зворотній зв'язок у системах передачі даних необхідний для:

- 4) Формування сигналу зворотного зв'язку;
- 5) розширення функціональних можливостей апаратури;
- 6) адаптації до зміни параметрів каналу зв'язку.

Обґрунтуйте відповідь.

31. Запишіть номер правильної, на Ваш погляд, відповіді:

Ефективність системи передачі із зворотним зв'язком і виявленням помилок знижується при:

- 1) групуванні помилок в каналі;
- 2) незалежному потоці помилок в каналі

Обґрунтуйте відповідь.

32. Запишіть номер правильної, на Ваш погляд, відповіді:

У якому каналі передачі даних кратність появи помилок менша:

- 1) у каналі з групуванням помилок;
- 2) у каналі незалежними помилками

Обґрунтуйте відповідь.

33. Імовірність прийому помилкової комбінації (комбінації, що містить хоча б одну помилку)  $p(\geq 1, n)$  довжиною  $n=7$  елементів з імовірністю помилки  $p_{\text{пом}}=0,01$  складає:

- 4)  $1,19 \cdot 10^{-4}$
- 5)  $1,19 \cdot 10^{-6}$
- 6)  $7,00 \cdot 10^{-1}$

Обґрунтуйте відповідь.

34. Запишіть номери правильних, на Ваш погляд, відповідей:

Що відбувається при збільшенні у каналі коефіцієнту групування помилок  $\alpha$  :

- 6) кратність появи помилок в кодовій комбінації зменшується;
- 7) кратність появи помилок в кодовій комбінації збільшується;
- 8) вірогідність спотворення кодової комбінації зменшується;
- 9) вірогідність спотворення кодової комбінації збільшується;
- 10) число запитів в системі із зворотного зв'язку зменшується.

Обґрунтуйте відповідь.

35. Запишіть номер правильної, на Ваш погляд, відповіді:

Кількість символів алфавіту складає  $N = 128$ . Чому дорівнює ентропія повідомлення?

- 1) 4
- 2) 5
- 3) 7

Обґрунтуйте відповідь.

36. Запишіть номер правильної, на Ваш погляд, відповіді:

Яка із систем з багатократною передачею має кращу здатність виправляти помилки:

- 1) з мажоритарним поелементним прийомом;
- 2) з мажоритарним посимвольним прийомом;

Обґрунтуйте відповідь.

37. Запишіть номер правильної, на Ваш погляд, відповіді:

Мінімальна кодова відстань  $d_0=9$ . Чому дорівнює кратність виправлення помилки?

- 1) 2
- 2) 3
- 3) 4

Обґрунтуйте відповідь.

38. Запишіть номер правильної, на Ваш погляд, відповіді:

У системі передачі даних з інформаційним зворотнім зв'язком (ізз) оцінка якості прийнятого повідомлення приймачем прямого каналу виробляється на:

- 4) передавальній стороні прямого каналу;
- 5) приймальній стороні прямого каналу;
- 6) як на передавальній так й на приймальній сторонах прямого каналу.

Обґрунтуйте відповідь.

39. Запишіть номер правильної, на Ваш погляд, відповіді:

У системі передачі даних з вирішальним зворотнім зв'язком та очікуванням (ВЗЗ-ОЧ) чергова передача блоку інформації здійснюється лише після:

- 1) одержання сигналу підтвердження зворотнім зв'язком;
- 2) одержання сигналу перезапиту зворотнім зв'язком;
- 3) одержання будь-якого сигналу зворотнім зв'язком.

Обґрунтуйте відповідь.

40. Запишіть номер правильної, на Ваш погляд, відповіді:

Зворотній зв'язок у системах передачі даних необхідний для:

- 4) збільшення швидкості модуляції у каналі зв'язку;
- 5) розширення функціональних можливостей апаратури;
- 6) адаптації до зміни параметрів каналу зв'язку.

Обґрунтуйте відповідь.

41. Запишіть номер правильної, на Ваш погляд, відповіді:

Кількість символів алфавіту складає  $N = 16$ . Чому дорівнює ентропія повідомлення?

1) 4      2) 5      3) 6      Обґрунтуйте відповідь.

42. Запишіть номер правильної, на Ваш погляд, відповіді:

Яка із систем з багатократною передачею має кращу здатність виправляти помилки:

1) з мажоритарним поелементним прийомом;

2) з мажоритарним посимвольним прийомом;

Обґрунтуйте відповідь.

43. Запишіть номер правильної, на Ваш погляд, відповіді:

Мінімальна кодова відстань  $d_0 = 10$ . Чому дорівнює кратність виправлення помилки?

1) 2      2) 3      3) 4

Обґрунтуйте відповідь.

44. Запишіть номер правильної, на Ваш погляд, відповіді:

У системі передачі даних з інформаційним зворотнім зв'язком (іЗЗ) оцінка якості прийнятого повідомлення приймачем прямого каналу виробляється на:

4) передавальній стороні прямого каналу;

5) приймальною стороною прямого каналу;

6) як на передавальній так й на приймальною сторонах прямого каналу.

Обґрунтуйте відповідь.

45. Запишіть номер правильної, на Ваш погляд, відповіді:

У системі передачі даних з вирішальним зворотнім зв'язком та очікуванням (ВЗЗ-ОЧ) чергова передача блоку інформації здійснюється лише після:

1) одержання сигналу підтвердження зворотнім зв'язком;

2) одержання сигналу перезапиту зворотнім зв'язком;

3) одержання будь-якого сигналу зворотнім зв'язком.

Обґрунтуйте відповідь.

### Методи та засоби технічного захисту інформації

1. Забезпечення безпеки інформаційних ресурсів в акредитованому центрі.

2. Перелік посад адміністраторів та їх обов'язки у акредитованому центрі.

3. Вимоги до спеціальних приміщень акредитованого центру.

4. Яка інформація підлягає захисту в інформаційній, телекомунікаційній та інформаційно-телекомунікаційній системі.

5. Вимоги до забезпечення захисту інформації в інформаційній, телекомунікаційній та інформаційно-телекомунікаційній системі.

6. Організаційні засади забезпечення захисту інформації в інформаційній, телекомунікаційній та інформаційно-телекомунікаційній системі.

7. Поясніть основні загальні положення щодо категорювання об'єктів інформаційної діяльності.

8. Порядок проведення робіт з категорювання об'єктів інформаційної діяльності.

9. Дайте короткий опис можливого витоку інформації каналами ПЕМВН.

10. Організація захисту інформації у засобах обчислювальної техніки від витоку каналами ПЕМВН.

11. Рекомендації із захисту інформації від перехоплення випромінювань технічних засобів об'єкта електронно-обчислювальної техніки.

12. Рекомендації із захисту інформації від перехоплення наводок на незахищені технічні засоби та допоміжні технічні засоби зв'язу (ДТЗС), що мають вихід за межі контрольованої зони (КТ).

13. Рекомендації із захисту інформації від витоку колами заземлення.

14. Рекомендації із захисту інформації від витоку колами електроживлення.

15. Рекомендації із застосування системи просторового шумлення об'єктів електронно-обчислювальної техніки (ЕОТ).

16. Основні рекомендації з обладнання та застосування екранувальних конструкцій.

17. Вимоги до серверних приміщень і приміщень електронних архівів.

18. Вимоги до екранованих приміщень

19. Вимоги до систем заземлення банків та систем захисту від пошкодження блискавкою.

20. Вимоги до систем електроживлення банків.

21. Організаційні заходи захисту серверних.

22. Технічні вимоги до приміщень серверних.

23. Екранування приміщень.

24. Рекомендації по вибору та встановленню фільтрів.

25. Заземлення об'єктів ЕОТ.

26. Екранування кабельних мереж.

27. Екрануючі конструкції, що виконані з труб.

28. Коробчасті екрануючі конструкції.

29. Вимоги щодо розміщення трансформаторної підстанції.

30. Вимірювання ефективності екранування приміщень.

## ПЕРЕЛІК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Богуш В.М., Юдін О.К. Інформаційна безпека держави. Навчальний посібник – К.: «МК-Прес», 2005. – 432 с.
2. Вильям Столлингс Криптографическая защита сетей. – М.: Издательский дом “Вильямс”, 2001.
3. Домарев В.В./ Защита информации и безопасность компьютерных систем / Киев: диа-софт, 1999.
4. Конахович Г.Ф. и др. Защита информации в телекоммуникационных системах. – К.: «МК-Прес», 2005. – 288 с.
5. Тардаскін М.Ф., Савицький Л.Ю., Кононович В.Г., Технічна експлуатація систем захисту інформації. Частина 1. Захист мовної інформації в каналах зв'язку та на об'єктах інформаційної діяльності: Навч. посібник / за ред. М.В. Захарченка. – Одеса: ОНАЗ, 2004. – С 188.
6. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. Учебное пособие. М.: Гостехкомиссия России, 1998. – 320 с.
7. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: Термінологічний навчальний довідник / За ред. Кривуци В.Р – Київ. ООО "Д.В.К.", 2004 . – 508 с.
8. Герасименко В.А., Малюк А.А. Основы защиты информации. – М.: МОПО РФ. МИФИ, 1997. – 537 с.
9. Захарченко Н.В., Йона Л.Г., Щербина Ю.В., Онацкий А.В., Учебное пособие «Развитие криптографии и ее место в современном обществе». Часть 1 «Классические методы шифрования». – Одесса, 2003. – 94 с.
10. Горохов С.М., Йона Л.Г., Онацкий О.В. «Сучасні криптографічні системи». Навчальний посібник. – Одеса.: ОНАС, 2007. – 152 с.
11. Передача дискретных сообщений. Учебник для ВУЗ-ов связи. Под редакцией В.П. Шувалова – М.: Радио и связь, 1990.
12. Крисько А.С. Захарченко В.Н. Основы кодирования: учебное пособие \_ Одесса УГАС 1999.
13. Владишевський Б.С. Киреев И.А. Информационные службы документальной электросвязи. Учеб. пособие – Одесса, УГАС. 1995.
14. Захарченко Н.В., Вараксин А.А., Филатов Г.Г. Изучение принципов построения кодеров циклического кода. Методическое пособие к лабораторной работе №7. – Одесса, ОНАС. – 2004.
15. Захарченко Н.В., Вараксин А.А., Филатов Г.Г. Адаптивные системы передачи данных с переспросом. Учеб. Пособие по курсу СДЕС. ОНАС, Одесса. – 2002.
16. Захарченко Н.В., Вараксин А.А., Филатов Г.Г. Изучение алгоритмов работы адаптивных систем передачи данных с переспросом. Методическое пособие к практическим и лабораторным работам №3 – 6. – ОНАС, Одесса, 2002.
17. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. – Затверджено наказом ДСТСЗІ СБ України № 125 від 8.11.2005. – (Серія видань “Нормативний документ”).
18. Положення про Державну експертизу в сфері технічного захисту інформації. – Затверджено наказом Адміністрації ДССЗІ України № 93 від 16.05.07. – Офіційний вісник України. – 2007. – № 52, ст. 2153. – (Серія видань “Нормативний документ”).
19. 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. – Затверджено наказом Адміністрації ДССЗІ України № 65 від 12 березня 2011. – (Серія видань “Нормативний документ”).
20. НД ТЗІ 1.1-005-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення. – Затверджено наказом Адміністрації ДССЗІ України № 232 від 12.12.2007. – (Серія видань “Нормативний документ”).
21. НД ТЗІ 3.1-001-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи. – Затверджено наказом Адміністрації ДССЗІ України № 232 від 12.12.2007. – (Серія видань “Нормативний документ”).
22. НД ТЗІ 2.1-002-07. Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення. – Затверджено наказом Адміністрації ДССЗІ України № 232 від 12.12.2007. – (Серія видань “Нормативний документ”).