ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ
4 курс 1 семестр екзамен

1. На кого покладено забезпечення робіт з технічного захисту інформації в Україні?
2. Що таке інформація?
3. Які складові життєвого циклу інформації?
4. Що є об'єктами захисту з урахуванням їх пріоритетів?
5. Що включає в себе поняття «безпечна діяльність» підприємства чи організації?
6. Що є гарантією того, що конкретна інформація доступна лише тому колу осіб, для яких вона призначена?
7. Як можна розділити інформацію на категорії за рівнем важливості?
8. Як називається комплекс правових норм, організаційних заходів, технічних, програмних і криптографічних засобів, що забезпечує захист інформації відповідно до прийнятої політики безпеки?
9. Як називають осіб, що пов'язані з опрацюванням інформації?
10. Які рівні (грифи) таємності встановлено в Україні в державних структурах?
11. Як називають адміністративні чи законодавчі заходи, що відповідають мірі відповідальності особи за витік конкретної інформації, регламентованої спеціальними документами, з урахуванням державних, воєнно-стратегічних, комерційних, службових чи особистих інтересів?
12. Як називають показники, що характеризують інформацію як ресурс для забезпечення процесу отримання розв'язків різноманітних задач?
13. Як називають показник інформації, що характеризує відповідність її потребам задачі, яка розв'язується?
14. Як називають показник інформації, що характеризує зручність сприйняття та використання інформації в процесі розв'язання відповідної задачі?
15. Як називають організаційно-технічну систему, що об'єднує обчислювальну систему, фізичне середовище, персонал і опрацьовувану інформацію?
16. Що є фундаментальними властивостями захищеної інформації?
17. Що таке властивість інформації, яка полягає в тому, що вона не може бути доступною для модифікації користувачам і/або процесам, що не мають на це відповідних повноважень?
18. Що таке властивість інформації, яка полягає в тому, що процес її опрацювання повинен постійно перебувати під контролем певного керуючого захистом органу?
19. Що таке властивість інформації, що полягає в можливості її використання на вимогу користувача, який має відповідні повноваження?
20. Що таке властивість інформації, яка полягає в тому, що вона не може бути доступною для ознайомлення користувачам і/або процесам, що не мають на це відповідних повноважень?

21. Якими особливостями характеризуються фундаментальні властивості захищеної інформації (ФВЗІ)?
22. Як поділяються всі заходи забезпечення безпеки АС за способами реалізації?
23. Як називають чинні в країні закони, укази і нормативні акти, які регламентують правила поводження з інформацією, закріплюють права та обов'язки учасників інформаційних відносин у процесі її опрацювання і використання, а також встановлюють відповідальність за порушення цих правил?
24. Як називають заходи організаційного характеру, які регламентують процеси функціонування системи опрацювання даних, використання її ресурсів, діяльність персоналу, а також порядок взаємодії користувачів із системою таким чином, щоб наскільки можливо ускладнити або виключити можливість реалізації загроз безпеці?
25. Як називають заходи захисту, що базуються на використанні різних електронних пристроїв і спеціальних програм, що входять до складу АС і виконують (самостійно або в комплексі з іншими засобами) функції захисту?
26. Що є гарантією того, що джерелом інформації є саме та особа, яку заявлено як її автора?
27. Як називається підрозділ, який створюється для організації кваліфікованої розробки системи захисту інформації і забезпечення її функціонування?
28. Яка операція буде проведена, якщо інформація, не змінюючись, переноситься на інший носій, додаючись до інформації, що є там, і не модифікуючи її?
29. Яка операція буде проведена, якщо інформація, не змінюючись, переноситься на інший носій, модифікуючи інформацію, що є там?
30. Що таке канал обміну інформацією?
31. Що таке канал обміну, за допомогою якого реалізовано будь-який збиток ІТС і\або порушення хоча б одної із основних властивостей інформації ІТС?
32. Як називають властивість інформації, яка полягає в тому, що вона не може бути доступною для ознайомлення користувачам і/або процесам, які не мають на це відповідних повноважень?
33. Як називають властивість, яка полягає в тому, що вона не може бути доступною для модифікації користувачам і/або процесам, які не мають на це відповідних повноважень?
34. Як називають властивість, яка полягає в можливості її використання за вимогами користувача і/або процесу, що мають відповідні повноваження?
35. Як називають властивість комп'ютерних систем, що дозволяє фіксувати діяльність користувачів і процесів, використання об'єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і/або процесів?
36. Що таке інформаційні загроза?

37. Що таке можливість реалізації певної множини доступів для ознайомлення з інформацією користувачам і/або процесам, які не мають на це відповідних повноважень?
38. Що таке можливість реалізації певної множини доступів для модифікації інформації користувачам і/або процесам, які не мають на це відповідних повноважень?
39. Що таке можливість реалізації певної множини заходів, які не дозволяють її використовувати за вимогами користувачів і/або процесів, що мають на це відповідні повноваження?
40. Що таке можливість реалізації певної множини заходів, які не дозволяють фіксувати діяльність користувачів і процесів, використання об'єктів і/або однозначно установлювати ідентифікатори причетних до певних подій користувачів і/або процесів?
41. За допомогою яких послуг можна забезпечити протидію загрозам порушення конфіденційності в КС?
42. Дайте визначення поняттю «криптографія».
43. Дайте визначення поняттю «криптоаналіз».
44. Як називають процес, що відбувається коли вихідний текст, що має також назву відкритого тексту, заміняється шифрованим текстом?
45. Як називають процес, що відбувається, коли шифрований текст, заміняється вихідним текстом?
46. Як називається інформація, яка необхідна для безперешкодного шифрування і дешифрування?
47. Як поділяють криптосистеми?
48. Які ключі використовують у симетричних системах і для шифрування, і для дешифрування?
49. Які ключі використовують у системах з відкритим ключем?
50. Як називається приєднане до тексту його криптографічне перетворення, що дозволяє при одержанні тексту іншим користувачем перевірити авторство і дійсність повідомлення?
51. Що таке криптостійкість?
52. До яких класів перетворень зводять криптографічні методи?
53. Принцип такого шифрування полягає в генерації гами шифру за допомогою датчика псевдовипадкових чисел і накладенні отриманої гами на відкриті дані. Як називають такий вид шифрування?
54. Що таке захист конфіденційної інформації від несанкціонованого доступу, камуфляжі програмного забезпечення та захист авторського права на деякі види інтелектуальної власності?
55. За якими напрямками розвиваються методи комп'ютерної стеганографії?
56. За якою формулою розраховується класичний шифр Цезаря?
57. Якою буде шифрограма тексту «метод» при використанні перетворення класичним шифром Цезаря?
58. Якою буде шифрограма тексту «студент» при використанні перетворення шифром Цезаря, ключ «-3»?
59. Для шифрування й дешифрування використовують ключ у вигляді квадрата. Кожну літеру або знак відкритого тексту замінюють парою цифр

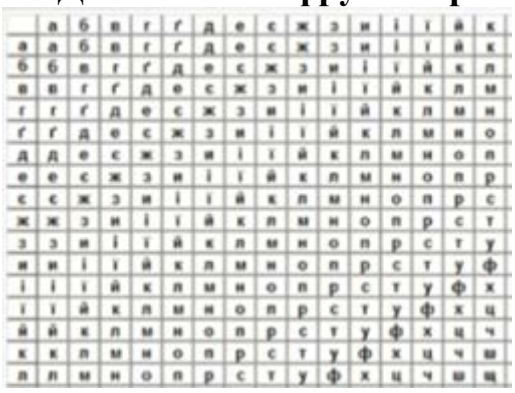
– номером рядка й номером стовпця, на перетині яких міститься цей символ. Як називається такий шифр?

60. Які символи використовують для шифрування за допомогою квадрата Полібія?

61. Ключем є фраза, яка містить половину літер абетки. Наприклад, для української абетки, ключова фраза повинна мати 16 різних літер (але може бути довшою, ніж 16 літер, тобто деякі літери можуть повторюватися). Як називається такий шифр?

62. Для шифрування вибирають ключ. Якщо довжина ключа менша від довжини явного тексту, то ключ циклічно продовжується. Шифрування повідомлень здійснюється на основі згаданого перетворення букв вихідного повідомлення та на основі ключа. Як називається такий шифр?

63. Для якого шифру використовується представлена частина таблиці?



64. За допомогою якого із шифрів можна зробити багаторівневе шифрування?

65. При використанні шифру Плейфера, якщо літери пари стоять в одному рядку, то на які літери їх заміняють?

66. Виберіть шифр перестановки.

67. При використанні шифру частоколу відкритий текст записується по «стовпчиках». Чим визначається кількість «стовпчиків»?

68. До якого методу належить шифр одноразового блокноту?

69. Як ключ вибирається довільний бітовий рядок, довжина якого збігається з довжиною вихідного тексту. Відкритий текст також перетвориться в послідовність двійкових розрядів, ці два рядки порозрядно складаються по модулю 2. Як називають такий шифр?

70. Суть такого шифрування заснована на отриманні з його допомогою послідовності випадкових чисел, тоді як процедура зашифровування проводиться за принципом системи одноразових шифроблокнотів. Як називають такий шифр?

71. Що відносять до методів гамування?

72. До яких шифрів відносять шифрування алгоритмом DES?

73. Як називають шифри, коли для шифрування повідомлення використовується один ключ, а при дешифруванні – інший?

74. Які функції безпеки обчислювальної системи реалізують програмні засоби захисту інформації?

75. Що таке агент безпеки?

76. За допомогою методу стандартної перестановки (горизонтальної) зашифрувати слово «перестановка» з ключовим словом «шифр»:

Ш	И	Ф	Р
п	е	р	е
с	т	а	н
о	в	к	а

77. За допомогою методу стандартної перестановки (горизонтальної) зашифрувати слово «повідомлення» з ключовим словом «ключ»:

к	л	ю	ч
п	о	в	і
д	о	м	л
е	н	н	я

78. За допомогою методу стандартної перестановки (горизонтальної) зашифрувати слово «криптографія» з ключовим словом «пазл»:

п	а	з	л
к	р	и	п
т	о	г	р
а	ф	і	я

79. За допомогою методу стандартної перестановки (горизонтальної) зашифрувати слово «національний» з ключовим словом «кадр»:

к	а	д	р
н	а	ц	і
о	н	а	л
ь	н	и	й

80. За допомогою методу стандартної перестановки (горизонтальної) зашифрувати слово «незалежність» з ключовим словом «вежа»:

в	е	ж	а
н	е	з	а
л	е	ж	н
і	с	т	ь

81. Яким буде повідомлення «перестановка» з ключами «шифр» і «лід», зашифроване за допомогою методу комбінованих перестановок, результат показати по горизонталі:

	Ш	И	Ф	Р
Л	п	е	р	е
І	с	т	а	н
Д	о	в	к	а

82. Яким буде повідомлення «незалежність» з ключами «вежа» і «січ», зашифроване за допомогою методу комбінованих перестановок, результат показати по горизонталі:

	в	е	ж	а
с	н	е	з	а
і	л	е	ж	н
ч	і	с	т	ь

83. Яким буде повідомлення «національний» з ключами «кадр» і «дим», зашифроване за допомогою методу комбінованих перестановок, результат показати по горизонталі:

	к	а	д	р
д	н	а	ц	і
и	о	н	а	л
м	ь	н	и	й

84. Яким буде повідомлення «криптографія» з ключами «пазл» і «сон», зашифроване за допомогою методу комбінованих перестановок, результат показати по горизонталі:

	п	а	з	л
с	к	р	и	п
о	т	о	г	р
н	а	ф	і	я

.

85. Яким буде повідомлення «повідомлення» з ключами «ключ» і «лев», зашифроване за допомогою методу комбінованих перестановок, результат показати по горизонталі:

	к	л	ю	ч
л	п	о	в	і
е	д	о	м	л
в	е	н	н	я

.

86. Яким буде після шифрування класичним шифром Цезаря повідомлення «VENI VIDI VICI»

87. Яким буде текст «ЗАГРОЗА ІСНУЄ ЗАВЖДИ І ВСЮДИ» із ключами 416325 (стовпці) і 2431 (рядки), зашифрований методом подвійної перестановки:

	4	1	6	3	2	5
2	З	А	Г	Р	О	З
4	А	І	С	Н	У	Є
3	З	А	В	Ж	Д	И
1	І	В	С	Ю	Д	И

.

88. Зашифрувати текст "ВСЕ ТАЄМНЕ СТАЄ ЯВНИМ" шифром Плейфера. Ключове слово – «бандероль»:

Б	А	Н	Д	Е	Р	О	Л
Ь	В	Г	Є	Ж	З	И	І
Ї	Й	К	М	П	С	Т	У
Ф	Х	Ц	Ч	Ш	Щ	Ю	Я

.

89. Що таке криптоаналіз?

90. Як називають отримання ключа не криптографічним способом?

91. Що відносять до методів крипто аналізу?

92. Зашифрувати за допомогою одноразового блокноту текст ШИФР з гамою 01100101100101111010101101010010 1. Використати кодування ASCII.

11110110 10110111 10101010 11100001

XOR

01100101 10010111 01010110 10100101

93. Зашифрувати за допомогою одноразового блокноту текст ШИФР з гамою 00000000111111111000000001111111 1. Використати кодування ASCII.

11110110 10110111 10101010 11100001

XOR

00000000 11111111 00000000 11111111

94. Як називають спробу розкриття конкретного шифру із застосуванням методів криптоаналізу на цей шифр?

95. Як називають вид криптоаналізу, який ґрунтується на знанні частини відкритого тексту, та зашифрованого тексту повідомлення?
96. Як називають криптоаналіз, який вивчає методи атак на програмні, програмно-апаратні та апаратні реалізації криптографічних перетворень?
97. Як називають елементи, з яких складається дискретне повідомлення?
98. Якими положеннями характеризується проблема захисту інформації?
99. Яка природа походження загроз безпеки?
100. Що є джерелами загроз безпеки інформації?