1. Опишіть властивості інформації щодо її захисту.
2. Що використається для захисту від некоректних дій користувачів і програм (від реалізації випадкових погроз) – ідентифікація й аутентифікація, знищення залишкових даних, шифрування інформації або дублювання компонентів обчислювальної системи?
3. Що таке загрозі інформаційної безпеки комп'ютерної системи?
4. Які існують загрози інформаційної безпеки?
5. Опишіть випадкові загрози інформації.
6. Опишіть навмісні загрози інформації.
7. В чому полягає загроза порушення конфіденційності інформації?
8. В чому полягає загроза порушення цілісності інформації?
9. В чому полягає порушення доступності інформації?
10. Що таке інформаційна безпека автоматизованої системи?
11. Які існують моделі порушника інформаційної безпеки?
12. Які основні функції служби безпеки інформації?
13. Які існують рівні захисту інформації в компьютерних системах?
14. Сформулюйте принципи надійної системи захисту інформації.
15. Назвіть етапи побудови системи захисту інформації в комп'ютерній системі.
16. Як і статті Кримінального кодексу України стосуються захисту інформації?
17. Сформулюйте кримінальні дії, що підпадають під ст.361 Кримінального кодексу України.
18. Сформулюйте кримінальні дії, що підпадають під ст.362 Кримінального кодексу України.
19. Сформулюйте кримінальні дії, що підпадають під ст.363 Кримінального кодексу України.
20. До якої статті Кримінального кодексу України відноситься впровадження вірусів в комп'ютерну систему?
21. Сформулюйте морально-етичні правила дотримання вимог захисту інформації.
22. Наведіть приклади комп'ютерних злочинів.
23. В чому полягають адміністративні заходи щодо захисту інформації в комп'ютерній системі?
24. Хто здійснює організаційно адміністративний захист інформації в комп'ютерній системі?
25. Наведіть засоби технічного знімання інформації.
26. Наведіть фізико-технічні засоби захисту інформації в компьютерних системах.
27. Що таке побічні електромагнітні випромінювання й наведення?
28. Наведіть канали витоку інформації.
29. В чому полягає криптографічний захист інформації?
30. Опишіть найпростіші шифри: зміни та перестановці.
31. Коли виникла асиметрична криптографія?

32. Що таке криптоаналіз?
33. На чем засновується стійкість криптоалгоритмів?
34. Що застосовується для захисту від несанкціонованого використання ресурсів обчислювальної системи – ідентифікація й аутентифікація, розмежування доступу, шифрування й контроль дійсності інформації або дублювання компонентів обчислювальної системи?
35. В чому полягає стеганографічний захист інформації?
36. За вдяки якому протоколу (TCP/IP, SSL/TLS, PPP, HTTP або IPX/SPX) здійснюється шифрування інформації при передачі конфіденційний даних між клієнтом та Web-сервером в мережі Інтернет (наприклад при проведенні платіжних операцій)?
37. Які алгоритми називаються симетричними?
38. Які алгоритми називаються потоковими?
39. Які алгоритми називаються блочними?
40. Як генеруються ключі в симетричних шифрах?
41. Наведіть приклади блочних шифрів.
42. Який алгоритм є Міждержавним стандартом шифрування і використається в Україні?
43. Яка довжина ключа в алгоритмі шифрування ГОСТ 28147-89?
44. Яка довжина блоку в алгоритмі шифрування ГОСТ 28147-89
45. Які режими використовуються в алгоритмі ГОСТ 28147-89?
46. В чому полягає режим простій зміни алгоритму ГОСТ 28147-89?
47. В чому полягає режим гамування алгоритму ГОСТ 28147-89?
48. Що таке імітоприкладка та для чого вона використається?
49. Опишіть вплив помилок в режимі простій зміни алгоритму ГОСТ 28147-89.
50. Опишіть вплив помилок в режимі гамування алгоритму ГОСТ 28147-89.
51. Який алгоритм є стандартом шифрування США? Які його числові характеристики?
52. Які алгоритми шифрування називаються асиметричними?
53. Наведіть приклади асиметричних шифрів.
54. Як генеруються ключі в алгоритмі шифрування RSA?
55. Опишіть схему шифрування в алгоритмі RSA.
56. За допомогою якого ключа здійснюється шифрування в алгоритмі RSA?
57. Як можна вирішіть проблему передачі секретного ключа симетричного шифру?
58. Опишіть схему Діффі-Хеллмана вироблення спільного секретного ключа.
59. У якому протоколі (SSL, SOCKS, SKIP або IPSec) на схемі Діффі-Хеллмана засновано формування тимчасових секретних ключів для пар користувачів мережі?
60. Що таке «цифровій конверт»? Для чого він використається?
61. Що таке електронний цифровий підпис? Для чого він використається?
62. За допомогою якого ключа підписується електронний документ?
63. За допомогою якого ключа здійснюється перевірка підпису електронного документа?

64. Який алгоритм є Українським стандартом електронного цифрового підпису?
65. Для чого може використатися
66. Для чого використається функція хешування?
67. Наведіть приклади функцій хешування.
68. Опишіть властивості функцій хешування.
69. Наведіть класіфікацію каналів несанкціонованого доступу до інформації.
70. Які функції повинні виконувати системи захисту від несанкціонованого доступу?
71. Порівняйте методи аутентифікації електронних даних – за допомогою імітоприкладки та електронного цифрового підпису.
72. Що таке ідентифікація?
73. Що таке аутентифікація?
74. Які існують засобі аутентифікації?
75. Що використається для захисту від несанкціонованого доступу до ресурсів обчислювальної системи – ідентифікація і аутентифікація, знищення залишкових даних, шифрування інформації або дублювання компонентів обчислювальної системи?
76. Що таке одностороння аутентифікація?
77. Що таке двустороння аутентифікація?
78. Опишіть метод аутентифікації з використанням електронних ключів.
79. Опишіть протокол аутентифікації користувача в комп'ютерної системі.
80. Опишіть протокол аутентифікації користувача в комп'ютерної системі з «підсоленими» паролями.
81. Що таке клавіатурний почерк?
82. Опишіть засоби взаємної аутентифікації користувачів.
83. Опишіть механізм «запит – відповідь» при взаємної аутентифікації користувачів.
84. Опишіть процедуру «Рукостискання» при взаємної аутентифікації користувачів.
85. Опишіть основні вимоги до паролів.
86. Що таке паролі та як вони генеруються?
87. Як можна зберігати паролі в парольній системі?
88. Опишіть атаки на паролі.
89. Для чого використаються «підсолені» паролі?
90. Який метод захисту інформації можна використати при зберіганні паролів у відкритій області даних ?
91. Як підрахувати ймовірність зламання пароля програмою - зломщиком паролів?
92. Наведіть приклади віддалених мережевих атак.
93. Опишіть мережеву атаку Mailbombing.
94. Опишіть мережеву атаку Переповнення буфера.
95. Наведіть приклади комп'ютерних вірусів.
96. Що таке Sniffing пакетів?

97. Опишіть мережеву атаку IP-spoofing.

98. Опишіть DoS-атаку.

99. Опишіть DDoS-атаку.

100. Які існують засоби захисту від віддалених мережевих атак?

101. Що таке Firewall? Для чого і как використається?

102. Наведіть приклади захищених мережевих криптопротоколів.

103. В чому полягає адміністративний метод захисту від віддалених мережевих атак?

104. Що таке політика безпеки?

105. В чому полягає програма забезпечення інформаційної безпеки?

106. В чому полягає аудит комп'ютерної системи?

107. В чому полягає контроль коректності функціонування засобів захисту комп'ютерної системи?

108. Наведіть критерії захищеності автоматизованих систем згідно нормативним документам України.

109. Опишіть критерії конфіденційності згідно нормативним документам України.

110. Опишіть критерії цілісності згідно нормативним документам України.

111. Опишіть критерії доступності згідно нормативним документам України.

112. Опишіть критерії спостереженості згідно нормативним документам України.

113. Опишіть критерії гарантій згідно нормативним документам України.

114. Опишіть критерій цілісності «Відкат» згідно нормативним документам України.

115. Опишіть критерій спостереженості «Достовірний канал» згідно нормативним документам України.