Программирование кибериммунных систем на языке C++.фип_БАК_Прикладная информатика [09.03.03]_н/с

1. Что такое компилятор?
2. Что такое функция в программировании?
3. Что значит «статически типизированный язык»?
4. Что такое переменная в программировании?
5. Можно ли преобразовать переменную к другому типу данных?
6. Как вывести текст “Hello World!” в консоль?
7. Может ли быть опущен блок ˂else˃ в условном операторе?
8. Как обозначается логическая операция «И»?
9. Что такое итерация цикла?
10. Что нужно добавить в цикле while (true) для выхода из цикла?
11. Сколько раз выполнится тело цикла for (int i = 0; i ˂ 7; i+=2)
12. С какого индекса начинается массив?
13. Выберите истинное утверждение об инициализации массива
14. Могут ли в массиве быть переменные разных типов данных?
15. Что хранит в себе указатель?
16. Что будет, если к указателю прибавить целое число?
17. Что обязательно нужно делать после выделения памяти под указатель с помощью оператора new?

18. Что получится при сложении двух указателей?
19. Что такое стек?
20. Существует ли в программировании чистая случайность?
21. Что позволяет сделать отладчик в Visual Studio?
22. Какая строка считается бОльшей в C++?
23. Что такое конкатенация строк?
24. Как считать предложение (слова, разделённые пробелами) с консоли и записать его в переменную типа string?
25. Что такое файл?
26. Файл был открыт для записи. Что будет, если его не закрыть?
27. Как вызвать функцию?
28. При передаче аргументов по значению:
29. Перегруженные функции это:
30. Функция является рекурсивной если:
31. Какова суть кибериммунного подхода к разработке?
32. Какова цель принципа минимизации доверенной кодовой базы в кибериммунной системе?
33. С чего начинается создание кибериммунных решений?
34. Что представляют собой предположения безопасности?
35. Какой метод используется для определения предположений безопасности?
36. Что представляют собой «артефакты» разработки в кибериммунном подходе?
37. Что представляют собой цели безопасности для кибериммунной информационной системы?

38 Какие методы могут использоваться для определения целей безопасности? Выберите все верные ответы

39 Какие фундаментальные правила лежат в основе кибериммунной системы? Выберите все верные ответы

40 Для обеспечения кибериммунного подхода в процессе разработки необходимы требования к организации разработки и требования к … и дизайну системы.

41 Доверенная кодовая база - это тот код, который влияет на наши … в системе, на то как она работает, какую ценность она приносит.

42 В киберимунном подходе требования безопасности приравниваются к … требованиям и влияют на выбор архитектуры решения и аппаратной базы.

43 Кибериммунный подход предъявляет требования к результатам … этапа разработки.

44 … – первый артефакт для построения кибериммунной системы

45 Для определения примерных объемов работ, трудоемкости и цены создания безопасной системы необходима диаграмма … .

46 Установите соответствие между размером (объемом) кода компонентов системы и их обозначениями:

47 Установите соответствие между элементами системы и их обозначениями:

48 Установите соответствие между терминами и их определениями:

49 Расположите этапы кибериммунного процесса по порядку их выполнения:

50 Расположите этапы кибериммунного процесса по порядку их выполнения:

51 Как реализуется архитектура FLASK в кибериммунном подходе?

52 Какая цель у концепции Zero Trust?

53 Что является ключевыми принципами концепции нулевого доверия? Выберите все верные ответы

54 Что может входить в комплекс мероприятий по внедрению «нулевого доверия»? Выберете все верные ответы

55 Что включает в себя политика минимальных привилегий?

56 Какие системы в российских стандартах соответствуют системам с разделением доменов?

57 Что предполагает концепция системы с разделением доменов?

58 Secure By Design предполагает, что … должны быть интегрированы на ранних стадиях проектирования, чтобы обеспечить надежную защиту от киберугроз.

59 Каждый домен безопасности полагается на свои собственные функции безопасности и не доверяет никому, кроме … – самого доверенного компонента всей системы.

60 Концепция … — многоуровневая система безопасности с изолированными разделами.

61 Архитектура … — архитектура безопасности операционной системы, которая обеспечивает гибкую поддержку политик безопасности.

62 Нулевое доверие — концепция информационной безопасности, предполагающая … доверия к каким бы то ни было объектам IT-инфраструктуры организации, будь то пользователи, устройства или программы.

63 Все компоненты, входящие в состав системы, должны быть полностью … друг от друга, внешней среды и не влиять на работу друг друга.

64 … подразумевает, что все информационные потоки, которые проходят в системе при взаимодействии этих компонентов должны обязательно проверяться.

65 … количество целей безопасности приведет к тому, что потребуется создавать более дорогие и сложные системы.

66 В комплекс мероприятий по внедрению «нулевого доверия» может входить настройка … в соответствии с политиками безопасности.

67 Еще до формального моделирования угроз нужно определить критические части системы, непосредственно отвечающие за … системы, и изолировать их от любого потенциально возможного нежелательного воздействия.

68 Суть Secure by Design заключается в проектировании киберсистем, в которых меры безопасности глубоко интегрированы в … и программный код решения и являются его частью.

69 Установите соответствия между свойствами монитора безопасности и их обозначениями.

70 Установите соответствия между терминами и их определениями.

71 Каким образом претворяется в жизнь архитектура FLASK в рамках кибериммунного подхода?

72 Какой метод используется для определения предположений безопасности?

73 Что является главными принципами концепции нулевого доверия? Выберите все верные ответы

74 Что НЕ входит в комплекс мероприятий по внедрению «нулевого доверия»? Выберете все верные ответы

75 Что представляют собой цели безопасности?

76 Что включает в себя политика минимальных привилегий?

77 Что представляют собой «артефакты» разработки в кибериммунном подходе?

78 Что предполагает концепция системы с разделением доменов?

79 Какова основная цель концепции Zero Trust?

80 Какие методы могут использоваться для определения целей безопасности? Выберите все верные ответы

81 С чего начинается создание кибериммунных решений?

82 Что представляют собой предположения безопасности?

83 Какова цель принципа минимизации доверенной кодовой базы в кибериммунной системе?

84 Какое правило НЕ относится к кибериммунной системе?

85 Какие системы в российских стандартах соответствуют системам с разделением доменов?

86 Какова суть кибериммунного подхода к разработке?

87 Для обеспечения кибериммунного подхода в процессе разработки необходимы требования к организации разработки и требования к архитектуре и … системы.

88 … - это тот код, который влияет на наши активы в системе, на то как она работает, какую ценность она приносит.

89 В киберимунном подходе требования … приравниваются к функциональным требованиям и влияют на выбор архитектуры решения и аппаратной базы.

90 Кибериммунный подход предъявляет требования к результатам … этапа разработки.

91 Концепция безопасности продукта – первый … для построения кибериммунной системы

92 «…» - выходные данные каждого этапа разработки в кибериммунном подходе.

93 Secure By Design предполагает, что меры безопасности должны быть интегрированы на … стадиях проектирования, чтобы обеспечить надежную защиту от киберугроз.

94 Каждый домен безопасности полагается на свои собственные функции безопасности и не доверяет никому, кроме ядра разделения – самого … компонента всей системы.

95 Концепция … — многоуровневая система безопасности с изолированными разделами.

96 Архитектура … — архитектура безопасности операционной системы, которая обеспечивает гибкую поддержку политик безопасности.

97 … — концепция информационной безопасности, предполагающая отсутствие доверия к каким бы то ни было объектам IT-инфраструктуры организации, будь то пользователи, устройства или программы.

98 Все компоненты, входящие в состав системы, должны быть полностью … друг от друга, внешней среды и не влиять на работу друг друга.

99 Контроль подразумевает, что все информационные потоки, которые проходят в системе при взаимодействии этих компонентов должны обязательно ….

100 Большое количество … безопасности приведет к тому, что потребуется создавать более дорогие и сложные системы.

101 В комплекс мероприятий по внедрению «нулевого доверия» может входить настройка … в соответствии с политиками безопасности.

102 Еще до формального моделирования угроз нужно определить … части системы, непосредственно отвечающие за активы системы, и изолировать их от любого потенциально возможного нежелательного воздействия.

103 Суть … заключается в проектировании киберсистем, в которых меры безопасности глубоко интегрированы в архитектуру и программный код решения и являются его частью.

104 Установите соответствия между свойствами монитора безопасности и их обозначениями.

105 Установите соответствия между терминами и их определениями.

106 Установите соответствие между размером (объемом) кода компонентов системы и их обозначениями:

107 Установите соответствие между элементами системы и их обозначениями:

108 Установите соответствие между терминами и их определениями:

109 Расположите этапы кибериммунного процесса по порядку их выполнения:

110 Расположите этапы кибериммунного процесса по порядку их выполнения: