Информационная безопасность и защита информации.dor_БАК_24-178-Б

1. Информационная … – это защита информации и поддерживающей инфраструктуры от случайных или намеренных воздействий естественного или искусственного происхождения, которые могут нанести значительный ущерб участникам информационных отношений, включая владельцев и пользователей информации и поддерживающей инфраструктуры
2. … информационной безопасности – это условия и факторы, которые создают потенциальную или реальную опасность нарушения защиты информации
3. … – это попытка реализовать угрозу информационно безопасности
4. «… злоумышленник» – это сотрудник подразделения организации, зарегистрированный как пользователь системы, действующий целенаправленно из корыстных интересов или мести за нанесенную обиду, возможно в сговоре с лицами, не являющимися сотрудниками организации
5. Те, кто потенциально может совершить атаку, – это … угрозы
6. Информационные … – это процессы, методы поиска, сбора, хранения, обработки, предоставления и распространения информации, а также способы осуществления этих процессов и методов
7. Право на защиту информации у человека и организации возникает на основе …
8. … – это любые сведения (сообщения, данные) вне зависимости от формы их представления
9. Установите соответствие между свойствами информации и их характеристиками:
10. Расположите уровни защиты информации в порядке от наиболее значимого к наименее значимому:
11. … защита информации – это защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением

12 В области защиты информации издан Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении … информационной безопасности Российской Федерации»

13 В области защиты информации издан Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению … Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»

14 В области защиты информации издан Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений … характера»

15 … Правительства РФ– это акты, имеющие нормативный характер (то есть адресованные неограниченному кругу лиц и предполагающие постоянное или многократное действие)

16 Информационная … — совокупность информационных систем, сетей и ресурсов, используемых для обработки, хранения и передачи информации.

17 В … Конституции РФ говорится, что «Человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина – обязанность государства»

18 В … Конституции РФ говорится, что «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются»

19 Установите соответствие между законами в области защиты информации и их названиями:

20 Расположите в хронологической последовательности этапы реализации системы обеспечения информационной безопасности (СОИБ):

21 … защита информации – это установление порядка работы и взаимодействия сотрудников на основе законов и правил, который позволяет предотвратить или значительно усложнить незаконное получение конфиденциальной информации

22 … мероприятия по обеспечению информационной безопасности – это мероприятия, которые осуществляются при определенных изменениях в защищаемой системе или внешней среде

23 … защиты информации – это комплекс технических и организационных мер, направленных на обеспечение информационной безопасности организации

24 … мероприятия по обеспечению информационной безопасности – это мероприятия, которые проводятся один раз и повторяются только после полного пересмотра принятых решений

25 К … мероприятиям по обеспечению информационной безопасности относятся: создание научно-технической и методологической основы защиты системы, включая концепции и руководящие документы; мероприятия, проводимые при проектировании, строительстве и оборудовании объекта; специальные проверки всех технических средств и т.д.

26 К … проводимым мероприятиям по обеспечению информационной безопасности относятся: распределение / разграничение реквизитов разграничения доступа (например, раздача паролей); анализ системных журналов и принятие мер по обнаруженным недостаткам и проблемам; анализ состояния и оценка эффективности мер защиты информации и др.

27 Организационная защита информации включает в себя … (укажите 2 варианта ответа)

28 Условия эффективной организационной защиты информации включают в себя … (укажите 2 варианта ответа)

29 Установите соответствие между принципами организационной защиты информации и их характеристиками:

30 Расположите группы сотрудников службы безопасности в иерархическом порядке (снизу вверх):

31 … – это комплекс мер и подходов, которые направлены на защиту информации от внешних и внутренних угроз на объектах информатизации

32 … источники появления угрозы – это источники, вызванные воздействиями на информационную систему объективных физических процессов или стихийных природных явлений, не зависящих от человека

33 … источники появления угрозы – это угрозы, вызванные деятельностью человека

34 Уязвимости делят на классы: объективные, случайные и …

35 … уязвимости – это тип угроз, связанный с техническими характеристиками оборудования, которое необходимо защитить

36 … уязвимости часто возникают из-за ошибок, допущенных сотрудниками на этапе создания систем хранения и защиты информации

37 Главная … информационной безопасности – защитить информацию и инфраструктуру, которая ее обрабатывает, от потери или утечки данных третьим лицам

38 Согласно ГОСТ …, ПЭМИ – это паразитные электромагнитные излучения, возникающие при работе средств электронной обработки информации

39 Установите соответствие между принципами создания системы информационной безопасности на объекте информатизации и их характеристиками:

40 Установите правильный порядок реализации метода скремблеров:

41 В ГОСТ «Защита информации. Основные термины и определения» … описывается как состояние защищенности информации, при котором гарантируются ее конфиденциальность, доступность и целостность

42 Информационная … – это совокупность информации, которая содержится в базах данных, информационных технологий, обеспечивающих ее обработку, и технических средств

43 … – это информация, позволяющая точно идентифицировать человека

44 … тайна – это данные, находящиеся под ограничением государственных органов и требующие специальных мер защиты

45 … информационной системы – это гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы и обеспечивающие обработку информации, которая содержится в ее базах данных

46 …информации – это лицо, которое самостоятельно создало информацию или получило право разрешать или ограничивать доступ к информации на основании закона или договора

47 Установите соответствие между уровнями информационное безопасности и их характеристиками:

48 Упорядочьте шаги по внедрению политики информационной безопасности в компании:

49 Расположите в иерархическом порядке уровни документации, которые включает в себя эффективная политика информационной безопасности компании, от высшего уровня к низшему:

50 Установите соответствие понятий и их определений:

51 … акты – это нормативно-правовые документы министерств и ведомств по реализации направлений государственного управления

52 … тайна — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

53 … тайна – это режим конфиденциальности информации, который позволяет ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду

54 … законы – ключевой элемент законодательного регулирования в России, они могут затрагивать любые вопросы, отнесенные Конституцией РФ к предметам ведения Федерации либо совместного ведения Федерации и субъектов РФ, требующие государственного регулирования

55 Конфиденциальные … — информация, к которой ограничен доступ, и которая не подлежит разглашению без разрешения владельца.

56 Грамотный подбор кадров и своевременная мотивация персонала обеспечивают до … гарантий успешной защиты коммерческой тайны

57 Соедините элементы задания, чтобы получилось верное предложение:

58 Соедините элементы задания, чтобы получилось верное предложение:

59 Расположите в хронологической последовательности этапы планирования системы обеспечения информационной безопасности (СОИБ):

60 Расположите в правильной последовательности действия инспектора при оценке информационной безопасности в кредитной организации:

61 … — взаимодействие различных элементов системы защиты для обеспечения комплексной безопасности.

62 … система защиты информации – это комплексный подход к обеспечению безопасности информационных активов организации, основанный на многоуровневой защите

63 Работа по обеспечению информационной безопасности должна быть спланирована на основании принципа … подхода

64 К … мероприятиям по обеспечению информационной безопасности относятся: мероприятия, связанные с кадровыми изменениями в составе персонала; мероприятия, связанные с ремонтом и модификацией оборудования, программного обеспечения

65 Организационная защита информации включает в себя … (укажите 2 варианта ответа)

66 … создания систем защиты информации – минимизировать риски и возможный ущерб, который может быть нанесен владельцу информации

67 Сопоставьте принципы многорубежной системы защиты информации и их характеристики:

68 Сопоставьте сотрудников службы безопасности с их обязанностями:

69 Расположите в правильной последовательности этапы аудита информационной безопасности:

70 Упорядочьте шаги разработки и внедрения систем защиты информации:

71 … источники появления угроз делят на непреднамеренные и преднамеренные

72 … искусственные источники появления угроз вызваны ошибками проектирования и разработки компонентов информационных систем, а также ошибками в действиях персонала в процессе эксплуатации; они бывают только внутренними

73 … искусственные источники появления угроз вызваны действиями нарушителей

74 Преднамеренные искусственные источники появления угроз бывают …

75 … информационной безопасности не возникают сами по себе, они проявляются через взаимодействие с наиболее слабыми звеньями системы защиты, то есть через факторы уязвимости

76 Разрабатываемые на объекте информатизации документы, которые регулируют вопросы информационной безопасности, относятся к … методам защиты информации

77 Установите хронологическую последовательность этапов развития информационной безопасности:

78 Установите правильную последовательность этапов проверки системы обеспечения информационной безопасности (СОИБ):

79 … — программное обеспечение для информационной безопасности, расширяющее адресное пространство и создающее ложные информационные направления, изменяя IP-адреса.

80 Сопоставьте виды критериев ранжирования уязвимостей с их характеристиками:

81 Один из сотрудников крупной компании, занимающейся разработкой программного обеспечения, случайно отправил конфиденциальные данные клиента на личную электронную почту. Какие меры ему нужно предпринять?

82 В компании решили использовать новое облачное хранилище для всех данных. Какие действия необходимо предпринять, чтобы соблюсти принципы информационной безопасности?

83 В вашей компании внедряется система двухфакторной аутентификации. Сотрудники выражают недовольство, считая это неудобным. Как лучше объяснить необходимость этого шага?

84 Мария работает в крупной компании, занимающейся обработкой и хранением персональных данных клиентов. Недавно она получила запрос от руководства об усилении мер по защите данных в связи с новыми нормативными требованиями, а также прошла проверку, которая выявила несколько недостатков в системе безопасности. Руководитель попросил её подготовить план улучшения информационной безопасности с учётом нормативно-правовых требований, а также включить инструкции для сотрудников по обращению с персональными данными. Как Мария должна подойти к выполнению задания, чтобы соответствовать законодательству и требованиям компании?

85 Компания приняла решение хранить все данные о транзакциях клиентов на серверах за пределами страны. Какие правовые аспекты следует учесть?

86 При аудите информационной системы в вашей компании выявлены нарушения в соблюдении закона о защите персональных данных. Как лучше всего поступить в этой ситуации?

87 Компания обновляет политику информационной безопасности. Вам поручено организовать обучение сотрудников, чтобы они соблюдали новые правила. Какие шаги необходимо предпринять для успешного внедрения?

88 Компания «ИнфоТех» активно работает над повышением уровня информационной безопасности и защиты данных. В рамках этих мер генеральный директор поручил службе информационной безопасности разработать и внедрить административные и организационные меры для предотвращения утечек информации. Иван, руководитель службы безопасности, составляет список мер, которые будут обязательны для исполнения всеми сотрудниками. Ему нужно продумать, как эффективно организовать процесс внедрения этих мер, чтобы обеспечить их понимание и соблюдение. Какой подход к выполнению задачи Ивану следует выбрать?

89 При внутренней проверке было выявлено, что несколько сотрудников используют простые пароли, что противоречит политике компании. Как необходимо поступить?

90 Ваша компания внедряет новую информационную систему для обработки и хранения конфиденциальных данных. Какими должны быть первоочередные меры для защиты информации в этой системе?

91 Во время проведения планового аудита информационной системы обнаружено, что большинство пользователей используют одноразовые пароли для доступа к критически важным данным. Какие меры следует принять для повышения уровня безопасности?

92 В информационной системе, с которой работает ваша компания, начали появляться признаки несанкционированного доступа и возможных атак. Какие действия необходимо предпринять для минимизации рисков утечки данных?