Основы информационной безопасности.ои(dor_БАК)

1. … – это цифровая база данных информации, которая отражает все совершенные транзакции; все записи представляются в виде блоков, которые связаны между собой специальными ключами

2. … данные человека включают в себя отпечатки пальцев, радужную оболочку глаза, сетчатку глаза, геометрию лица и др.; эти данные являются эталонными, что позволяет получить доступ к информации без использования сложных паролей

3. Установите соответствие понятий и их характеристик:

4. … информации – это сохранение целостности и защита от утечки сведений, которые не предназначены для общего использования и несут интеллектуальную или экономическую ценность для обладателя

5. Установите соответствие методов обеспечения конфиденциальности и соответствующих задач, стоящих перед отделом IT-безопасности:

6. … шифрование – это способ шифрования данных, при котором один и тот же ключ используется и для кодирования, и для восстановления информации

7. … (система обнаружения вторжений) – это программный продукт или устройство, предназначенные для выявления несанкционированной и вредоносной активности в компьютерной сети или на отдельном хосте

8. … – это данные, оставляемые пользователем при использовании информационных систем; анализ этих данных может выявить несанкционированную активность и утечки информации, а также помочь в идентификации источников угроз

9. Такой метод выявления утечек, как …, используется для мониторинга сетевого трафика и системных событий

10. … инженерия – это метод получения доступа к конфиденциальным данным с помощью психологического воздействия на человека, обладающего информацией или доступом к защищенным системам, где она хранится

11 Методы, обычно изложенные в опубликованных материалах, которые используются для защиты киберсреды пользователя или организации, – это … информационной безопасности

12 Защищаемые государством сведения, распространение которых может нанести ущерб безопасности РФ, – это …

13 Установите соответствие органа (системы органов) и его характеристик:

14 … – это совокупность требований, правил, организационных, технических и иных мер, направленных на защиту сведений, составляющих государственную тайну

15 Режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду, – это …

16 Процесс, в результате которого для пользователя определяется его уникальный идентификатор, однозначно определяющий его в информационной системе, – это …

17 … – это реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него

18 Установите правильную последовательность этапов классификации информации как государственной тайны:

19 Установите соответствие принципов защиты информации и их характеристик:

20 … информационных технологий – это проверка соответствия IT-систем, использующихся в компании, требованиям безопасности, по результатам которой выдается официальное подтверждение установленного образца

21 … событий – это способ записи, управления и аудита информации о событиях в системе

22 Системы для управления событиями, полученными из различных источников, позволяющие анализировать события в режиме реального времени, имеют сокращенное английское обозначение …

23 Установите правильный порядок разработки политика информационной безопасности:

24 Установите соответствие ключевых элементов информационной безопасности и их содержания:

25 Принцип … предполагает предоставление пользователям только тех прав доступа, которые нужны для выполнения их работы

26 Система должна точно идентифицировать пользователей, которым предоставляет доступ к информации: после идентификации следует процесс …, который подтверждает, что пользователь – действительно тот, за кого себя выдает

27 … информацию раскрывать можно только ограниченно, и это может нанести определенный вред организации

28 … собираемой и хранимой информации – это стратегия, суть которой заключается в уменьшении количества данных, которые организация собирает, обрабатывает и хранит

29 … – это процесс проверки всех событий безопасности, получаемых от различных источников; источниками событий могут быть антивирусные системы, журналы операционных систем, сетевое оборудование и др.

30 Английское сокращенное обозначение управления событиями безопасности – …

31 … информационной безопасности – это независимая проверка системы защиты данных, которая соответствует нескольким критериям, например, требованиям закона или стандартам компании

32 Установите соответствие типов вредоносных программ могут и их характеристик:

33 Злоумышленники, чтобы захватить управление над операционной системой, привести ее к отказу в обслуживании или получить доступ к защищенной информации, осуществляют прямые сетевые …, такие как сканирование портов, или используют вредоносные программы

34 Согласно принципу …, каждый участник процесса организации защиты информации получает информацию о своих задачах в данной области и последствиях нарушения установленных правил

35 … – это сетевые атаки, при которых злоумышленник перехватывает и модифицирует трафик между двумя сторонами, часто для кражи данных

36 …, или межсетевой экран, контролирует входящий и исходящий сетевой трафик на основе заранее установленных правил безопасности; может быть программным или аппаратным

37 Установите соответствие названий и описаний компаний и программных продуктов:

38 … защита сетевой инфраструктуры включает меры по обеспечению безопасности оборудования, которое используется для хранения и передачи данных (серверов, коммутаторов и маршрутизаторов), а также контроль доступа в помещения с оборудованием, использование замков, систем видеонаблюдения и охраны

39 Компьютерный … – вид вредоносных программ, способных внедряться в код других программ, системные области памяти, загрузочные секторы и распространять свои копии по разнообразным каналам связи.

40 … данных на уровне хранения – это метод защиты информации, при котором данные преобразуются из исходного видимого формата в такой формат, доступ к которому возможен только с соответствующим ключом, что помогает обезопасить данные от несанкционированного доступа

41 Установите соответствие понятий и их характеристик:

42 … – это цифровая база данных информации, отражающая все совершенные транзакции; все записи представляются в виде блоков, которые связаны между собой специальными ключами

43 … аутентификация – это метод аутентификации, основанный на предъявлении уникальных биологических характеристик человека, таких как отпечаток пальца, сетчатка или радужная оболочка глаза, геометрия лица, форма ладони

44 … безопасности – это систематический процесс мониторинга и анализа событий в информационной системе для обнаружения нарушений безопасности и оценки их последствий

45 Установите соответствие аспектов безопасности и их значения:

46 … – это способ шифрования данных, при котором один и тот же ключ используется и для кодирования, и для восстановления информации

47 Установите соответствие сокращенных обозначений и их содержания:

48 … – это небольшой файл в формате JSON, в котором хранится информация о пользователе, например, уникальный идентификатор, время входа в систему и истечения срока действия

49 Установите соответствие компонентов целостности данных и информационных систем и характеристик этих компонентов:

50 Контрольная … – это значение, которое может быть получено с помощью какой-либо хеш-функции (например, MD5)

51 В Российской Федерации главный документ в сфере защиты информационной безопасности – это …, где определены основные понятия, принципы и правовые основы обеспечения информационной безопасности

52 Защищаемые государством сведения, распространение которых может нанести ущерб безопасности РФ, – это …

53 Установите соответствие органа (системы органов) и его характеристик:

54 Режим … – это совокупность требований, правил, организационных, технических и иных мер, направленных на защиту сведений, составляющих государственную тайну

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

56 Установите соответствие понятия и его характеристики:

57 … секретности – это реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него

58 Установите соответствие принципов защиты информации и их характеристик:

59 Федеральный закон … устанавливает основные принципы обработки и защиты информации в информационных системах, включая персональные данные граждан, и регулирует отношения, связанные с созданием, получением, передачей и распространением информации

60 Установите правильную последовательность этапов классификации информации как государственной тайны:

61 … – это способ записи, управления и аудита информации о событиях в системе

62 Системы мониторинга событий можно разделить на две категории – в частности, системы, осуществляющие сбор и анализ действий пользователей для поиска возможных внутренних угроз и атак, имеют сокращенное английское обозначение …

63 Установите соответствие ключевых элементов информационной безопасности и их содержания:

64 … информационной безопасности – это формализованный документ, который устанавливает общие принципы, цели и требования в области защиты информации внутри организации; этот документ служит основой для разработки конкретных процедур и мер

65 Установите правильный порядок разработки политика информационной безопасности:

66 Установите соответствие ключевых аспектов регулирования прав доступа к информации и их предназначения:

67 Расположите уровни конфиденциальности информации в порядке увеличения ее закрытости:

68 … – это стратегия, суть которой заключается в уменьшении количества данных, которые организация собирает, обрабатывает и хранит

69 … событий информационной безопасности – это процесс проверки всех событий безопасности, получаемых от различных источников; источниками событий могут быть антивирусные системы, журналы операционных систем, сетевое оборудование и др.

70 Английское сокращенное обозначение управления информацией о безопасности – …

71 … информационной безопасности – это независимая проверка системы защиты данных, которая соответствует нескольким критериям, например, требованиям закона или стандартам компании

72 Сетевая … – это вторжение в операционную систему удаленного компьютера, которое предпринимают злоумышленники, чтобы захватить управление над операционной системой, привести ее к отказу в обслуживании или получить доступ к защищенной информации

73 Установите соответствие основных принципов организации процесса защиты информации и их характеристик:

74 Установите соответствие типов вредоносных программ могут и их характеристик:

75 … – это распределенные атаки типа «отказ в обслуживании», которые представляют собой массированные запросы к ресурсу, приводящие к его перегрузке и недоступности для легитимных пользователей

76 Малварь (Malware), или … программное обеспечение, – это любой тип программы или кода, который наносит ущерб системе, крадет данные или нарушает нормальную работу сети; это общее название для всех видов кибер-угроз, таких как: вирусы, трояны, шпионские программы и др.

77 Установите соответствие названий и описаний компаний и программных продуктов:

78 Попытки определить открытые порты и уязвимые службы на атакуемой машине, – это … портов

79 … – это вид вредоносных программ, способных внедряться в код других программ, системные области памяти, загрузочные секторы и распространять свои копии по разнообразным каналам связи

80 Процесс … занимает центральное место в стратегии защиты данных от потенциальных утечек, т. к. осведомленность каждого члена организации о существующих угрозах, методах их нейтрализации, а также о правилах корректного обращения с корпоративной информацией – это фундаментальный аспект в обеспечении надежной защиты данных

81 Физическая защита оборудования включает меры по защите от несанкционированного физического доступа, повреждения или кражи. Существуют разные методы физической защиты. Один из этих методов позволяет вести постоянный мониторинг помещений с оборудованием. Это помогает выявить потенциальных злоумышленников, а также позволяет оперативно реагировать на инциденты и фиксировать все действия в зоне доступа к оборудованию. Назовите данный метод.

82 Технические средства защиты информации предназначены для того, чтобы обеспечивать безопасность данных. Они предотвращают несанкционированный доступ, защищают от угроз и поддерживают целостность и доступность информации. В частности, есть технические средства защиты информации, которые: - контролируют входящий и исходящий сетевой трафик на основе заранее установленных правил безопасности; - действуют как барьер между защищенной внутренней сетью и ненадежными внешними сетями, такими как интернет; - реализовываются в аппаратной и в программной форме; - используются для защиты отдельных компьютеров и сетевых инфраструктур организаций. О каком виде технических средств защиты информации говорится в описании?

83 Технические средства защиты информации предназначены для того, чтобы обеспечивать безопасность данных. Они предотвращают несанкционированный доступ, защищают от угроз и поддерживают целостность и доступность информации. В частности, есть технические средства защиты информации, которые: - мониторят сетевой трафик на подозрительные активности и угрозы; - активно блокируют и предотвращают вторжения; - используют разные методики для анализа трафика и идентификации атак; - разворачиваются на ключевых точках сети для защиты критически важных систем и данных; О каком виде технических средств защиты информации говорится в описании?

84 Инструменты проверки соответствия нормативам информационной безопасности помогают организациям убедиться, что их системы и процессы соответствуют установленным требованиям и стандартам. Для проверки соответствия нормативам используют документы, на которые ориентируются в процессе разработки и эксплуатации ИТ-продуктов. Один из таких документов описывает назначение ИТ-продукта, характеризует среду его эксплуатации и устанавливает задачи защиты и требования, которым должен отвечать продукт. Этот документ служит основой для создания спецификаций средств защиты, обеспечивая понимание требований безопасности, к которым должен быть адаптирован продукт. О каком документе идет речь?

85 Инструменты проверки соответствия нормативам информационной безопасности помогают организациям убедиться, что их системы и процессы соответствуют установленным требованиям и стандартам. Для проверки соответствия нормативам используют документы, на которые ориентируются в процессе разработки и эксплуатации ИТ-продуктов. Один из таких документов составляется на завершающем этапе квалификационного анализа, результат которого – официальное заключение о соответствии ИТ-продукта требованиям безопасности, основанным на единых критериях. Этот документ подтверждает качество и надежность средств защиты продукта, что способствует повышению доверия к продукту со стороны потребителей и увеличению его конкурентоспособности на рынке. О каком документе идет речь?

86 Инструменты проверки соответствия нормативам информационной безопасности помогают организациям убедиться, что их системы и процессы соответствуют установленным требованиям и стандартам. Для проверки соответствия нормативам используют документы, на которые ориентируются в процессе разработки и эксплуатации ИТ-продуктов. Один из таких документов включает в себя спецификации средств защиты и обоснование соответствия ИТ-продукта задачам защиты. Этот документ представляет собой подробное описание мер безопасности, которые воплощаются в продукте. Он считается ключевым элементом для анализа соответствия продукта установленным требованиям безопасности. О каком документе говорится в описании?

87 Процессы создания и управления системой информационной безопасности включают в себя ряд мер и процедур, направленных на защиту информационных активов компании от разных угроз. В чем состоит главная цель этих процессов?

88 Медицинский центр сохраняет информацию о своих пациентах на внешних носителях информации, которые хранятся в безопасном месте вне медицинского учреждения. Это обеспечивает возможность восстановить данные в случае их потери или повреждения в результате технического сбоя или кибератаки. Назовите описанную стратегию защиты информации.

89 Компания, которая занимается обработкой конфиденциальных финансовых данных, регулярно применяет патчи безопасности к своим серверам баз данных и приложений, чтобы предотвратить уязвимости, которые могли бы позволить хакерам украсть или изменить ценную информацию. Назовите описанную стратегию защиты информации.

90 В компании, которая занимается разработкой программного обеспечения, доступ к исходному коду проектов строго регламентирован. Разработчикам открыты свои ветки репозитория, а доступ к ветке релиза имеют только старшие разработчики и менеджеры проекта. Таким образом минимизируется риск, что кто-то случайно или преднамеренно внесет вредоносные изменения в продукт. Какой принцип организации процесса защиты информации реализуется в приведенном примере?

91 В медицинском учреждении за соблюдение конфиденциальности информации о пациентах отвечает специально назначенный сотрудник. Он отслеживает доступ к медицинским записям, обучает персонал правилам работы с конфиденциальной информацией и реагирует на инциденты, связанные с утечкой данных. Это позволяет эффективно предотвращать и минимизировать возможные нарушения в области защиты информации. Какой принцип организации процесса защиты информации реализуется в приведенном примере?

92 Существуют различные технологические средства защиты данных. В частности, есть системы, предназначенные для предотвращения утечки конфиденциальной информации за пределы корпоративной сети. Эти системы контролируют и фильтруют потоки данных, которые перемещаются внутри и за пределами организации, и могут блокировать передачу чувствительной информации по неавторизованным каналам. Такая система следит за тем, куда и как движется информация внутри компании и за ее пределами, проверяет, соответствует ли это перемещение установленным правилам, и предотвращает утечку информации. Например, такая система может помочь, когда вы отправляете кому-то электронное письмо, но не хотите, чтобы его прочитал кто-либо еще, кроме указанного получателя. О каком технологическом средстве защиты данных идет речь в приведенном описании?