Управление информационной безопасностью.ти (2/2)

1. Что такое инцидент информационной безопасности?
2. Какой этап НЕ входит в процесс управления инцидентами ИБ?
3. Что такое SIEM-система?
4. Какой инструмент используется для отслеживания и управления инцидентами ИБ?
5. Что включает в себя план реагирования на инциденты (IRP)?
6. Что такое непрерывность бизнеса (BC)?
7. Что такое анализ влияния на бизнес (BI)?
8. Что такое Recovery Time Objective (RTO)?
9. Что такое Recovery Point Objective (RPO)?
10. Что такое план обеспечения непрерывности бизнеса (BCP)?
11. Что такое план восстановления после сбоев (DRP)?
12. Какой тип резервного копирования копирует только те данные, которые изменились с момента последнего полного или инкрементного копирования?
13. Какой тип резервного копирования копирует все данные, которые изменились с момента последнего полного резервного копирования?
14. Что такое отказоустойчивость системы?
15. Что предполагает тестирование планов BCP и DRP?
16. Какой из следующих вариантов НЕ является примером инцидента ИБ?

17. В какой фазе управления инцидентом происходит идентификация источника атаки?
18. Какой из следующих элементов НЕ является частью Incident Response Plan (IRP)?
19. Что такое Tabletop exercises в контексте тестирования планов BCP и DRP?
20. Какая модель облачных вычислений предполагает наибольшую ответственность клиента за обеспечение безопасности?
21. Что из перечисленного НЕ является риском для ИБ в облачной среде?
22. Какой стандарт регулирует защиту персональных данных граждан ЕС в облачной среде?
23. Какой метод помогает защитить IoT-устройства от внешних атак, изолируя их от основной сети?
24. Что такое Big Data?
25. Как можно использовать Big Data в ИБ?
26. Какой метод используется для сокрытия конфиденциальной информации в больших наборах данных?
27. Какую угрозу представляет собой “отравление данных” в контексте AI?
28. Что подразумевает собой концепция Zero Trust Architecture?
29. Что такое SOAR (Security Orchestration, Automation and Response)?
30. Что такое Threat Intelligence?
31. Что такое DevSecOps?
32. Что необходимо учитывать при оценке рисков ИБ при переходе на облачные технологии?
33. Что следует предпринять для защиты IoT-инфраструктуры?
34. Что является ключевым преимуществом использования искусственного интеллекта в системах обнаружения вторжений?