



## Информационная безопасность компьютерных систем.ТИ

- 1) Что является примером контрмеры безопасности (security control)?
- 2) Какой из этих терминов описывает слабость в системе безопасности, которая может быть использована для нанесения вреда?
- 3) Что такое "нулевой день" (нулевой день) в контексте информационной безопасности?
- 4) Какой из следующих нормативных документов наиболее непосредственно связан с защитой персональных данных?
- 5) Что такое "глубокоэшелонированная оборона" (эшелонированная оборона) в информационной безопасности?
- 6) Что такое "принцип наименьших привилегий" (принцип наименьших привилегий)?
- 7) Что такое фишинг?
- 8) Какое из следующих действий наиболее эффективно для защиты от атак методом "грубой силы" (brute-force)?
- 9) Что такое криптографический хэш?
- 10) Что из перечисленного является наиболее важным для обеспечения физической безопасности серверной комнаты?
- 11) Что такое IDS (Intrusion Detection System)?
- 12) Что такое "аутентификация"?
- 13) Какой из следующих пунктов наиболее важен для реагирования на инцидент информационной безопасности?
- 14) Что такое "сканирование портов"?
- 15) Что означает термин "компрометация" (compromise) в контексте информационной безопасности?
- 16) Какой из следующих факторов наименее важен при выборе надежного пароля?



- 17) Что такое "межсетевой экран" (firewall)?
- 18) Что такое CVE (Common Vulnerabilities and Exposures)?
- 19) Что такое аутентификация?
- 20) Что такое авторизация?
- 21) Что такое "единый вход" (Single Sign-On - SSO)?
- 22) Какой протокол чаще всего используется для аутентификации пользователей в беспроводных сетях Wi-Fi?
- 23) Что такое "LDAP" (Lightweight Directory Access Protocol)?
- 24) Что такое "Kerberos"?
- 25) Что такое "двуухфакторная аутентификация" (2FA) с использованием временных одноразовых паролей (TOTP)?
- 26) Для чего используются списки контроля доступа (ACL)?
- 27) Что такое "авторизация" в контексте веб-приложений?
- 28) Какой из перечисленных типов вредоносного ПО шифрует файлы пользователя и требует выкуп за их расшифровку?
- 29) Что такое сигнатурный анализ в антивирусном ПО?
- 30) Что такое эвристический анализ в антивирусном ПО?
- 31) Что такое межсетевой экран (Firewall)?
- 32) Что такое DMZ (Demilitarized Zone)?
- 33) Какой протокол безопасности чаще всего используется для защиты беспроводных сетей Wi-Fi?
- 34) Что такое DoS-атака (Denial-of-Service)?
- 35) Что такое DDoS-атака (Distributed Denial-of-Service)?
- 36) Что такое "ботнет"?





- 37) Что такое "сниффинг" (sniffing) сетевого трафика?
- 38) Что такое "спуфинг" (spoofing)?
- 39) Что такое "сканер уязвимостей"?
- 40) Что такое "система обнаружения вторжений" (IDS)?
- 41) Что такое "система предотвращения вторжений" (IPS)?
- 42) Что такое Cross-Site Scripting (XSS)?
- 43) Как можно защититься от XSS-атак?
- 44) Что такое Cross-Site Request Forgery (CSRF)?
- 45) Как можно защититься от CSRF-атак?
- 46) Что такое Broken Authentication?
- 47) Что такое Confidential Data Exposure?
- 48) Что такое HTTP-заголовки безопасности?
- 49) Что такое Content Security Policy (CSP)?
- 50) Какой из принципов SOLID наиболее важен с точки зрения безопасности?
- 51) Что такое принцип "Fail Safe"?
- 52) Что такое "управление уязвимостями"?

