examundo

Пробный тест CISSP на русском

Вопросов с ответами: 50. Гиды и переводы сделала и проверила программа. Человек их пока не проверял.

Обновлено 25 ноября 2026 г. · examundo.tech/ru/cissp/

Домен 3: архитектура безопасности

1. Какая криптографическая концепция гарантирует, что отправитель не сможет отрицать отправку сообщения?

Which cryptographic concept ensures that a sender cannot deny having sent a message?

A. Конфиденциальность (confidentiality)
B. Целостность (integrity)
C. Неотказуемость (non-repudiation)
D. Аутентификация (authentication)

---

2. Архитектор безопасности проектирует систему для защиты секретных государственных данных. Какую модель безопасности нужно применить, чтобы информация не передавалась с высоких уровней секретности на низкие?

A security architect is designing a system to protect classified government data. Which security model should be implemented to prevent information from flowing from higher classification levels to lower classification levels?

A. Модель Bell-LaPadula
B. Модель Clark-Wilson
C. Модель Brewer-Nash
D. Модель целостности Biba

---

3. Интернет-магазину нужно безопасно обмениваться симметричными ключами шифрования с браузерами клиентов. Какой протокол следует использовать?

An e-commerce application needs to securely exchange symmetric encryption keys with customers' browsers. Which protocol should be used?

A. TLS с обменом ключами Diffie-Hellman
B. IPsec в транспортном режиме с предварительно согласованными ключами (PSK)
C. Kerberos с билетами TGT (ticket-granting tickets)
D. S/MIME с шифрованием на основе сертификатов

---

4. Для доступа в серверную защищённого объекта требуется правило двух лиц (two-person integrity). Какой тип физического контроля доступа реализует это требование?

A secure facility requires two-person integrity for access to the server room. What type of physical access control implements this requirement?

A. Кодовый замок (cipher lock) со сменой кода раз в квартал

B. Считыватель карт (card reader) с видеозаписью всех входов

C. Биометрический считыватель (biometric reader) с PIN-клавиатурой для многофакторной аутентификации

D. Тамбур-шлюз (mantrap) с двойной аутентификацией, требующий присутствия двух допущенных лиц

---

5. Какое описание ЛУЧШЕ всего соответствует принципу эшелонированной защиты (defense in depth)?

Defense in depth is BEST described as which of the following security principles?

A. Использование нескольких уровней мер безопасности для защиты активов

B. Проектирование систем так, чтобы при ошибках они переходили в безопасное состояние

C. Предоставление пользователям минимальных прав, необходимых для работы

D. Усиление защиты систем (hardening) за счёт удаления лишних служб и функций

---

6. К какому типу мер физической безопасности относится тамбур-шлюз (mantrap)?

A mantrap is classified as which type of physical security control?

A. Превентивная мера (preventive control)

B. Компенсирующая мера (compensating control)

C. Обнаруживающая мера (detective control)

D. Корректирующая мера (corrective control)

---

7. Финансовая система должна не допускать изменения записей о транзакциях неуполномоченными пользователями, но разрешать чтение для аудита. Какая модель безопасности ЛУЧШЕ всего отвечает этому требованию?

A financial system must prevent unauthorized users from modifying transaction records while allowing read access for auditing. Which security model BEST supports this requirement?

A. Модель конфиденциальности Bell-LaPadula

B. Модель Brewer-Nash (Chinese Wall)

C. Модель целостности Biba

D. Модель управления доступом Graham-Denning

---

8. Организация внедряет новую криптосистему для защиты данных в состоянии покоя (data at rest) в облаке. Система должна соответствовать нормативному требованию о депонировании ключей (key escrow) и при этом сохранять операционную независимость от облачного провайдера. Какой подход ЛУЧШЕ всего удовлетворяет обоим требованиям?

An organization is implementing a new cryptographic system to protect data at rest in a cloud environment. The system must support regulatory compliance requirements for key escrow while maintaining operational independence from the cloud provider. Which approach BEST satisfies both requirements?

A. Шифрование на стороне клиента с ключами в локальном HSM и передачей копий ключей на депонирование сторонней службе

B. Конвертное шифрование (envelope encryption) с управляемыми клиентом ключами в службе управления ключами облачного провайдера

C. Прозрачное шифрование данных (TDE) на уровне базы данных с ключами в конфигурации приложения

D. Встроенная служба шифрования облачного провайдера с автоматической ротацией ключей и копией в другом облачном регионе

---

9. Архитектор безопасности выбирает формальную модель безопасности для системы военной разведки, работающей с документами разных уровней секретности. ОСНОВНОЕ требование: не допустить передачу информации на более низкие уровни секретности. Какая модель НАИБОЛЕЕ подходит?

A security architect must select a formal security model for a military intelligence system handling documents at multiple classification levels. The PRIMARY requirement is preventing information from flowing to lower classification levels. Which model is MOST appropriate?

A. Модель целостности Biba

B. Модель целостности Clark-Wilson

C. Модель Bell-LaPadula

D. Модель Brewer-Nash (Chinese Wall)

---

10. В центре обработки данных над серверной прорвало водопроводную трубу. Какая мера контроля среды в помещении (environmental control) ЛУЧШЕ всего предотвратила бы повреждение критичного оборудования водой?

A data center experiences a water pipe burst above the server room. Which environmental control would have BEST prevented water damage to critical equipment?

A. Системы избыточного давления воздуха, не пускающие влагу

B. Датчики протечки воды с автоматическими запорными клапанами

C. Фальшпол, поднимающий оборудование над уровнем пола

D. Системы HVAC с контролем влажности и оповещением

Домен 7: операции безопасности

11. Какая практика управления конфигурацией ЛУЧШЕ всего выявляет несанкционированные изменения конфигурации рабочих (production) серверов?

Which configuration management practice BEST detects unauthorized changes to production server configurations?

A. Регулярно сравнивать фактические конфигурации с утверждёнными базовыми

B. Автоматически одобрять изменения, сделанные привилегированными администраторами

C. Проверять записи о закупке оборудования, не просматривая настройки серверов

D. Заменять утверждённые базовые конфигурации текущими после каждого сканирования

---

12. Какая роль в группе реагирования на инциденты отвечает за то, чтобы первым выявить и локализовать инцидент?

Which role in an incident response team is responsible for initially identifying and containing the incident?

A. Координатор инцидента (incident coordinator)

B. Криминалист (forensic analyst)

C. Сотрудник первичного реагирования (first responder)

D. Ответственный за коммуникации (communications lead)

---

13. Инцидент, вызвавший незначительный сбой в некритичных системах без потери данных, обычно относят к какому уровню серьёзности?

An incident that causes minor disruption to non-critical systems with no data loss would typically be classified as what severity level?

A. Критический
B. Высокий
C. Низкий
D. Чрезвычайный

---

14. При разборе инцидента группа выяснила, что злоумышленник закрепился в системе и оставался незамеченным 87 дней. Какое улучшение в работе службы безопасности НАИБОЛЕЕ эффективно сократит время скрытого присутствия (dwell time) в будущем?

During a post-incident review, the team identifies that the attacker maintained persistence for 87 days before detection. Which security operations improvement would MOST effectively reduce future dwell time?

A. Обязательное ежеквартальное обучение всех сотрудников основам безопасности
B. Установка дополнительных межсетевых экранов на границах сегментации сети
C. Сканирование уязвимостей раз в неделю вместо раза в месяц
D. Непрерывный мониторинг безопасности с поведенческой аналитикой и активным поиском угроз

---

15. Эшелонированная защита (defense in depth) в физической безопасности обычно включает несколько уровней. Какой порядок от внешнего уровня к внутреннему ПРАВИЛЬНЫЙ?

Defense in depth for physical security typically includes multiple layers. Which of the following represents the CORRECT order from outermost to innermost layer?

A. Ограждение периметра, контроль доступа в здание, контроль доступа в помещение, замки на оборудовании
B. Замки на оборудовании, контроль доступа в помещение, контроль доступа в здание, ограждение периметра
C. Контроль доступа в помещение, замки на оборудовании, ограждение периметра, контроль доступа в здание
D. Контроль доступа в здание, ограждение периметра, замки на оборудовании, контроль доступа в помещение

---

16. К какому виду доказательств относятся копии или воспроизведения оригинальных доказательств?

Which type of evidence consists of copies or reproductions of original evidence?

A. Вторичные доказательства (secondary evidence)
B. Наилучшие доказательства (best evidence)
C. Показания с чужих слов (hearsay evidence)
D. Подтверждающие доказательства (corroborative evidence)

---

17. Организация определяет цели аварийного восстановления. Бизнес требует восстановить критичные системы в течение 4 часов после аварии. Какой показатель восстановления определяет это требование?

An organization is defining its disaster recovery objectives. The business requires that critical systems must be restored within 4 hours of a disaster. This requirement defines which recovery metric?

A. Среднее время ремонта (MTTR)
B. Максимально допустимое время простоя (MTD)
C. Целевое время восстановления (RTO)
D. Целевая точка восстановления (RPO)

---

18. План аварийного восстановления организации требует RTO 4 часа и RPO 1 час для клиентской базы данных. Какая стратегия резервного копирования ЛУЧШЕ всего отвечает этим требованиям?

An organization's disaster recovery plan requires a recovery time objective (RTO) of 4 hours and a recovery point objective (RPO) of 1 hour for its customer database. Which backup strategy BEST meets these requirements?

A. Дифференциальные копии (differential backups) каждые 4 часа с хранением на своей площадке

B. Инкрементные копии (incremental backups) каждые 6 часов с хранением на лентах вне площадки

C. Полные копии (full backups) раз в неделю и инкрементные каждый день

D. Полные копии каждую ночь и непрерывная репликация базы данных на тёплую площадку (warm site)

---

19. Сотрудник первичного реагирования (first responder) подходит к скомпрометированному рабочему (production) серверу, который всё ещё включён и обрабатывает транзакции. Какой источник данных, согласно RFC 3227, нужно собрать ПЕРВЫМ при сборе доказательств на работающей системе?

A first responder arrives at a compromised production server that is still powered on and actively processing transactions. Per RFC 3227 guidelines, which data source should be collected FIRST during live evidence acquisition?

A. Регистры процессора и кэш

B. Содержимое оперативной памяти (RAM)

C. ARP-кэш и таблицы маршрутизации

D. Временная файловая система и данные файла подкачки (swap)

---

20. В IT-отделе действует формальный процесс управления изменениями (change management). Какой шаг авторизации должен быть выполнен ДО внесения изменения в рабочие (production) системы?

An IT department follows a formal change management process. Which authorization step should occur BEFORE implementing a change to production systems?

A. Тестирование изменения в тестовой (non-production) среде

B. Одобрение комитета по изменениям (Change Advisory Board, CAB)

C. Документирование изменения в базе данных управления конфигурациями (CMDB)

D. Уведомление всех сторон, которых затрагивает изменение

Домен 4: безопасность сетей

21. Организация внедряет 802.1X для контроля доступа к сети. Какой компонент выступает посредником между клиентом (supplicant) и сервером аутентификации?

An organization implements 802.1X for network access control. Which component acts as the intermediary between the supplicant and the authentication server?

A. Центр сертификации (certificate authority)

B. Сетевой контроллер (network controller)

C. Аутентификатор (authenticator)

D. Прокси RADIUS (RADIUS proxy)

---

22. Организация внедряет WPA3-Enterprise для защиты беспроводной сети. Какую схему аутентификации использует WPA3-Enterprise?

An organization implements WPA3-Enterprise for wireless security. What authentication framework does WPA3-Enterprise use?

A. 802.1X с EAP
B. Фильтрация по MAC-адресам
C. Общий ключ (pre-shared key, PSK)
D. LEAP

---

23. Организации нужен безопасный удалённый доступ для выездных сотрудников, которые подключаются из разных стран при нестабильном интернете. Решение должно поддерживать трафик и TCP, и UDP и проходить через большинство межсетевых экранов. Какой протокол VPN НАИБОЛЕЕ подходит?

An organization needs to provide secure remote access for field personnel who connect from various international locations with unreliable internet connectivity. The solution must support both TCP and UDP traffic and work through most firewalls. Which VPN protocol is MOST appropriate?

A. PPTP
B. SSL/TLS VPN
C. L2TP/IPSec
D. IPSec в туннельном режиме

---

24. Веб-приложение компании сталкивается с наплывом трафика из многих источников, из-за чего сервер не справляется с ответами. Какая атака НАИБОЛЕЕ вероятна?

A company's web application experiences a surge in traffic from multiple sources, overwhelming the server's ability to respond. Which attack is MOST likely occurring?

A. Атака «человек посередине» (Man-in-the-Middle, MitM)
B. Межсайтовая подделка запроса (CSRF)
C. Перехват сессии (session hijacking)
D. Распределённая атака типа «отказ в обслуживании» (DDoS)

---

25. Какой уровень модели OSI отвечает за надёжную сквозную доставку данных, управление потоком и восстановление после ошибок между взаимодействующими узлами?

Which OSI model layer is responsible for end-to-end reliable data delivery, flow control, and error recovery between communicating hosts?

A. Уровень 2 (канальный, Data Link)
B. Уровень 4 (транспортный, Transport)
C. Уровень 3 (сетевой, Network)
D. Уровень 5 (сеансовый, Session)

---

26. Против веб-сервера организации идут атаки SYN flood. Какой метод защиты был бы НАИБОЛЕЕ эффективным?

An organization is experiencing SYN flood attacks against its web server. Which defensive technique would be MOST effective?

A. Отключение меток времени TCP (timestamps)
B. Фильтрация по MAC-адресам
C. Ограничение частоты ICMP-пакетов (rate limiting)
D. SYN cookies

---

27. При внедрении TLS для веб-приложения какую версию следует считать МИНИМАЛЬНО допустимой для новых развёртываний?

When implementing TLS for a web application, which version should be considered the MINIMUM acceptable standard for new deployments?

A. TLS 1.0
B. SSL 3.0
C. TLS 1.2
D. TLS 1.1

---

28. Финансовое учреждение требует взаимной аутентификации клиентов и серверов. Какая возможность TLS это обеспечивает?

A financial institution requires mutual authentication between clients and servers. Which TLS feature provides this capability?

A. Возобновление сеанса (session resumption)
B. Аутентификация по клиентскому сертификату (client certificate authentication)
C. Совершенная прямая секретность (PFS)
D. Указание имени сервера (SNI)

---

29. Система обнаружения вторжений (IDS) генерирует множество оповещений на нормальный трафик. Какая это ошибка?

An intrusion detection system (IDS) is generating numerous alerts for normal traffic patterns. What type of error is occurring?

A. Ложное срабатывание (false positive)
B. Ложный пропуск (false negative)
C. Истинно отрицательный результат (true negative)
D. Истинно положительный результат (true positive)

---

30. В многонациональной корпорации происходят сбои интернет-маршрутизации. Расследование показывает, что иностранный провайдер объявляет по BGP адресное пространство компании. Какая атака НАИБОЛЕЕ вероятна и в чём ОСНОВНОЕ отличие от отравления маршрутов (route poisoning)?

A multinational corporation experiences Internet routing disruptions. Investigation reveals that a foreign ISP is advertising the company's IP address space via BGP. Which attack is MOST likely occurring, and what is the PRIMARY difference from route poisoning?

A. Перехват BGP (BGP hijacking); он нацелен на принадлежность префикса, а не на метрики маршрутов
B. Отравление маршрутов; оно затрагивает внешнюю маршрутизацию, а не внутренние дистанционно-векторные протоколы
C. Колебание маршрутов (route flapping); оно вызывает периодические сбои, а не устойчивое перенаправление трафика
D. AS path prepending; оно манипулирует номерами автономных систем, чтобы влиять на решения о маршрутизации

Домен 2: безопасность активов

31. Базовый стандарт безопасности финансовой компании требует шифрования AES-256 для всех данных клиентов. Оценка рисков показывает, что некоторые устаревшие системы не поддерживают AES-256. Какой процесс должен применить архитектор безопасности для решения этой проблемы?

A financial services firm's baseline security standard requires AES-256 encryption for all customer data. A risk assessment reveals that certain legacy systems cannot support AES-256. What process should the security architect apply to address this constraint?

A. Адаптация (tailoring)
B. Компенсирующие меры (compensating controls)
C. Определение области применения (scoping)
D. Принятие риска (risk acceptance)

---

32. Согласно политике классификации правительства США, какая метка применяется к информации, несанкционированное раскрытие которой может, как разумно ожидать, нанести «серьёзный ущерб» (serious damage) национальной безопасности?

Under U.S. government classification policy, which label applies to information whose unauthorized disclosure could reasonably be expected to cause 'serious damage' to national security?

A. Secret (секретно)

B. Controlled Unclassified Information, CUI (контролируемая несекретная информация)

C. Confidential (конфиденциально)

D. Top Secret (совершенно секретно)

---

33. Кто в конечном итоге отвечает за определение уровня классификации данных в организации?

Who is ultimately responsible for determining the classification level of data within an organization?

A. Хранитель данных (data custodian)

B. Владелец данных (data owner)

C. Администратор безопасности (security administrator)

D. Директор по информационной безопасности (CISO)

---

34. Организация обязана хранить некоторую документацию по соответствию HIPAA не менее 6 лет по HIPAA и не менее 10 лет по применимому закону штата. Какой срок хранения этой документации должен рекомендовать менеджер по безопасности?

An organization must retain certain HIPAA compliance documentation for a minimum of 6 years under HIPAA and a minimum of 10 years under an applicable state law. What retention period should the security manager recommend for that documentation?

A. 8 лет как компромисс между требованиями

B. 10 лет, чтобы выполнить самое строгое требование

C. Бессрочное хранение, чтобы избежать рисков несоответствия

D. 6 лет в соответствии с федеральными требованиями HIPAA

---

35. Многонациональная корпорация хранит данные клиентов из ЕС в облачных центрах обработки данных. Французские клиенты опасаются, что организации вне ЕС смогут законным путём потребовать их данные. Какой принцип ЛУЧШЕ всего отвечает этой проблеме?

A multinational corporation stores EU customer data in cloud data centers. French customers are concerned about their data being legally compelled from non-EU entities. Which principle BEST addresses this concern?

A. Суверенитет данных (data sovereignty)

B. Локализация данных (data localization)

C. Географическая избыточность (geographic redundancy)

D. Резидентность данных (data residency)

---

36. Политика хранения данных организации требует хранить записи о транзакциях клиентов семь лет. Какой шаг процесса уничтожения данных должен быть ПЕРВЫМ по окончании этого срока?

An organization's data retention policy requires keeping customer transaction records for seven years. At the end of this period, what is the FIRST step in the disposal process?

A. Убедиться, что на данные не распространяется юридический запрет на уничтожение

B. Перезаписать данные инструментом, соответствующим DoD 5220.22-M

C. Физически уничтожить все носители с этими данными

D. Удалить все резервные копии из внешнего хранилища

---

37. Какая роль В ПЕРВУЮ ОЧЕРЕДЬ отвечает за определение уровня классификации информационного актива (data asset) организации?

Which role is PRIMARILY responsible for determining the classification level assigned to an organizational data asset?

A. Распорядитель данных (data steward)
B. Владелец данных (data owner)
C. Хранитель данных (data custodian)
D. Обработчик данных (data processor)

---

38. Медицинская организация списывает ноутбуки, на которых хранились незашифрованные медицинские карты пациентов. Какой метод очистки носителей (sanitization) даёт НАИВЫСШУЮ гарантию, что данные нельзя восстановить?

A healthcare organization is decommissioning laptops that stored unencrypted patient health records. Which sanitization method provides the HIGHEST assurance of data irrecoverability?

A. Физическое уничтожение (physical destruction) измельчением или сжиганием
B. Криптографическое стирание (cryptographic erasure) ключей шифрования
C. Семикратная перезапись (overwrite) случайными данными
D. Размагничивание (degaussing) устройством типа I или II

---

39. Организация классифицирует новую базу данных с оценками работы сотрудников, информацией о зарплатах и персональными данными (PII). Несанкционированное раскрытие может привести к потере конкурентного преимущества и юридической ответственности. Какой уровень классификации НАИБОЛЕЕ подходит?

An organization is classifying a new database containing employee performance reviews, salary information, and personally identifiable information (PII). The unauthorized disclosure could result in competitive disadvantage and potential legal liability. What classification level is MOST appropriate?

A. Secret (секретно)
B. Confidential (конфиденциально)
C. Internal Use Only (только для внутреннего использования)
D. Public (общедоступно)

---

40. Медицинская организация должна определить, кто отвечает за то, чтобы медицинские карты пациентов были правильно классифицированы, хранились в сроки, установленные регуляторами, и были доступны только уполномоченным сотрудникам. Кто несёт ОСНОВНУЮ ответственность за эти решения?

A healthcare organization must determine accountability for ensuring patient health records are properly classified, retained according to regulatory requirements, and accessible only to authorized personnel. Who has PRIMARY responsibility for these decisions?

A. Обработчик данных (data processor)
B. Директор по информационной безопасности (CISO)
C. Владелец данных (data owner)
D. Хранитель данных (data custodian)

Домен 1: безопасность и риски

41. Аналитик безопасности выяснил, что сотрудник открывал конфиденциальные файлы отдела кадров без делового обоснования. Должность сотрудника не требует доступа к кадровым данным. Какой принцип безопасности ВЕРОЯТНЕЕ ВСЕГО нарушен?

A security analyst discovers an employee has been accessing confidential HR files without business justification. The employee's role does not require access to HR data. Which security principle was MOST likely violated?

A. Принцип необходимого знания (need-to-know)
B. Эшелонированная защита (defense in depth)
C. Разделение обязанностей (separation of duties)
D. Принцип наименьших привилегий (least privilege)

---

42. Директор по информационной безопасности (CISO) хочет согласовать программу безопасности с целями бизнеса. Какая система (framework) ЛУЧШЕ всего подходит для этого?

An organization's CISO wants to align the security program with business objectives. Which framework is BEST suited for this purpose?

A. ISO 27002
B. COBIT
C. CIS Controls
D. NIST SP 800-53

---

43. Медицинская организация пострадала от атаки программы-вымогателя, зашифровавшей медицинские карты пациентов. CISO докладывает об инциденте совету директоров. Какую концепцию демонстрирует CISO?

A healthcare organization suffers a ransomware attack that encrypts patient records. The CISO reports the incident to the board. Which concept is the CISO demonstrating?

A. Должная осмотрительность (due diligence)
B. Разделение обязанностей (separation of duties)
C. Правило благоразумного человека (prudent man rule)
D. Должная забота (due care)

---

44. CISO объясняет совету директоров соотношение между планированием непрерывности бизнеса (BCP) и планированием аварийного восстановления (DRP). Какое утверждение НАИБОЛЕЕ верно?

A CISO is explaining the relationship between Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) to the executive board. Which statement is MOST accurate?

A. BCP касается только IT-систем и данных, а DRP охватывает все бизнес-операции
B. Термины BCP и DRP взаимозаменяемы и описывают один и тот же процесс планирования
C. DRP служит более широким стратегическим планом и включает BCP как часть
D. BCP служит более широким стратегическим планом, а DRP входит в него как тактическая часть о восстановлении IT

---

45. Во время учений по аварийному восстановлению выяснилось, что резервные ленты не читаются. Какой этап жизненного цикла BCP/DRP ВЕРОЯТНЕЕ ВСЕГО был упущен?

During a disaster recovery exercise, the backup tapes are found to be unreadable. Which phase of the BCP/DRP lifecycle was MOST likely neglected?

A. Оценка рисков (risk assessment)
B. Анализ влияния на бизнес (business impact analysis, BIA)
C. Разработка плана (plan development)
D. Тестирование и учения (testing and exercises)

---

46. Аналитик рисков определил, что файловый сервер может быть скомпрометирован программой-вымогателем с вероятностью 20% в год, а ожидаемый ущерб от одного инцидента составляет 50 000 долларов. Чему равна величина ожидаемых годовых потерь (Annualized Loss Expectancy, ALE)?

A risk analyst determines that a file server has a 20% annual probability of being compromised by ransomware, with an estimated loss of $50,000 per incident. What is the Annualized Loss Expectancy (ALE)?

A. 10 000 долларов
B. 50 000 долларов
C. 40 000 долларов
D. 250 000 долларов

---

47. Группа безопасности организации разрабатывает новую политику управления доступом. Какой тип документа должен быть НАИБОЛЕЕ строгим и содержать конкретные обязательные действия?

An organization's security team is developing a new access control policy. Which document type should be MOST restrictive and provide specific mandatory actions?

A. Процедура (procedure)
B. Стандарт (standard)
C. Руководство (guideline)
D. Политика (policy)

---

48. Компания внедряет принципы Privacy by Design («приватность по замыслу») для новой платформы данных о клиентах. Какой подход ЛУЧШЕ всего отражает этот принцип?

A company is implementing Privacy by Design principles for a new customer data platform. Which approach BEST demonstrates this principle?

A. Добавление шифрования и контроля доступа для защиты данных клиентов до ввода в эксплуатацию
B. Встраивание мер приватности в архитектуру системы с самого начала проектирования, включая минимизацию данных и настройки приватности по умолчанию
C. Обучение разработчиков требованиям приватности и проверка кода на соответствие этим требованиям
D. Проведение оценки влияния на приватность (PIA) после разработки системы для выявления и устранения рисков

---

49. Компания хочет передать финансовый риск, связанный с утечкой данных. Какая стратегия применяется?

A company wants to transfer financial risk associated with a data breach. Which strategy is being employed?

A. Снижение риска (risk mitigation)
B. Передача риска (risk transference)
C. Принятие риска (risk acceptance)
D. Избегание риска (risk avoidance)

---

50. При инциденте безопасности с несанкционированным доступом к финансовым системам какая роль В ПЕРВУЮ ОЧЕРЕДЬ отвечает за решение о том, уведомлять ли правоохранительные органы?

During a security incident involving unauthorized access to financial systems, which role is PRIMARILY responsible for determining whether law enforcement should be notified?

A. Руководитель группы реагирования на инциденты, поскольку у него самая свежая информация об инциденте
B. Директор по информационной безопасности (CISO), поскольку он отвечает за все вопросы безопасности
C. Высшее руководство или юрисконсульт, поскольку это деловое и юридическое решение с регуляторными последствиями
D. Ответственный за связь с правоохранительными органами, поскольку он поддерживает отношения с внешними органами

Правильный ответ

1. C Неотказуемость (non-repudiation) не даёт стороне отрицать своё действие и обычно обеспечивается цифровой подписью. Подпись создаётся закрытым ключом отправителя и проверяется его открытым ключом, поэтому она доказывает авторство. Аутентификация проверяет личность, но не даёт неоспоримого доказательства: при общем пароле нельзя понять, кто именно действовал. Конфиденциальность защищает от раскрытия, целостность от изменения, но ни то ни другое не доказывает, кто отправил данные.

2. A Модель Bell-LaPadula обеспечивает конфиденциальность: правило *-property запрещает запись вниз (no write down), а простое свойство безопасности (simple security property) запрещает чтение вверх (no read up). Так информация не утекает с высокого уровня на низкий. Biba и Clark-Wilson защищают целостность, а не конфиденциальность. Brewer-Nash (Chinese Wall) предотвращает конфликт интересов в коммерческой среде и не управляет доступом по уровням секретности.

3. A TLS с Diffie-Hellman позволяет двум сторонам выработать общий секрет по незащищённому каналу; так работает HTTPS. Эфемерный вариант (DHE/ECDHE) даёт совершенную прямую секретность (perfect forward secrecy). IPsec обычно применяют для VPN, он требует предварительной настройки и не подходит для произвольных клиентов. S/MIME шифрует почту. Kerberos рассчитан на корпоративную среду с заранее установленным доверием и центром KDC, поэтому для публичного магазина не годится.

4. D Правило двух лиц требует физического присутствия двух допущенных сотрудников, чтобы никто не мог действовать в одиночку. Тамбур-шлюз с двойной аутентификацией пропускает внутрь, только когда проверку прошли оба. Биометрия с PIN даёт многофакторную проверку, но одного человека. Видеонаблюдение только фиксирует вход и не мешает войти в одиночку. Кодовый замок откроет любой, кто знает код, а передача кода размывает персональную ответственность.

5. A Эшелонированная защита (её называют и многоуровневой) строится из нескольких независимых слоёв: если один слой отказал, остальные продолжают защищать. Например, вместе работают межсетевые экраны, IDS/IPS, управление доступом, шифрование и физические барьеры. Удаление лишних служб уменьшает поверхность атаки, и называется оно hardening. Минимальные права относятся к принципу наименьших привилегий (least privilege), а безопасное состояние при отказе называется fail-safe или fail-secure.

6. A Тамбур-шлюз (access control vestibule) относится к превентивным мерам: он не пропускает постороннего, потому что требует аутентификации у двух дверей подряд, и открыта может быть только одна из них. Так нельзя пройти следом за другим человеком (tailgating, piggybacking). Обнаруживающие меры выявляют уже случившееся (CCTV, датчики движения, журналы). Корректирующие исправляют ущерб (восстановление из копии, патчи). Компенсирующие заменяют основную меру, когда она недоступна.

7. C Biba обеспечивает целостность: запрет записи вверх (no write up) не даёт субъектам с низкой целостностью портить объекты с высокой, а запрет чтения вниз (no read down) не даёт надёжным субъектам читать ненадёжные данные. Bell-LaPadula отвечает за конфиденциальность. Chinese Wall предотвращает конфликт интересов. Graham-Denning описывает операции субъектов и объектов и на целостность не ориентирована. В условии главное не допустить чужих изменений, то есть сохранить целостность.

8. A Шифрование на стороне клиента с ключами в локальном HSM даёт независимость от провайдера, а депонирование через третью сторону закрывает требование регулятора. Шифрование отделено от контроля провайдера. Встроенная служба провайдера создаёт зависимость от него (vendor lock-in). При конвертном шифровании с ключами в облаке доступ к ключам всё равно привязан к провайдеру. TDE с ключами в конфигурации приложения плохо защищает ключи и не решает вопрос депонирования.

9. C Bell-LaPadula реализует мандатное управление доступом (MAC) ради конфиденциальности с помощью двух правил: simple security property (no read up) и *-property (no write down). Они не дают информации перетекать с высокого уровня на низкий, что и требуется. Biba защищает целостность, её правила зеркальны. Clark-Wilson обеспечивает целостность в коммерческих системах и не использует решётку уровней секретности. Brewer-Nash динамически ограничивает доступ из-за конфликта интересов.

10. B Датчики с автоматическими клапанами обнаруживают протечку, подают сигнал и сами перекрывают воду, поэтому ущерб минимален. Датчики работают как обнаруживающая мера, автоматическое перекрытие как корректирующая. Фальшпол помогает при затоплении снизу, но не защищает от воды сверху. Избыточное давление не пускает загрязнения снаружи и не связано с авариями водопровода. Контроль влажности HVAC не останавливает воду из лопнувшей трубы.

11. A Регулярное сравнение фактических конфигураций с утверждёнными базовыми (approved baselines) выявляет дрейф конфигурации (configuration drift) и помогает расследовать изменения, на которые не было разрешения. Автоматическое одобрение изменений от администраторов обходит согласование. Замена базовой конфигурации текущей превращает несанкционированные изменения в норму. Записи о закупках не показывают, что изменилось в настройках серверов.

12. C Сотрудник первичного реагирования (first responder) сталкивается с инцидентом первым: он выявляет его и сразу принимает меры по локализации, чтобы ущерб не рос. Координатор управляет всем процессом реагирования. Криминалист собирает и анализирует доказательства, включая энергозависимые данные, которые иногда нужно сохранить до локализации или во время неё. Ответственный за коммуникации сообщает об инциденте внутри и вне организации.

13. C К низкому уровню относят незначительные сбои некритичных систем без потери данных и без серьёзного влияния на бизнес. Критические инциденты затрагивают основные бизнес-процессы: крупные отказы систем или утечки данных. Высокий уровень присваивают, если пострадали важные, но не самые критичные системы или раскрыта ограниченная часть данных. Чрезвычайный означает прямую угрозу жизни, безопасности или критической инфраструктуре.

14. D Dwell time сокращает активное обнаружение, а не одни превентивные меры. Поведенческая аналитика и поиск угроз (threat hunting) находят аномалии, признаки компрометации. Сканирование уязвимостей находит слабые места, но не действующие угрозы. Обучение снижает риск взлома, но не выявляет действия после него. Новые межсетевые экраны относятся к превентивным мерам. Непрерывный мониторинг, UEBA и поиск угроз снижают среднее время обнаружения (MTTD) с месяцев до дней или часов.

15. A Эшелонированная защита строится слоями снаружи внутрь: периметр (ограждение, ворота, охрана), вход в здание (считыватели пропусков, стойка регистрации), внутренние помещения (доступ в серверную) и, наконец, защита самих активов (запертые шкафы, тросовые замки). Так у злоумышленника появляется несколько барьеров. В остальных вариантах порядок нарушен. Многоуровневый подход лежит в основе как физической, так и логической архитектуры безопасности.

16. A Вторичные доказательства включают копии, фотографии и воспроизведения оригинала; в суде их обычно ценят меньше, чем best evidence. Best evidence означает сам оригинал, документ или предмет. Подтверждающие доказательства поддерживают другие и не обязательно являются копией. Hearsay означает показания о том, что сказал кто-то другой, и суд их обычно не принимает.

17. C RTO (Recovery Time Objective) задаёт целевое время восстановления системы или процесса после сбоя, и 4 часа здесь типичный пример. RPO определяет допустимую потерю данных, измеренную во времени (например, не более 2 часов транзакций). MTD показывает, какой максимальный простой выдержит бизнес, и RTO должен укладываться в него с запасом. MTTR показывает среднее время ремонта и бизнес-требованием не является.

18. D RTO (4 часа) ограничивает простой, а RPO (1 час) ограничивает потерю данных. Непрерывная репликация может обеспечить RPO в 1 час, а подготовленная тёплая площадка может уложиться в RTO 4 часа, но это нужно подтвердить тестом восстановления. Копии раз в 6 часов и раз в 4 часа нарушают RPO, а хранение только на своей площадке создаёт единую точку отказа. Недельные и ежедневные копии допускают потерю до 24 часов данных.

19. A RFC 3227 приводит пример порядка волатильности (order of volatility): сначала регистры и кэш, затем группа, в которую входят таблицы маршрутизации, ARP-кэш, таблицы процессов, статистика ядра и память. Дальше идут временные файловые системы, диск, журналы и данные мониторинга с других систем, физическая конфигурация и топология сети, архивные носители. Поэтому первыми собирают регистры и кэш. RAM и ARP-кэш стоят в одной группе, и RFC 3227 не требует собирать RAM раньше сетевых таблиц.

20. B В описанном формальном процессе разрешение даёт CAB, и получить его нужно до внедрения: комитет оценивает риски и соответствие потребностям бизнеса. Тестирование и уведомление заинтересованных сторон обычно тоже проводят до внедрения, но разрешения они не дают. Запись в CMDB обновляют, чтобы отразить состояние после внедрения.

21. C В архитектуре 802.1X посредником служит аутентификатор (authenticator), обычно коммутатор или точка доступа Wi-Fi. Он пересылает запросы от клиента (supplicant) серверу аутентификации, как правило по RADIUS, и применяет его решение. Прокси RADIUS может стоять на пути, но в терминах 802.1X посредником не называется. Центр сертификации выдаёт сертификаты и в самой аутентификации не участвует. Сетевой контроллер не является стандартным компонентом 802.1X.

22. A WPA3-Enterprise использует 802.1X с протоколом EAP (Extensible Authentication Protocol) для аутентификации каждого пользователя на сервере RADIUS по индивидуальным учётным данным. Режим WPA3-Personal, напротив, использует SAE (Simultaneous Authentication of Equals). Общие ключи относятся к режиму Personal. Фильтрация по MAC слаба, так как адреса легко подделать. LEAP, устаревший собственный протокол Cisco с известными уязвимостями, в WPA3 не входит.

23. B SSL/TLS VPN подходит лучше всего: он работает через TCP-порт 443, который обычно проходит через межсетевые экраны и NAT. Туннельные реализации могут переносить и TCP-, и UDP-трафик приложений, а многие используют UDP-канал для скорости и переходят на TCP, если он недоступен. IPSec в туннельном режиме умеет обходить NAT, но строгие экраны могут его блокировать. L2TP/IPSec тоже зависит от разрешённого IPsec-трафика (UDP 500 и 4500). PPTP небезопасен из-за известных уязвимостей, а его GRE-трафик тоже упирается в экраны и NAT.

24. D DDoS использует множество распределённых источников, чтобы завалить цель трафиком, исчерпать ресурсы сервера и лишить легитимных пользователей доступа. Ключевые признаки: всплеск трафика из многих источников и исчерпание ресурсов. MitM перехватывает связь между двумя сторонами и не создаёт наплыва трафика. Перехват сессии захватывает аутентифицированный сеанс, но не вызывает всплесков. CSRF использует аутентифицированный сеанс для несанкционированных действий и не связан с перегрузкой.

25. B Транспортный уровень (уровень 4) обеспечивает сквозную связь между процессами отправителя и получателя. Надёжность даёт TCP: нумерация, подтверждения, повторная передача потерянных сегментов и управление потоком скользящим окном. UDP работает на том же уровне, но без соединения и гарантий. Канальный уровень доставляет между узлами одного сегмента по MAC-адресам, сетевой маршрутизирует по IP, а сеансовый управляет диалогом и синхронизацией, но не восстановлением после ошибок.

26. D SYN cookies позволяют серверу не выделять ресурсы при установлении TCP-соединения, пока оно не подтверждено, и тем самым устраняют уязвимость исчерпания состояний. Сервер кодирует данные соединения в порядковом номере, а не хранит полуоткрытое состояние. Ограничение ICMP относится к другому вектору атаки. Фильтрация по MAC работает на 2 уровне и бесполезна против атак 4 уровня из интернета. Отключение timestamps убирает функцию, но не защищает от исчерпания ресурсов.

27. C По стандартам NIST и PCI DSS минимально допустимая версия для новых развёртываний: TLS 1.2. Она даёт надёжные наборы шифров, обязательную поддержку SHA-256 и защиту от известных атак. TLS 1.0 и 1.1 признаны устаревшими из-за уязвимостей и слабых шифров. SSL 3.0 критически уязвим (атака POODLE) и не должен использоваться. TLS 1.3 лучше, но минимальной планкой остаётся TLS 1.2.

28. B Аутентификация по клиентскому сертификату требует, чтобы клиент предъявил сертификат X.509 при TLS-рукопожатии. Тогда аутентификация становится двусторонней: обе стороны проверяют друг друга. Обычный TLS аутентифицирует только сервер. SNI позволяет размещать несколько TLS-сайтов на одном IP и не влияет на направление аутентификации. Возобновление сеанса ускоряет повторные подключения. PFS защищает ключи прошлых сеансов при компрометации долговременного ключа, но взаимную аутентификацию не даёт.

29. A При ложном срабатывании (false positive) IDS ошибочно считает обычный трафик вредоносным и поднимает тревогу. Из-за этого аналитики тратят время и перестают реагировать на оповещения (alert fatigue). Ложный пропуск (false negative) означает обратное: вредоносный трафик не замечен. При true positive система верно нашла атаку, при true negative верно не подняла тревогу. Ложные срабатывания устраняют настройкой сигнатур, порогов или белых списков.

30. A При BGP hijacking чужая автономная система (AS) без права объявляет префиксы, которыми не владеет, и другие AS направляют трафик к злоумышленнику. Route poisoning служит законным приёмом сходимости в дистанционно-векторных протоколах вроде RIP: для отказавшего маршрута объявляют бесконечную метрику. AS path prepending тоже законно, так маршрут делают менее предпочтительным. Route flapping означает нестабильные объявления маршрутов, а не намеренное перенаправление.

31. A Tailoring адаптирует базовые меры защиты к ограничениям организации, особенностям систем и условиям работы. Именно это нужно, когда базовую меру нельзя выполнить буквально. Scoping определяет, к каким системам относится базовый набор, а не как приспособить нужную, но технически невыполнимую меру. Компенсирующие меры могут быть выбраны в ходе tailoring. Принятие риска требует санкции на остаточный риск и не заменяет выполнение применимых требований.

32. A Указ президента США (Executive Order 13526) делит секретную информацию о национальной безопасности на три уровня. Secret присваивают, если раскрытие может нанести «серьёзный ущерб» (serious damage). Top Secret: «исключительно тяжёлый ущерб» (exceptionally grave damage). Confidential: «ущерб», без слова «серьёзный». CUI не является уровнем секретности, это отдельная категория NARA для чувствительной, но несекретной информации. По возрастанию: Confidential, Secret, Top Secret.

33. B Владелец данных (обычно руководитель подразделения или топ-менеджер) отвечает за определение уровня классификации, потому что понимает ценность и чувствительность данных для бизнеса и принимает на себя связанный риск. Хранители реализуют технические меры, но уровни не устанавливают. Администраторы безопасности обеспечивают соблюдение политик, заданных другими. CISO задаёт общую структуру и политику классификации, но не классифицирует отдельные данные: это бизнес-решение владельцев.

34. B Срок 10 лет соответствует самому строгому требованию и покрывает оба минимальных срока. Требование штата не отменяет федеральное, и хранение 10 лет выполняет оба. Срок 6 лет нарушил бы закон штата. Компромисс в 8 лет не выполнил бы требование штата. Бессрочное хранение излишне, дорого и создаёт риски для конфиденциальности, потому что данные хранятся дольше необходимого.

35. A Суверенитет данных (data sovereignty) означает, что данные подчиняются законам и юрисдикции страны, где находятся, в том числе в вопросе, какие государства могут требовать доступ. Это прямо касается запросов властей вне ЕС (например, по U.S. CLOUD Act). Data residency говорит лишь о месте хранения: данные могут лежать во Франции, но быть доступны по закону США через материнскую компанию. Локализация служит инструментом суверенитета, а не самим принципом. Географическая избыточность относится к доступности.

36. A Перед уничтожением данных нужно убедиться, что их не обязывает хранить legal hold (юридический запрет на уничтожение), текущий судебный процесс, проверка регулятора или другое обязательство. Уничтожение таких данных грозит санкциями за уничтожение доказательств (spoliation) и обвинением в воспрепятствовании правосудию. Физическое уничтожение, перезапись и удаление копий допустимы, но только после этой проверки. Сначала право и соответствие требованиям, потом техника.

37. B Владелец данных, обычно руководитель подразделения или топ-менеджер, присваивает активу уровень классификации и периодически его пересматривает. Хранитель (часто IT-отдел или системный администратор) выполняет заданные владельцем меры: копии, списки доступа, шифрование. Распорядитель (data steward) следит за качеством и происхождением данных, а не за метками. Обработчик работает с данными по поручению и не влияет на классификацию. Владельцы решают, хранители исполняют.

38. A Физическое уничтожение даёт наивысшую гарантию: носитель полностью непригоден, данные не восстановить никаким способом. Криптографическое стирание работает, только если данные изначально были зашифрованы, а здесь шифрования не было. Семикратная перезапись эффективна, но данные теоретически могут остаться в служебных областях прошивки, плохих секторах и резервном пространстве, а на современных SSD она менее надёжна. Размагничивание действует на магнитные носители и бесполезно для SSD с памятью NAND.

39. B Confidential подходит для коммерческих данных, раскрытие которых нанесло бы организации серьёзный ущерб, включая вред конкурентным позициям и юридическую ответственность. Персональные данные, зарплаты и оценки работы явно соответствуют этому порогу. Internal Use Only слишком слабый уровень для таких последствий. Secret относится к государственной классификации и в бизнесе обычно не применяется. Public явно не подходит. Уровень Confidential требует строгого контроля доступа.

40. C Владелец данных (обычно руководитель или топ-менеджер) несёт основную ответственность за классификацию, сроки хранения и решения о доступе. Он отвечает за ценность данных для бизнеса и их защиту. Хранители реализуют технические меры по указаниям владельца и политику не определяют. Обработчики работают с данными по поручению контролёра и не принимают решений о классификации. CISO даёт рекомендации и управляет безопасностью, но конкретными данными не владеет: это функция бизнеса.

41. A Need-to-know означает, что доступ дают, только если он нужен для конкретной рабочей задачи, даже при подходящем уровне допуска. Технические права у сотрудника, возможно, были (система пустила), но рабочей необходимости не было. Least privilege близок, но говорит о минимальном объёме прав, а не об обоснованности доступа. Разделение обязанностей предотвращает мошенничество, а эшелонированная защита означает многоуровневую стратегию. Подсказка в условии: «без делового обоснования».

42. B COBIT (Control Objectives for Information and Related Technologies) создан, чтобы связать управление IT (IT governance) с целями бизнеса. ISO 27002 содержит свод практик по мерам защиты, технических и операционных. NIST SP 800-53 подробно описывает меры безопасности и приватности для федеральных систем, но не связь с целями бизнеса. CIS Controls дают список приоритетных тактических действий. Если вопрос о согласовании безопасности с целями бизнеса, думайте о COBIT: сначала управление, потом меры.

43. D Due care означает вовремя поступить правильно, то есть так, как поступил бы разумный человек. Доклад об инциденте совету директоров и, если требуется, регуляторам служит примером due care. Due diligence означает изучать риски и постоянно проверять, что меры и процессы остаются эффективными. Prudent man rule говорит об обязанности руководителей бережно защищать активы, но вопрос именно о действии CISO. Разделение обязанностей здесь ни при чём.

44. D BCP описывает, как сохранить все критичные функции бизнеса во время сбоя и после него: люди, процессы, помещения, цепочки поставок, связь, технологии. DRP охватывает меньше и работает на тактическом уровне: в нём описаны процедуры восстановления IT-систем, данных и инфраструктуры после аварии. DRP входит в BCP, а не наоборот. Планы дополняют друг друга, но не взаимозаменяемы. Мыслите как менеджер: BCP относится к стратегии бизнеса, DRP служит технической инструкцией по восстановлению.

45. D Регулярные тесты и учения проверяют, что процедуры восстановления работают, в том числе целостность резервных копий. Если ленты нечитаемы во время учений, значит, тестирования было недостаточно или не было вовсе. BIA определяет критичные системы и RTO, но не проверяет носители. Оценка рисков выявляет угрозы и уязвимости и не тестирует меры. Разработка плана создаёт документированные процедуры, но без тестов неизвестно, работают ли они. Иметь план недостаточно, его нужно тестировать.

46. A ALE = SLE × ARO. SLE (Single Loss Expectancy, потери от одного случая) = 50 000 долларов. ARO (Annualized Rate of Occurrence, ожидаемая частота за год) = 0.20 (20%). ALE = 50 000 × 0,20 = 10 000 долларов. Сумма 50 000 равна только SLE, без учёта частоты. 250 000 получится, если ошибочно умножить 50 000 на 5. 40 000 из условия не следует. ALE сравнивают с ценой защиты: если мера стоит больше предотвращённых потерь, она может быть невыгодна.

47. B Стандарт (standard) задаёт конкретные обязательные настройки и требования, например «все пароли не короче 12 символов». Политика (policy) выражает намерения руководства на высоком уровне и менее конкретна. Процедура (procedure) описывает пошаговые действия и тоже может быть обязательной. Руководство (guideline) содержит рекомендации, а не обязательные требования. Стандарт подходит лучше всего, потому что устанавливает обязательные требования, а процедура описывает шаги их выполнения.

48. B Privacy by Design требует встраивать приватность в архитектуру с самого начала, включая минимизацию данных (собирать только необходимое) и privacy by default (самые защищённые настройки по умолчанию). Оценка влияния на приватность после разработки запаздывает. Шифрование и контроль доступа перед запуском решают задачу безопасности, но не сокращают сбор данных и не встраивают приватность во всю систему. Обучение разработчиков полезно, но не гарантирует приватности на уровне архитектуры.

49. B Передача риска (risk transference) переносит финансовые последствия на другую сторону, обычно через страхование (полис киберстрахования) или договор (SLA облачного провайдера со штрафами). Это не избегание (отказ от деятельности, создающей риск), не снижение (внедрение мер для уменьшения вероятности или ущерба) и не принятие (осознанное признание риска без действий). Передача не устраняет риск, а переносит финансовое бремя. Примеры: страхование, гарантии, аутсорсинг с положениями об ответственности.

50. C Обращение в правоохранительные органы затрагивает бизнес и право: обязательства перед регуляторами, риск судебных споров, публичность, репутацию. Поэтому его одобряет высшее руководство или юрисконсульт. Группа реагирования даёт технические данные, но стратегических решений не принимает. CISO консультирует по безопасности, но для такого решения нужны полномочия руководства. Ответственный за связь лишь налаживает контакт. Технические команды эскалируют, руководители решают.

Ключевые английские слова

Due care	Должная забота	Разумные действия для защиты, как поступил бы осмотрительный человек.
Due diligence	Должная осмотрительность	Изучение рисков и постоянная проверка, работают ли меры защиты.
Risk owner	Владелец риска	Тот, кто отвечает за риск и может решить, что с ним делать.

Risk acceptance	Принятие риска	Осознанно оставить риск как есть и записать это решение.
Risk transference	Передача риска	Перенести финансовые потери на страховщика или другую сторону.
Risk avoidance	Избегание риска	Прекратить деятельность, которая создаёт риск.
Risk mitigation	Снижение риска	Уменьшить вероятность или ущерб с помощью мер защиты.
Residual risk	Остаточный риск	Риск, который остаётся после внедрения мер защиты.
Single Loss Expectancy (SLE)	Ожидаемые потери от одного случая	Сколько денег теряют при одном инциденте.
Annualized Rate of Occurrence (ARO)	Ожидаемая частота за год	Сколько раз в год ожидают инцидент; 20% записывают как 0,20.
Annualized Loss Expectancy (ALE)	Ожидаемые годовые потери	SLE, умноженная на ARO; с ней сравнивают цену защиты.
Business Continuity Planning (BCP)	Планирование непрерывности бизнеса	Как сохранить важные функции бизнеса во время и после сбоя.
Disaster Recovery Planning (DRP)	Планирование аварийного восстановления	Как восстановить IT-системы и данные; входит в BCP.
Business impact analysis (BIA)	Анализ влияния на бизнес	Определяет важнейшие системы и срок их восстановления.
Recovery Time Objective (RTO)	Целевое время восстановления	За какое время нужно восстановить систему после сбоя.
Recovery Point Objective (RPO)	Целевая точка восстановления	Допустимая потеря данных, измеренная во времени.
Maximum Tolerable Downtime (MTD)	Максимально допустимый простой	Предел простоя, после которого ущерб для бизнеса неприемлем.
Mean Time to Detect (MTTD)	Среднее время обнаружения	Сколько в среднем проходит до обнаружения инцидента.
Dwell time	Время скрытого присутствия	Сколько злоумышленник находится в системе до обнаружения.
Need-to-know	Принцип необходимого знания	Доступ только при рабочей необходимости, даже если допуск есть.
Least privilege	Принцип наименьших привилегий	Только те права, без которых работу не выполнить.
Separation of duties	Разделение обязанностей	Задачу делят между людьми, чтобы предотвратить мошенничество.
Defense in depth	Эшелонированная защита	Несколько независимых слоёв защиты вместо одного.

Data owner	Владелец данных	Руководитель, который определяет классификацию и доступ к данным.
Data custodian	Хранитель данных	Выполняет меры, заданные владельцем: копии, доступ, шифрование.
Tailoring	Адаптация мер	Приспособление базовых мер защиты к условиям конкретной системы.
Scoping	Определение области применения	Выбор систем, к которым относится базовый набор мер.
Legal hold	Запрет на уничтожение данных	Обязанность хранить данные из-за суда, проверки или расследования.
Data sovereignty	Суверенитет данных	Данные подчиняются законам страны, где находятся.
Sanitization	Очистка носителя	Удаление данных так, чтобы их нельзя было восстановить.
Non-repudiation	Неотказуемость	Отправитель не может отрицать, что совершил действие.
Key escrow	Депонирование ключей	Хранение копии ключей у доверенной третьей стороны.
Preventive control	Превентивная мера	Не даёт инциденту произойти, например mantrap.
Detective control	Обнаруживающая мера	Выявляет инцидент: видеонаблюдение, датчики, журналы.
Corrective control	Корректирующая мера	Устраняет ущерб после инцидента, например восстановление из копии.
Compensating control	Компенсирующая мера	Заменяет основную меру, когда применить её нельзя.
Order of volatility	Порядок волатильности	Доказательства собирают от самых недолговечных к самым стойким.
Change Advisory Board (CAB)	Комитет по изменениям	Оценивает и разрешает изменения до их внедрения.
Mutual authentication	Взаимная аутентификация	Клиент и сервер проверяют друг друга.
False positive	Ложное срабатывание	Система подняла тревогу из-за нормальной активности.

Сайт Examundo независим. Он не связан с организациями, которые проводят эти экзамены, и не одобрен ими. Вопросы оригинальные, они не взяты из настоящих экзаменов. examundo.tech/ru/cissp/