

1. **K каком классу угроз относится несанкционированный доступ к информации?**

("Việc truy cập thông tin trái phép thuộc loại mối đe dọa nào?")

1. Угрозы конфиденциальности. (Mối đe dọa đến tính bảo mật.) ✓
  2. Угрозы целостности. (Mối đe dọa đến tính toàn vẹn.)
  3. Физической безопасности. (An toàn vật lý.)
  4. Аппаратным угрозам. (Mối đe dọa phần cứng.)
- 

2. **Что такое конфиденциальность информации?**

("Bảo mật thông tin là gì?")

1. Защита информации от всех пользователей. (Bảo vệ thông tin khỏi tất cả người dùng.)
2. Обеспечение доступа к информации только для уполномоченных лиц. (Đảm bảo chỉ những người được ủy quyền mới có quyền truy cập thông tin.) ✓
3. Ограничение доступа к любым данным, включая общедоступную информацию. (Hạn chế truy cập vào mọi dữ liệu, bao gồm cả thông tin công khai.)
4. Полное исключение возможности копирования данных. (Loại bỏ hoàn toàn khả năng sao chép dữ liệu.)

3. **Что является основным инструментом защиты от спама на почтовых серверах?**

("Công cụ chính để bảo vệ khỏi thư rác trên máy chủ thư là gì?")

1. Использование общего антивируса. (Sử dụng phần mềm diệt virus chung.)
  2. Полная блокировка всех внешних писем. (Chặn hoàn toàn tất cả thư từ bên ngoài.)
  3. Шифрование всех писем. (Mã hóa tất cả thư.)
  4. Фильтры спама, основанные на анализе содержимого сообщений. (Bộ lọc thư rác dựa trên phân tích nội dung tin nhắn.) ✓
- 

4. **Как называется процесс восстановления данных после кибератаки или технического сбоя?**

("Quá trình khôi phục dữ liệu sau một cuộc tấn công mạng hoặc lỗi kỹ thuật được gọi là gì?")

1. Удаление зараженных данных. (Xóa dữ liệu bị nhiễm.)
  2. **Резервное копирование и восстановление.** (Sao lưu và khôi phục.) ✓
  3. Контроль доступа. (Kiểm soát truy cập.)
  4. Обновление программного обеспечения. (Cập nhật phần mềm.)
- 

5. **Какую цель преследует шифрование данных?**

("Mục đích của việc mã hóa dữ liệu là gì?")

1. Скрытие размера файлов. (Che giấu kích thước tệp.)
  2. **Преобразование данных таким образом, чтобы они были недоступны без ключа шифрования.** (Chuyển đổi dữ liệu để chúng không thể truy cập nếu không có khóa giải mã.) ☒
  3. Полное удаление данных с устройства. (Xóa hoàn toàn dữ liệu khỏi thiết bị.)
  4. Ограничение доступа конкретным пользователям. (Hạn chế quyền truy cập đối với người dùng cụ thể.)
- 

**6. Что НЕ является основным фактором в организации физической безопасности?**

(Dịch: "Yếu tố nào KHÔNG phải là yếu tố chính trong việc tổ chức an ninh vật lý?")

Các đáp án:

1. Ограничение доступа к серверным помещениям. (Hạn chế truy cập vào phòng máy chủ.)
  2. Установка видеонаблюдения и сигнализации. (Lắp đặt hệ thống giám sát video và báo động.)
  3. Регистрация доступа сотрудников в помещение. (Ghi nhận quyền truy cập của nhân viên vào phòng.)
  4. **Наличие фаерволов и антивирусов.** (Sự hiện diện của tường lửa và phần mềm diệt virus.) ☒
- 

**7. Какую роль выполняет антивирусное программное обеспечение?**

("Phần mềm diệt virus thực hiện vai trò gì?")

1. Контролирует доступ к интернет-ресурсам. (Kiểm soát quyền truy cập vào tài nguyên Internet.)
  2. Выполняет резервное копирование всех данных. (Thực hiện sao lưu tất cả dữ liệu.)
  3. **Обнаруживает и нейтрализует вредоносные программы на устройстве.** (Phát hiện và vô hiệu hóa các phần mềm độc hại trên thiết bị.) ☒
  4. Шифрует данные для предотвращения утечек. (Mã hóa dữ liệu để ngăn chặn rò rỉ.)
- 


**8. Какой протокол рекомендуется использовать для безопасного соединения с веб-сайтом?**

("Giao thức nào được khuyến nghị sử dụng để kết nối an toàn với trang web?")

1. FTP
2. SMTP
3. HTTP
4. **HTTPS** ☒


---

9. **Что нужно сделать, прежде чем выдать доступ сотруднику к важной системе?**  
( "Cần làm gì trước khi cấp quyền truy cập cho nhân viên vào hệ thống quan trọng?" )

1. Выдать полный административный доступ для удобства. Изолировать доступ сотрудника к другой информации компании. (Cấp quyền quản trị đầy đủ để thuận tiện. Cô lập quyền truy cập của nhân viên vào thông tin khác của công ty.)
2. **Определить его уровень доступа в зависимости от рабочих задач.** (Xác định mức độ truy cập của nhân viên tùy theo nhiệm vụ công việc.) 
3. Настроить антивирусное ПО на его устройстве. Выдать полный административный доступ для удобства. (Cài đặt phần mềm diệt virus trên thiết bị của nhân viên. Cấp quyền quản trị đầy đủ để thuận tiện.)
4. Изолировать доступ сотрудника к другой информации компании. Настроить антивирусное ПО на его устройстве. (Cô lập quyền truy cập của nhân viên vào thông tin khác của công ty. Cài đặt phần mềm diệt virus trên thiết bị của họ.)

---

10. **Какую угрозу могут представлять слабые пароли?**  
( "Mật khẩu yếu có thể gây ra mối đe dọa nào?" )

1. Повышают шансы на заражение вирусами. (Tăng khả năng bị nhiễm virus.)
2. Упрощают резервное копирование данных. (Làm cho việc sao lưu dữ liệu dễ dàng hơn.)
3. **Упрощают несанкционированный доступ злоумышленникам.** (Tạo điều kiện cho kẻ xấu truy cập trái phép.) 
4. Не оказывают никакого воздействия на безопасность. (Không ảnh hưởng gì đến bảo mật.)