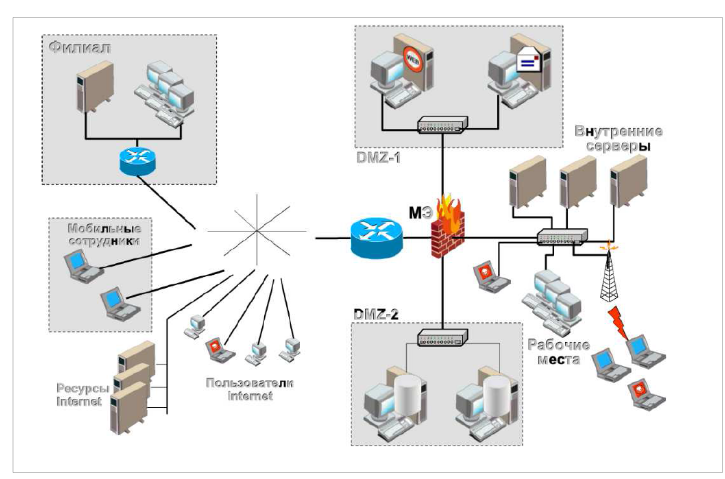
# **Mạng tính toán và kiểm soát an ninh trong mạng máy tính**

# 🔹 **Chủ đề 1. Giới thiệu về an ninh hệ thống máy tính. Các khái niệm cơ bản.**

## **Mạng IP điển hình của tổ chức**



Mạng IP của một tổ chức được thiết kế để **đảm bảo kết nối giữa các bộ phận**, đồng thời **bảo vệ dữ liệu và hệ thống khỏi các mối đe dọa từ bên ngoài**. Sơ đồ này thể hiện cách tổ chức **phân chia mạng, quản lý lưu lượng dữ liệu và bảo vệ thông tin**.

## **1️⃣ Các khu vực chính trong mạng tổ chức**

### **🔹 Mạng nội bộ (Internal Network)**

* Là **phần quan trọng nhất**, nơi nhân viên làm việc và sử dụng các hệ thống nội bộ.
* Gồm các **máy chủ nội bộ, máy tính cá nhân (workstations), thiết bị mạng**.
* **Chỉ nhân viên trong công ty có quyền truy cập**.
* Được bảo vệ bởi **tường lửa (firewall)** để ngăn truy cập trái phép từ bên ngoài.

📌 **Thiết bị chính:** ✅ **Máy tính làm việc** - Рабочие места (Workstations) của nhân viên.  
 ✅ **Máy chủ nội bộ** - Внутренние серверы (Internal Servers) chứa dữ liệu quan trọng.

### **🔹 DMZ (De-Militarized Zone - Vùng phi quân sự)**

* **Là khu vực chứa các dịch vụ công khai** mà khách hàng hoặc đối tác có thể truy cập từ Internet.
* Các máy chủ trong **DMZ có thể được truy cập từ bên ngoài**, nhưng vẫn **tách biệt với mạng nội bộ**.

📌 **Ví dụ về hệ thống trong DMZ:** ✅ **Web server** (chạy website công ty).  
 ✅ **Mail server** (máy chủ email).  
 ✅ **VPN server** (cho phép nhân viên kết nối từ xa).

💡 **Mục đích:**

* Ngăn chặn hacker tấn công trực tiếp vào hệ thống nội bộ.
* Nếu có xâm nhập, thiệt hại chỉ giới hạn trong DMZ, không ảnh hưởng đến toàn bộ hệ thống.

### **🔹 Tường lửa (Firewall) - МЭ - Межсетевой экран**

* **Bảo vệ mạng bằng cách kiểm soát lưu lượng dữ liệu vào/ra**.
* Chặn truy cập trái phép từ Internet.
* Kiểm soát lưu lượng giữa **DMZ và mạng nội bộ**.
* Phát hiện và ngăn chặn **các cuộc tấn công mạng**.

📌 **Chức năng chính:** ✅ **Ngăn chặn hacker xâm nhập** vào hệ thống nội bộ.  
 ✅ **Giám sát và kiểm soát truy cập mạng** của người dùng.  
 ✅ **Lọc gói tin độc hại** trước khi đến hệ thống nội bộ.

### **🔹 Chi nhánh (Branch Office) - Филиал**

* Nếu tổ chức có nhiều **chi nhánh**, chúng cần kết nối với **trụ sở chính** qua **VPN hoặc mạng riêng**.
* Dữ liệu truyền qua chi nhánh được **mã hóa** để bảo mật thông tin.

📌 **Lợi ích:** ✅ **Nhân viên ở chi nhánh có thể truy cập hệ thống công ty** một cách an toàn.  
 ✅ **Bảo vệ dữ liệu** khỏi nguy cơ rò rỉ khi truyền qua mạng.

### **🔹 Người dùng bên ngoài (Internet Users) - Мобильные сотрудники**

* Người bên ngoài chỉ có thể truy cập **các dịch vụ công khai** như website, email.
* Họ không thể truy cập trực tiếp vào mạng nội bộ của tổ chức.

📌 **Ví dụ:** ✅ **Khách hàng truy cập website công ty** để xem thông tin sản phẩm.  
 ✅ **Đối tác truy cập email server** để gửi/nhận email.

### **🔹 Nhân viên làm việc từ xa (Remote Employees)**

* Nhân viên có thể làm việc từ xa bằng **laptop, điện thoại**.
* Họ sử dụng **VPN (Mạng riêng ảo)** để kết nối an toàn với hệ thống công ty.

📌 **Bảo mật kết nối từ xa:** ✅ **Xác thực 2 lớp (2FA)** để đảm bảo đúng người truy cập.  
 ✅ **Mã hóa dữ liệu VPN** để tránh bị đánh cắp thông tin.

## **2️⃣ Cách hoạt động của mạng tổ chức**

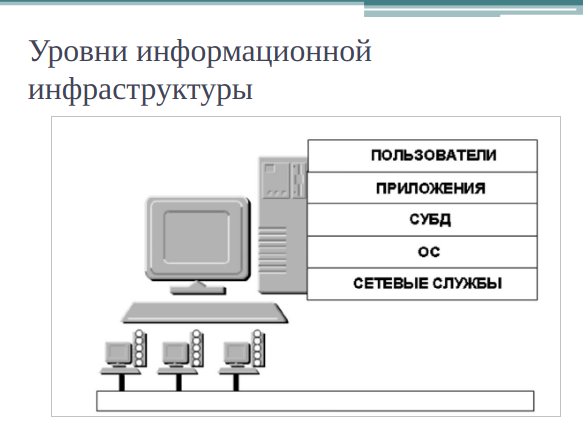
1️⃣ **Người dùng bên ngoài** truy cập **các dịch vụ trong DMZ**, nhưng **không thể vào mạng nội bộ**.  
 2️⃣ **Nhân viên từ xa** sử dụng **VPN** để **kết nối an toàn** vào hệ thống công ty.  
 3️⃣ **Tường lửa bảo vệ** hệ thống khỏi các mối đe dọa từ Internet.  
 4️⃣ **Các chi nhánh kết nối với trụ sở chính** qua **mạng riêng hoặc VPN**.  
 5️⃣ **Máy chủ nội bộ** lưu trữ thông tin quan trọng, **không thể truy cập từ bên ngoài**.

## **3️⃣ Kết luận**

* **Mạng tổ chức được thiết kế với nhiều lớp bảo vệ** để đảm bảo an toàn dữ liệu.
* **DMZ giúp cách ly các hệ thống công khai**, ngăn chặn tấn công vào mạng nội bộ.
* **Tường lửa kiểm soát và giám sát toàn bộ lưu lượng mạng** để bảo vệ hệ thống.
* **Nhân viên làm việc từ xa cần sử dụng VPN** để kết nối an toàn với công ty.

## **"Уровни информационной инфраструктуры" (Các cấp độ của hạ tầng thông tin)**

Hình ảnh mô tả **các cấp độ (layers) của một hệ thống hạ tầng thông tin**. Đây là mô hình thể hiện cách các thành phần trong hệ thống **tương tác và phụ thuộc lẫn nhau** để đảm bảo hoạt động của **mạng và hệ thống CNTT** trong tổ chức.



## **1️⃣ Giải thích từng cấp độ**

Hệ thống được chia thành **5 cấp độ**, từ **cơ sở hạ tầng mạng** đến **người dùng cuối**, theo thứ tự từ dưới lên trên:

### **🔹 1. Сетевые службы (Dịch vụ mạng)**

* Đây là **lớp cơ sở hạ tầng**, đóng vai trò nền tảng để kết nối hệ thống.
* Gồm các thành phần như:  
   ✅ **Mạng LAN/WAN** – Hệ thống kết nối giữa các máy tính.  
   ✅ **Máy chủ mạng (Network Servers)** – Quản lý truy cập, tài nguyên.  
   ✅ **Router, switch, firewall** – Điều phối luồng dữ liệu, bảo vệ mạng.  
   ✅ **Giao thức mạng (TCP/IP, DNS, DHCP)** – Hỗ trợ truyền tải dữ liệu.

💡 **Ý nghĩa:**

* Nếu không có **dịch vụ mạng**, hệ thống sẽ không thể hoạt động hoặc giao tiếp được.

### **🔹 2. ОС (Hệ điều hành – Operating System)**

* Cấp độ này bao gồm các **hệ điều hành máy chủ và máy trạm**.
* Hệ điều hành giúp **quản lý tài nguyên phần cứng và phần mềm**, đảm bảo các ứng dụng có thể chạy được.

📌 **Ví dụ:** ✅ **Windows Server, Linux, macOS** – Dùng cho máy chủ.  
 ✅ **Windows 10/11, Ubuntu, macOS** – Dùng cho người dùng cuối.

💡 **Ý nghĩa:**

* Hệ điều hành đóng vai trò **cầu nối giữa phần cứng và phần mềm ứng dụng**.
* Nếu hệ điều hành có lỗi, toàn bộ hệ thống sẽ bị ảnh hưởng.

### **🔹 3. СУБД (Hệ quản trị cơ sở dữ liệu – Database Management System - DBMS)**

* Đây là **lớp lưu trữ và quản lý dữ liệu** trong hệ thống.
* Các hệ thống thông tin hiện đại đều cần **CSDL để lưu trữ, truy xuất và xử lý dữ liệu**.

📌 **Ví dụ về hệ quản trị CSDL:** ✅ **MySQL, PostgreSQL, Microsoft SQL Server, Oracle Database**.  
 ✅ **MongoDB, Firebase** – CSDL NoSQL.

💡 **Ý nghĩa:**

* Hệ thống cần **DBMS để xử lý dữ liệu**, nếu lỗi xảy ra, toàn bộ dữ liệu có thể bị mất hoặc không thể truy xuất.

**🔹 4. Приложения (Ứng dụng – Applications)**

* Đây là **lớp phần mềm ứng dụng**, nơi người dùng tương tác với hệ thống.
* Các ứng dụng này **sử dụng dữ liệu từ CSDL và được chạy trên hệ điều hành**.

📌 **Ví dụ:** ✅ **Phần mềm quản lý doanh nghiệp (ERP, CRM, HRM, kế toán)**.  
 ✅ **Ứng dụng web, ứng dụng di động, trình duyệt web**.  
 ✅ **Phần mềm văn phòng (Microsoft Office, Google Docs, v.v.)**.

💡 **Ý nghĩa:**

* Nếu không có **ứng dụng**, người dùng không thể thực hiện các tác vụ cụ thể.

### **🔹 5. Пользователи (Người dùng – Users)**

* Đây là **cấp độ cao nhất**, nơi con người trực tiếp sử dụng hệ thống.
* Người dùng có thể là **nhân viên, quản trị viên, khách hàng, đối tác, v.v.**.

📌 **Ví dụ:** ✅ **Nhân viên nhập dữ liệu vào hệ thống quản lý**.  
 ✅ **Khách hàng sử dụng website để đặt hàng**.  
 ✅ **Quản trị viên giám sát và vận hành hệ thống**.

💡 **Ý nghĩa:**

* **Người dùng là mục tiêu chính của hệ thống**, nếu hệ thống không thân thiện, khó sử dụng thì hiệu quả sẽ giảm.

## **2️⃣ Mối quan hệ giữa các cấp độ**

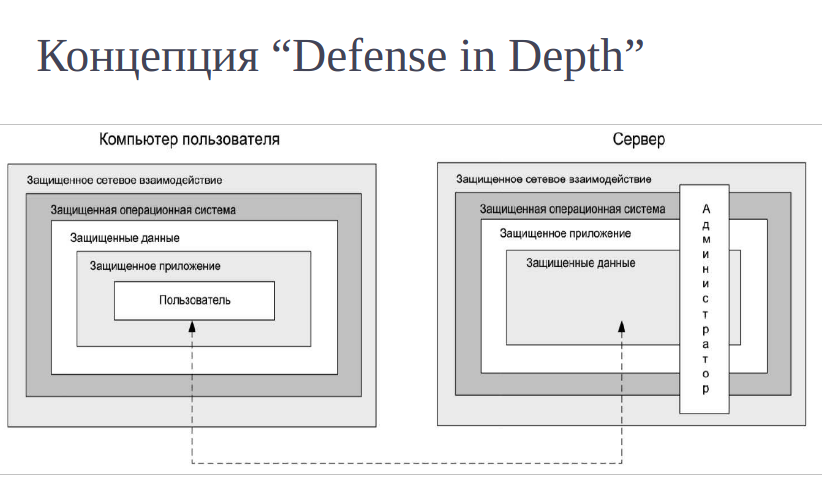
* **Dịch vụ mạng** cung cấp nền tảng kết nối để **hệ điều hành** hoạt động.
* **Hệ điều hành** hỗ trợ chạy **các hệ quản trị cơ sở dữ liệu (DBMS)**.
* **DBMS** lưu trữ dữ liệu cho **các ứng dụng**.
* **Ứng dụng** cung cấp giao diện để **người dùng** thao tác.

💡 **Nếu một cấp độ gặp lỗi, tất cả cấp độ trên nó đều bị ảnh hưởng!**

## **3️⃣ Kết luận**

* Hạ tầng thông tin **gồm nhiều lớp**, mỗi lớp **đóng vai trò quan trọng** để hệ thống hoạt động trơn tru.
* **Lớp thấp nhất (dịch vụ mạng)** là nền tảng cho các lớp trên.
* **Lớp cao nhất (người dùng)** là mục tiêu chính của hệ thống, nơi con người trực tiếp tương tác.
* **Bảo mật và quản lý tốt từng lớp sẽ giúp hệ thống ổn định, hiệu quả và an toàn hơn!**

## **Концепция "Defense in Depth" (Khái niệm "Phòng thủ theo chiều sâu")**



Hình ảnh minh họa khái niệm **"Defense in Depth"** – một chiến lược **bảo mật đa lớp** để bảo vệ hệ thống CNTT trước các mối đe dọa từ bên ngoài.

Mô hình này được áp dụng cho **cả máy tính người dùng (Копьютер пользователя) và máy chủ (Сервер)**, với nhiều lớp bảo vệ khác nhau.

## **1️⃣ Giải thích từng lớp bảo vệ**

### **🔹 Lớp ngoài cùng: "Защищенное сетевое взаимодействие" (Bảo mật kết nối mạng)**

* Đây là **tuyến phòng thủ đầu tiên**, đảm bảo kết nối giữa **máy người dùng và máy chủ** là **an toàn**.
* Sử dụng các phương pháp bảo vệ như:  
   ✅ **Tường lửa (Firewall)** – Lọc gói tin, chặn lưu lượng nguy hiểm.  
   ✅ **VPN, SSL/TLS** – Mã hóa dữ liệu khi truyền qua mạng.  
   ✅ **IDS/IPS (Hệ thống phát hiện/ngăn chặn xâm nhập)** – Giám sát và cảnh báo về các cuộc tấn công mạng.

💡 **Mục tiêu:**

* Ngăn chặn các **cuộc tấn công từ xa** (DDoS, Man-in-the-Middle).
* Bảo vệ **tính toàn vẹn và bảo mật dữ liệu khi truyền trên mạng**.

### **🔹 Lớp thứ hai: "Защищенная операционная система" (Hệ điều hành được bảo vệ)**

* Hệ điều hành là mục tiêu phổ biến của hacker, do đó cần có **các biện pháp bảo mật mạnh mẽ**.

📌 **Các biện pháp bảo vệ:** ✅ **Cập nhật hệ điều hành thường xuyên** để vá lỗ hổng.  
 ✅ **Cấu hình quyền truy cập hợp lý (Least Privilege Access)**.  
 ✅ **Sử dụng phần mềm diệt virus, HIPS (Host Intrusion Prevention System)**.  
 ✅ **Bật tường lửa hệ thống (Windows Defender Firewall, iptables trên Linux)**.

💡 **Mục tiêu:**

* Ngăn chặn **malware, ransomware, backdoor** từ hacker.
* Bảo vệ **quyền truy cập và tính ổn định của hệ điều hành**.

### **🔹 Lớp thứ ba: "Защищенные данные" (Dữ liệu được bảo vệ)**

* Dữ liệu là tài sản quan trọng nhất trong hệ thống CNTT, cần được bảo vệ khỏi:
  + **Mất mát dữ liệu (Data Loss)**.
  + **Rò rỉ thông tin nhạy cảm (Data Leakage)**.
  + **Tấn công mã hóa dữ liệu (Ransomware, SQL Injection, v.v.)**.

📌 **Các biện pháp bảo vệ:** ✅ **Mã hóa dữ liệu (AES, RSA, BitLocker, VeraCrypt, v.v.)**.  
 ✅ **Phân quyền chặt chẽ, hạn chế quyền truy cập không cần thiết**.  
 ✅ **Sao lưu dữ liệu thường xuyên (Backup & Disaster Recovery Plan)**.  
 ✅ **Hệ thống phát hiện truy cập bất thường (DLP – Data Loss Prevention)**.

💡 **Mục tiêu:**

* Ngăn chặn truy cập trái phép, bảo vệ dữ liệu trong mọi tình huống.

### **🔹 Lớp trong cùng (Người dùng và quản trị viên)**

* **Máy tính người dùng (Копьютер пользователя):**
  + Người dùng là yếu tố **dễ bị tổn thương nhất** trong hệ thống bảo mật.
  + Các **cuộc tấn công lừa đảo (phishing), social engineering** thường nhắm vào người dùng.
  + **Huấn luyện bảo mật** là điều bắt buộc.

📌 **Cách bảo vệ:** ✅ **Huấn luyện nhận diện email giả mạo, liên kết độc hại**.  
 ✅ **Không sử dụng mật khẩu yếu, bật xác thực hai yếu tố (2FA)**.  
 ✅ **Chỉ tải phần mềm từ nguồn đáng tin cậy**.

* **Máy chủ (Сервер):**
  + Máy chủ thường được quản lý bởi **quản trị viên (администратор)**.
  + Hacker **luôn tìm cách tấn công tài khoản quản trị viên** để kiểm soát toàn bộ hệ thống.

📌 **Cách bảo vệ:** ✅ **Sử dụng tài khoản quản trị riêng biệt, không dùng chung với tài khoản thông thường**.  
 ✅ **Giới hạn quyền truy cập từ xa (Remote Access)**.  
 ✅ **Giám sát hoạt động đăng nhập bất thường**.

💡 **Mục tiêu:**

* **Giảm thiểu rủi ro từ yếu tố con người**, hạn chế sai lầm gây ra lỗ hổng bảo mật.

## **2️⃣ Khái niệm "Defense in Depth" (Phòng thủ theo chiều sâu)**

* **"Defense in Depth" (Phòng thủ nhiều lớp)** là chiến lược **bảo mật nhiều tầng**, không phụ thuộc vào một biện pháp duy nhất.
* Nếu **một lớp bị tấn công**, vẫn còn các lớp bảo vệ khác để ngăn chặn hacker.
* Kết hợp **bảo vệ mạng, hệ điều hành, dữ liệu và con người** để đảm bảo an toàn hệ thống.

💡 **Ví dụ thực tế:** 🚀 Nếu tường lửa bị bypass, hệ điều hành vẫn có các biện pháp bảo vệ.  
 🚀 Nếu hacker vượt qua được hệ điều hành, họ vẫn không thể đọc dữ liệu vì dữ liệu đã được mã hóa.  
 🚀 Nếu hacker lừa được một nhân viên, hệ thống vẫn có cơ chế kiểm soát quyền truy cập.

## **3️⃣ Kết luận**

✅ **Defense in Depth là một mô hình bảo mật hiệu quả**, giúp bảo vệ hệ thống trước nhiều mối đe dọa.  
 ✅ **Không có một lớp bảo mật nào là tuyệt đối**, vì vậy cần **nhiều lớp bảo vệ phối hợp với nhau**.  
 ✅ **Bảo mật không chỉ là vấn đề công nghệ**, mà còn liên quan đến **quản lý, đào tạo nhân sự và giám sát liên tục**.

## 

## 

## **Khái niệm an toàn thông tin**

**ba nguyên tắc cốt lõi của an toàn thông tin**, thường được gọi là **CIA Triad (Confidentiality, Integrity, Availability)**. Đây là **nền tảng bảo mật** trong các hệ thống CNTT, đảm bảo dữ liệu được bảo vệ khỏi các mối đe dọa.

## **1️⃣ Ba nguyên tắc chính của an toàn thông tin**

### **🔹 1. Конфиденциальность (Tính bảo mật – Confidentiality)**

* **Bảo vệ thông tin khỏi truy cập trái phép**.
* Chỉ những **người dùng được ủy quyền mới có thể truy cập dữ liệu**.
* Ngăn chặn **rò rỉ dữ liệu, đánh cắp thông tin, truy cập trái phép**.

📌 **Phương pháp bảo vệ:** ✅ **Mã hóa dữ liệu (Encryption - AES, RSA)**.  
 ✅ **Hạn chế quyền truy cập (Access Control, Role-based Access Control - RBAC)**.  
 ✅ **Xác thực hai yếu tố (2FA, MFA - Multi-Factor Authentication)**.  
 ✅ **VPN, tường lửa, bảo vệ email chống lừa đảo (Phishing Protection)**.

💡 **Ví dụ thực tế:**

* **Dữ liệu tài chính, mật khẩu, thông tin cá nhân** cần được mã hóa.
* **Hệ thống ngân hàng chỉ cho phép nhân viên có quyền mới truy cập dữ liệu khách hàng**.

### **🔹 2. Целостность (Tính toàn vẹn – Integrity)**

* **Đảm bảo thông tin không bị thay đổi trái phép**.
* Ngăn chặn **mất mát, sửa đổi hoặc làm sai lệch dữ liệu**.
* Dữ liệu luôn đúng và chính xác **từ khi lưu trữ đến khi sử dụng**.

📌 **Phương pháp bảo vệ:** ✅ **Chữ ký số (Digital Signatures)** để xác minh dữ liệu không bị sửa đổi.  
 ✅ **Hashing (MD5, SHA-256)** để kiểm tra tính toàn vẹn của dữ liệu.  
 ✅ **Hệ thống kiểm soát phiên bản (Version Control - Git, Database Journaling)**.  
 ✅ **Cơ chế kiểm tra lỗi (Checksums, Parity Bits, RAID Storage)**.

💡 **Ví dụ thực tế:**

* **Tài liệu hợp đồng điện tử sử dụng chữ ký số để đảm bảo không bị thay đổi**.
* **Các giao dịch ngân hàng được ghi lại, nếu có sai lệch, hệ thống sẽ phát hiện ngay**.

### **🔹 3. Доступность (Tính sẵn sàng – Availability)**

* **Đảm bảo dữ liệu luôn sẵn có khi người dùng hợp pháp cần sử dụng**.
* Hệ thống phải **hoạt động ổn định, không bị gián đoạn**.
* Phòng chống **tấn công DDoS, lỗi hệ thống, mất điện, hỏng phần cứng**.

📌 **Phương pháp bảo vệ:** ✅ **Hệ thống sao lưu dữ liệu (Backup & Disaster Recovery Plan)**.  
 ✅ **Cân bằng tải (Load Balancing) để giảm tải hệ thống**.  
 ✅ **Hệ thống máy chủ dự phòng (Redundancy, Failover Systems)**.  
 ✅ **Bảo vệ chống tấn công DDoS bằng tường lửa và WAF (Web Application Firewall)**.

💡 **Ví dụ thực tế:**

* **Website thương mại điện tử cần đảm bảo không bị sập khi có nhiều người truy cập cùng lúc**.
* **Dữ liệu trong bệnh viện phải luôn sẵn sàng để bác sĩ có thể tra cứu ngay lập tức**.

## **2️⃣ Mối quan hệ giữa ba yếu tố CIA**

* **Tính bảo mật (Confidentiality) đảm bảo chỉ có người được phép truy cập dữ liệu**.
* **Tính toàn vẹn (Integrity) đảm bảo dữ liệu chính xác, không bị thay đổi trái phép**.
* **Tính sẵn sàng (Availability) đảm bảo dữ liệu luôn có thể truy cập khi cần**.

📌 **Sự cân bằng giữa các yếu tố**

* **Nếu bảo mật quá cao** (mã hóa phức tạp), có thể làm **giảm tính sẵn sàng** (hệ thống chậm, khó truy cập).
* **Nếu ưu tiên tính sẵn sàng** (mở rộng quyền truy cập), có thể **gây rủi ro bảo mật**.
* **Nếu dữ liệu không toàn vẹn**, nó **không còn giá trị** dù có bảo mật và sẵn sàng.

💡 **Một hệ thống an toàn phải duy trì cân bằng giữa cả ba yếu tố!**

## **3️⃣ Kết luận**

✅ **CIA Triad (Confidentiality - Integrity - Availability) là nền tảng của an toàn thông tin**.  
 ✅ **Bảo mật tốt không chỉ dựa vào công nghệ**, mà còn cần **quy trình quản lý và nhận thức của con người**.  
 ✅ **Cân bằng giữa bảo mật, toàn vẹn và sẵn sàng giúp hệ thống hoạt động hiệu quả và an toàn!**

## **"Угрозы, уязвимости и атаки" (Mối đe dọa, lỗ hổng và tấn công)**

**ba khái niệm quan trọng trong an toàn thông tin**:

* **Угроза (Mối đe dọa - Threat)**
* **Уязвимость (Lỗ hổng - Vulnerability)**
* **Атака (Tấn công - Attack)**

Đây là những yếu tố **cốt lõi của quản lý rủi ro an toàn thông tin**, giúp xác định và phòng chống các mối nguy hiểm trong hệ thống CNTT.

## **1️⃣ Giải thích từng khái niệm**

### **🔹 Угроза (Mối đe dọa - Threat)**

* **Mối đe dọa là một sự kiện có thể xảy ra, gây ảnh hưởng tiêu cực đến hệ thống hoặc dữ liệu.**
* Mối đe dọa có thể **từ bên trong hoặc bên ngoài tổ chức**, có thể là **tự nhiên (thiên tai) hoặc do con người gây ra**.

📌 **Ví dụ về mối đe dọa:** ✅ **Ransomware** – Phần mềm độc hại mã hóa dữ liệu và đòi tiền chuộc.  
 ✅ **Tấn công DDoS** – Hacker làm tắc nghẽn hệ thống, gây gián đoạn dịch vụ.  
 ✅ **Nội gián (Insider Threat)** – Nhân viên rò rỉ thông tin bí mật.  
 ✅ **Thiên tai (Hỏa hoạn, động đất)** – Hệ thống bị phá hủy do sự cố vật lý.

💡 **Mối đe dọa chưa chắc đã xảy ra, nhưng nếu có lỗ hổng, nó có thể trở thành một cuộc tấn công!**

### **🔹 Уязвимость (Lỗ hổng - Vulnerability)**

* **Lỗ hổng là điểm yếu trong hệ thống, có thể bị khai thác bởi mối đe dọa.**
* Lỗ hổng có thể tồn tại trong **phần mềm, phần cứng, quy trình quản lý hoặc con người**.

📌 **Ví dụ về lỗ hổng:** ✅ **Lỗi phần mềm (Bug, Zero-day vulnerability)** – Hacker có thể khai thác để chiếm quyền hệ thống.  
 ✅ **Mật khẩu yếu** – Dễ bị đoán hoặc tấn công brute force.  
 ✅ **Nhân viên không được đào tạo về bảo mật** – Dễ bị lừa đảo (phishing).  
 ✅ **Cấu hình sai trên tường lửa hoặc hệ thống mạng** – Dẫn đến lộ dữ liệu.

💡 **Lỗ hổng không gây hại nếu không có mối đe dọa khai thác nó.**

### **🔹 Атака (Tấn công - Attack)**

* **Tấn công là hành động khai thác lỗ hổng để thực hiện mối đe dọa**.
* Tấn công có thể do hacker, tổ chức tội phạm, hoặc các nhóm APT (Advanced Persistent Threat) thực hiện.

📌 **Ví dụ về các cuộc tấn công:** ✅ **Tấn công SQL Injection** – Khai thác lỗ hổng trong ứng dụng web để lấy dữ liệu.  
 ✅ **Tấn công Phishing** – Gửi email giả mạo để đánh cắp thông tin đăng nhập.  
 ✅ **Tấn công Man-in-the-Middle (MITM)** – Chặn và thay đổi dữ liệu truyền giữa hai bên.  
 ✅ **Tấn công Ransomware** – Mã hóa dữ liệu và đòi tiền chuộc.

💡 **Tấn công chính là sự hiện thực hóa của mối đe dọa bằng cách khai thác lỗ hổng.**

## **2️⃣ Mối quan hệ giữa Threat, Vulnerability, Attack**

* **Mối đe dọa (Threat) là nguy cơ có thể xảy ra.**
* **Lỗ hổng (Vulnerability) là điểm yếu có thể bị khai thác.**
* **Tấn công (Attack) là quá trình hacker sử dụng lỗ hổng để thực hiện mối đe dọa.**

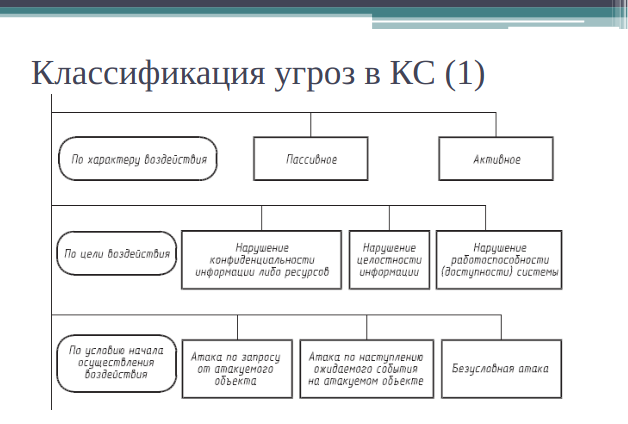
📌 **Ví dụ thực tế:** 1️⃣ **Mối đe dọa**: Một hacker muốn đánh cắp dữ liệu của công ty.  
 2️⃣ **Lỗ hổng**: Máy chủ có phần mềm lỗi chưa được cập nhật bảo mật.  
 3️⃣ **Tấn công**: Hacker khai thác lỗi đó để truy cập trái phép vào cơ sở dữ liệu.

💡 **Nếu lỗ hổng được vá, hacker sẽ không thể tấn công!**

## **3️⃣ Cách giảm thiểu rủi ro**

✅ **Phát hiện và vá lỗ hổng kịp thời (Patching, Penetration Testing).** ✅ **Đào tạo nhân viên về bảo mật để tránh bị lừa đảo.** ✅ **Triển khai các giải pháp bảo mật mạnh mẽ (Firewall, IDS/IPS, EDR).** ✅ **Sao lưu dữ liệu thường xuyên để giảm thiểu rủi ro từ ransomware.** ✅ **Xây dựng kế hoạch phản ứng sự cố để xử lý nhanh chóng khi bị tấn công.**

## **"Классификация угроз в КС" (Phân loại mối đe dọa trong hệ thống thông tin)**



Hình ảnh này mô tả cách **phân loại các mối đe dọa an toàn thông tin (угрозы) trong hệ thống máy tính (КС - Компьютерная система)** theo ba tiêu chí:  
 1️⃣ **Theo bản chất tác động (По характеру воздействия)** 2️⃣ **Theo mục tiêu tác động (По цели воздействия)** 3️⃣ **Theo điều kiện khởi tạo tấn công (По условию начала осуществления воздействия)**

## **1️⃣ Phân loại theo bản chất tác động (По характеру воздействия)**

Chia thành **hai loại chính**:

### **🔹 Пассивное (Thụ động - Passive)**

* **Không trực tiếp gây hại hoặc làm thay đổi hệ thống**, nhưng có thể **đánh cắp hoặc thu thập thông tin bí mật**.
* Kẻ tấn công **chỉ theo dõi, ghi lại dữ liệu mà không làm gián đoạn hệ thống**.

📌 **Ví dụ về tấn công thụ động:** ✅ **Sniffing (Chặn gói tin)** – Ghi lại dữ liệu truyền trên mạng.  
 ✅ **Shoulder Surfing** – Quan sát lén mật khẩu.  
 ✅ **Phân tích lưu lượng mạng (Traffic Analysis)** – Xác định hành vi người dùng.

💡 **Nguy hiểm vì khó bị phát hiện, nhưng có thể bị ngăn chặn bằng mã hóa dữ liệu (Encryption).**

### **🔹 Активное (Chủ động - Active)**

* **Tấn công trực tiếp vào hệ thống**, có thể **gây mất dữ liệu, thay đổi hoặc gián đoạn hoạt động**.
* Mối đe dọa loại này thường **dễ bị phát hiện nhưng gây thiệt hại nghiêm trọng**.

📌 **Ví dụ về tấn công chủ động:** ✅ **Tấn công DDoS** – Làm tê liệt máy chủ bằng cách gửi lượng lớn truy vấn.  
 ✅ **Tấn công SQL Injection** – Sửa đổi hoặc đánh cắp dữ liệu từ cơ sở dữ liệu.  
 ✅ **Tấn công Ransomware** – Mã hóa dữ liệu và yêu cầu tiền chuộc.

💡 **Cần có hệ thống phòng thủ mạnh như Firewall, IDS/IPS để phát hiện và ngăn chặn.**

## **2️⃣ Phân loại theo mục tiêu tác động (По цели воздействия)**

Mối đe dọa được chia thành ba loại chính:

### **🔹 Нарушение конфиденциальности информации (Xâm phạm tính bảo mật - Confidentiality Breach)**

* Dữ liệu **bị truy cập trái phép**, có thể bị **đánh cắp hoặc tiết lộ**.
* Mối đe dọa này thường xảy ra do **lỗ hổng trong hệ thống bảo mật hoặc do lỗi con người**.

📌 **Ví dụ:** ✅ **Phishing** – Giả mạo email để lấy thông tin đăng nhập.  
 ✅ **Data Breach** – Hacker xâm nhập và đánh cắp thông tin khách hàng.

### **🔹 Нарушение целостности информации (Xâm phạm tính toàn vẹn - Integrity Breach)**

* Dữ liệu bị **thay đổi, sửa đổi trái phép**, gây sai lệch thông tin.
* Điều này có thể dẫn đến **sai sót trong giao dịch tài chính, thông tin sai lệch trong hệ thống y tế, v.v.**.

📌 **Ví dụ:** ✅ **Tấn công Man-in-the-Middle (MITM)** – Thay đổi nội dung giao tiếp giữa hai bên.  
 ✅ **Tấn công giả mạo dữ liệu (Data Tampering)** – Sửa đổi thông tin trên cơ sở dữ liệu.

### **🔹 Нарушение работоспособности (Xâm phạm tính sẵn sàng - Availability Breach)**

* Mục tiêu là **làm gián đoạn hoạt động của hệ thống**, khiến người dùng không thể truy cập dữ liệu hoặc dịch vụ.

📌 **Ví dụ:** ✅ **DDoS** – Tấn công từ chối dịch vụ, làm sập website.  
 ✅ **Phá hoại phần cứng** – Gây lỗi vật lý trên hệ thống.

## **3️⃣ Phân loại theo điều kiện khởi tạo tấn công (По условию начала осуществления воздействия)**

Ba dạng tấn công chính dựa trên cách khởi động:

### **🔹 Атака по запросу от атакуемого объекта (Tấn công theo yêu cầu của mục tiêu bị tấn công)**

* Hacker **dụ dỗ nạn nhân tự kích hoạt mã độc** hoặc truy cập vào trang web lừa đảo.

📌 **Ví dụ:** ✅ **Phishing** – Người dùng nhấp vào email giả mạo và nhập thông tin cá nhân.  
 ✅ **Tải xuống phần mềm độc hại** – Người dùng tự tải và cài đặt mã độc.

### **🔹 Атака по наступлению ожидаемого события (Tấn công khi có sự kiện cụ thể xảy ra)**

* Hacker **cài sẵn mã độc**, nhưng chỉ kích hoạt khi có điều kiện nhất định xảy ra.

📌 **Ví dụ:** ✅ **Logic Bomb** – Mã độc chỉ kích hoạt khi có sự kiện cụ thể (ví dụ: ngày X, khi nhân viên bị sa thải, v.v.).  
 ✅ **Malware tiềm ẩn** – Chỉ tấn công khi nạn nhân thực hiện hành động nhất định.

### **🔹 Безусловная атака (Tấn công không điều kiện)**

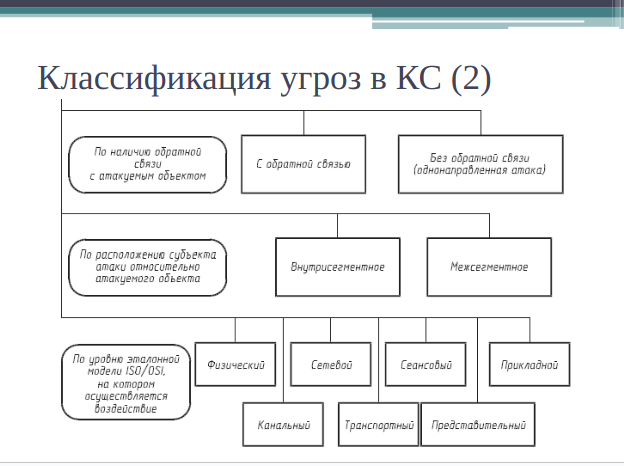
* Tấn công diễn ra ngay lập tức, **không cần sự tương tác từ phía nạn nhân**.

📌 **Ví dụ:** ✅ **Tấn công DDoS** – Nhắm vào máy chủ ngay khi hacker có thể.  
 ✅ **Worms (Sâu máy tính)** – Tự động lây lan mà không cần người dùng kích hoạt.

## **4️⃣ Kết luận**

* **Mối đe dọa có thể thụ động hoặc chủ động, tùy theo bản chất tấn công.**
* **Mục tiêu của mối đe dọa có thể là bảo mật, toàn vẹn hoặc tính sẵn sàng của hệ thống.**
* **Tấn công có thể xảy ra ngay lập tức hoặc khi có điều kiện cụ thể.**

## **"Классификация угроз в КС (2)" (Phân loại mối đe dọa trong hệ thống thông tin - Phần 2)**



tiếp tục phân loại **các mối đe dọa an toàn thông tin (угрозы) trong hệ thống máy tính (КС - Компьютерная система)** theo ba tiêu chí mới:  
 1️⃣ **Theo sự tồn tại của phản hồi từ mục tiêu bị tấn công (По наличию обратной связи с атакуемым объектом)** 2️⃣ **Theo vị trí của kẻ tấn công so với mục tiêu (По расположению субъекта атаки относительно атакуемого объекта)** 3️⃣ **Theo mô hình tầng ISO/OSI bị ảnh hưởng (По уровню эталонной модели ISO/OSI, на котором осуществляется воздействие)**

## **1️⃣ Phân loại theo sự tồn tại của phản hồi từ mục tiêu bị tấn công**

### **🔹 С обратной связью (Tấn công có phản hồi - Interactive Attack)**

* Hacker **nhận được phản hồi từ hệ thống mục tiêu** và có thể điều chỉnh cuộc tấn công dựa trên thông tin này.
* Thường được sử dụng trong **các cuộc tấn công có chủ đích (APT - Advanced Persistent Threats)** hoặc **tấn công thâm nhập sâu**.

📌 **Ví dụ:** ✅ **Brute Force Attack** – Thử nhiều mật khẩu khác nhau và nhận phản hồi từ hệ thống.  
 ✅ **SQL Injection** – Gửi truy vấn độc hại và nhận phản hồi từ cơ sở dữ liệu.  
 ✅ **Social Engineering** – Lừa đảo qua email, hacker chờ phản hồi từ nạn nhân.

💡 **Nguy hiểm vì hacker có thể tinh chỉnh chiến thuật dựa trên phản hồi nhận được.**

### **🔹 Без обратной связи (Tấn công một chiều - One-way Attack)**

* Hacker **không nhận được phản hồi từ mục tiêu**, mà chỉ gửi lệnh hoặc dữ liệu độc hại.
* Loại tấn công này **khó kiểm soát, nhưng ít hiệu quả hơn so với tấn công có phản hồi**.

📌 **Ví dụ:** ✅ **Tấn công DDoS** – Hacker gửi lượng lớn truy vấn nhưng không cần phản hồi từ máy chủ.  
 ✅ **Tấn công mã độc (Malware, Ransomware)** – Mã độc lây lan mà không cần chờ phản hồi từ hệ thống.  
 ✅ **Logic Bomb** – Mã độc được kích hoạt tự động mà không cần đầu vào từ hacker.

💡 **Dù không có phản hồi, loại tấn công này vẫn gây hậu quả nghiêm trọng, đặc biệt là trong các cuộc tấn công quy mô lớn.**

## **2️⃣ Phân loại theo vị trí của kẻ tấn công so với mục tiêu**

### **🔹 Внутрисегментное (Tấn công nội bộ - Intra-segment Attack)**

* Kẻ tấn công **nằm trong cùng một mạng với nạn nhân**.
* Nguy hiểm vì hacker có thể **khai thác lỗ hổng của hệ thống nội bộ mà không bị phát hiện từ bên ngoài**.

📌 **Ví dụ:** ✅ **ARP Spoofing** – Tấn công trong cùng mạng LAN để đánh cắp dữ liệu.  
 ✅ **MITM (Man-in-the-Middle)** – Chặn thông tin giữa hai thiết bị trong mạng nội bộ.  
 ✅ **Tấn công từ nhân viên nội bộ (Insider Threat)** – Nhân viên đánh cắp dữ liệu của công ty.

💡 **Tấn công nội bộ rất khó phòng ngừa nếu không có cơ chế giám sát mạnh.**

### **🔹 Межсегментное (Tấn công liên mạng - Inter-segment Attack)**

* Hacker **tấn công từ một mạng khác** hoặc **bên ngoài tổ chức**.
* Đây là kiểu tấn công phổ biến từ Internet vào hệ thống của công ty.

📌 **Ví dụ:** ✅ **Tấn công từ xa qua Internet (Remote Exploit)** – Hacker khai thác lỗ hổng trên máy chủ từ xa.  
 ✅ **Tấn công phishing** – Gửi email giả mạo để lừa người dùng.  
 ✅ **Zero-day Exploit** – Khai thác lỗ hổng chưa được vá từ mạng bên ngoài.

💡 **Cần có Firewall, IDS/IPS để ngăn chặn các mối đe dọa từ bên ngoài.**

## **3️⃣ Phân loại theo tầng ISO/OSI bị ảnh hưởng**

Các cuộc tấn công có thể nhắm vào **nhiều tầng khác nhau trong mô hình ISO/OSI**, gồm:

### **🔹 Физический (Tầng vật lý - Physical Layer)**

* **Tấn công vào phần cứng, cáp mạng hoặc tín hiệu vật lý**.

📌 **Ví dụ:** ✅ **Phá hoại thiết bị (Tampering, Hardware Sabotage)**.  
 ✅ **Tấn công tín hiệu Wi-Fi (Jamming, Signal Interference)**.

### **🔹 Сетевой (Tầng mạng - Network Layer)**

* **Tấn công vào giao thức mạng hoặc thiết bị định tuyến**.

📌 **Ví dụ:** ✅ **IP Spoofing** – Giả mạo địa chỉ IP.  
 ✅ **DDoS Attack** – Làm sập hệ thống bằng lượng lớn lưu lượng mạng.

### **🔹 Сеансовый (Tầng phiên - Session Layer)**

* **Tấn công vào phiên làm việc giữa người dùng và hệ thống**.

📌 **Ví dụ:** ✅ **Session Hijacking** – Chiếm quyền phiên làm việc của người dùng.

### **🔹 Прикладной (Tầng ứng dụng - Application Layer)**

* **Tấn công vào ứng dụng và dữ liệu người dùng**.

📌 **Ví dụ:** ✅ **SQL Injection** – Tấn công vào cơ sở dữ liệu của ứng dụng web.  
 ✅ **Phishing** – Giả mạo trang web để lừa người dùng nhập thông tin.

### **🔹 Канальный, Транспортный, Представительный (Tầng liên kết dữ liệu, vận chuyển, trình bày)**

* Ít phổ biến hơn nhưng vẫn có thể bị khai thác.
* **Ví dụ:**
  + **Tầng vận chuyển (Transport Layer) bị tấn công DoS qua TCP SYN Flood**.
  + **Tầng liên kết dữ liệu (Data Link Layer) bị tấn công MAC Flooding**.

## **4️⃣ Kết luận**

🔹 **Các cuộc tấn công có thể có hoặc không có phản hồi từ mục tiêu, ảnh hưởng đến cách hacker triển khai tấn công.** 🔹 **Tấn công có thể diễn ra từ bên trong mạng nội bộ hoặc từ Internet, cần biện pháp bảo vệ cả trong và ngoài.** 🔹 **Các cuộc tấn công có thể xảy ra ở nhiều tầng khác nhau trong mô hình OSI, cần bảo vệ toàn diện.**

## **"Источники уязвимостей" (Nguồn gốc của lỗ hổng bảo mật)**

Lỗ hổng bảo mật (уязвимость) xuất hiện do **các lỗi trong quá trình thiết kế, phát triển và bảo trì hệ thống**. nguyên nhân gây ra lỗ hổng thành **ba nhóm chính**:

1️⃣ **Ошибки проектирования (Lỗi thiết kế - Design Flaws)** 2️⃣ **Ошибки реализации (Lỗi triển khai - Implementation Flaws)** 3️⃣ **Ошибки обслуживания (Lỗi bảo trì - Maintenance Errors)**

## **1️⃣ Ошибки проектирования (Lỗi thiết kế - Design Flaws)**

* **Lỗi ngay từ giai đoạn thiết kế hệ thống** (phần mềm, phần cứng, giao thức).
* Nếu thiết kế có vấn đề, hệ thống sẽ dễ bị tấn công ngay cả khi mã nguồn không có lỗi.

📌 **Ví dụ về lỗi thiết kế:** ✅ **Thiết kế hệ thống không có mã hóa dữ liệu** → Dữ liệu có thể bị đánh cắp.  
 ✅ **Giao thức xác thực yếu** → Dễ bị tấn công brute-force.  
 ✅ **Không có kiểm soát truy cập (Access Control)** → Người dùng có thể truy cập trái phép.

💡 **Nếu lỗi nằm trong thiết kế, rất khó sửa chữa sau khi hệ thống đã triển khai!**

## **2️⃣ Ошибки реализации (Lỗi triển khai - Implementation Flaws)**

* **Lỗi xảy ra trong quá trình lập trình hoặc cấu hình hệ thống**.
* Có thể dẫn đến **lỗ hổng bảo mật nghiêm trọng như SQL Injection, Buffer Overflow**.

📌 **Ví dụ về lỗi triển khai:** ✅ **SQL Injection** – Do không kiểm tra dữ liệu đầu vào.  
 ✅ **Buffer Overflow** – Do lập trình viên không giới hạn kích thước bộ nhớ.  
 ✅ **Hardcoded Credentials** – Mật khẩu được ghi trực tiếp trong mã nguồn.

💡 **Hầu hết các cuộc tấn công mạng khai thác lỗi trong giai đoạn triển khai!**

## **3️⃣ Ошибки обслуживания (Lỗi bảo trì - Maintenance Errors)**

* **Lỗi xảy ra khi hệ thống không được cập nhật, giám sát hoặc bảo trì đúng cách**.
* Hệ thống an toàn khi mới triển khai, nhưng dễ bị tấn công nếu không bảo trì thường xuyên.

📌 **Ví dụ về lỗi bảo trì:** ✅ **Không cập nhật phần mềm (Patch Management)** → Lỗ hổng cũ không được sửa.  
 ✅ **Sử dụng mật khẩu mặc định** → Hacker dễ đoán và truy cập trái phép.  
 ✅ **Không giám sát nhật ký hệ thống** → Không phát hiện được cuộc tấn công sớm.

💡 **Hệ thống an toàn không chỉ phụ thuộc vào thiết kế và triển khai, mà còn cần bảo trì liên tục!**

## **4️⃣ Kết luận**

🔹 **Lỗ hổng bảo mật có thể xuất phát từ lỗi trong thiết kế, triển khai hoặc bảo trì hệ thống.** 🔹 **Lỗi thiết kế rất khó sửa, lỗi triển khai phổ biến nhất, lỗi bảo trì thường bị bỏ qua nhưng gây rủi ro cao.** 🔹 **Để bảo vệ hệ thống, cần kết hợp kiểm tra bảo mật từ giai đoạn thiết kế, coding đến bảo trì!**

💡 **Một hệ thống an toàn không chỉ cần mã nguồn sạch mà còn cần quản lý và giám sát tốt!** 🚀

## **"Уязвимости – степень риска" (Lỗ hổng – mức độ rủi ro)**

**các phương pháp đánh giá mức độ rủi ro của lỗ hổng bảo mật**, bao gồm **phương pháp định tính và định lượng**.

## **1️⃣ Đánh giá định tính (Качественный подход - Qualitative Approach)**

* **Sử dụng mô hình đèn giao thông** (светофорная модель) để phân loại rủi ro theo **mức độ nghiêm trọng**.
* Đây là phương pháp **dễ hiểu, nhanh chóng**, giúp doanh nghiệp đánh giá mức độ nguy hiểm của một lỗ hổng.

📌 **Ba mức độ rủi ro:** 🟥 **Высокий риск (Rủi ro cao - High Risk)**

* **Lỗ hổng nghiêm trọng**, có thể **bị khai thác ngay lập tức** và gây **hậu quả nghiêm trọng**.
* Cần **khắc phục ngay** để tránh bị tấn công.  
   ✅ **Ví dụ:** Lỗ hổng cho phép **chiếm quyền admin từ xa (Remote Code Execution - RCE)**.

🟨 **Средний риск (Rủi ro trung bình - Medium Risk)**

* **Lỗ hổng có thể bị khai thác trong một số điều kiện nhất định**.
* Không cần sửa ngay lập tức nhưng **cần theo dõi và vá lỗi sớm**.  
   ✅ **Ví dụ:** **Lỗ hổng XSS (Cross-Site Scripting)**, có thể bị hacker lợi dụng để đánh cắp phiên đăng nhập.

🟩 **Низкий риск (Rủi ro thấp - Low Risk)**

* **Lỗ hổng không có khả năng bị khai thác ngay**, tác động thấp.
* Có thể **chờ đến lần cập nhật tiếp theo** để khắc phục.  
   ✅ **Ví dụ:** **Lỗi giao diện hoặc hiển thị thông tin không nhạy cảm**.

💡 **Phương pháp này nhanh chóng nhưng không chính xác 100% vì dựa trên đánh giá chủ quan!**

## **2️⃣ Đánh giá định lượng (Количественный подход - Quantitative Approach)**

* **Dựa trên số liệu thực tế** để đánh giá mức độ rủi ro.
* Tính toán theo **hai yếu tố chính**:

📌 **1. Вероятность негативного сценария (Xác suất xảy ra tình huống tiêu cực)** ✅ **Lỗ hổng dễ khai thác** → Xác suất cao.  
 ✅ **Lỗ hổng yêu cầu quyền truy cập đặc biệt** → Xác suất thấp.

📌 **2. Ущерб от негативного сценария (Tổn thất khi bị khai thác)** ✅ **Gây mất dữ liệu quan trọng** → Tổn thất lớn.  
 ✅ **Gây gián đoạn tạm thời** → Tổn thất thấp hơn.

💡 **Phương pháp này chính xác hơn nhưng cần nhiều dữ liệu và phân tích chi tiết!**

## **3️⃣ So sánh hai phương pháp đánh giá rủi ro**

| **Tiêu chí** | **Đánh giá định tính 🟥🟨🟩** | **Đánh giá định lượng 📊** |
| --- | --- | --- |
| **Tốc độ đánh giá** | Nhanh, dễ hiểu | Cần nhiều thời gian |
| **Mức độ chính xác** | Tương đối (chủ quan) | Cao (dựa trên số liệu) |
| **Ứng dụng** | Phù hợp để đánh giá nhanh | Dùng trong phân tích rủi ro chuyên sâu |
| **Nhược điểm** | Dễ bị sai lệch nếu đánh giá không chính xác | Yêu cầu nhiều dữ liệu & công cụ hỗ trợ |

💡 **Tốt nhất là kết hợp cả hai phương pháp để có cái nhìn tổng quan và chính xác về mức độ rủi ro của lỗ hổng!** 🚀

Danh mục lỗ hổng

* SANS Top 20 Internet Vulnerabilities List <https://www.sans.org/critical-security-controls/>
* Common Vulnerabilities and Exposures (CVE) <http://cve.mitre.org/>
* National Vulnerability Database <https://nvd.nist.gov/>

## **"Механизмы реализации сетевых атак" (Cơ chế thực hiện tấn công mạng)**

**các cơ chế chính mà hacker sử dụng để thực hiện các cuộc tấn công mạng**. Các cơ chế này có thể được áp dụng độc lập hoặc kết hợp để **khai thác lỗ hổng, đánh cắp thông tin hoặc làm gián đoạn hệ thống**.

## **1️⃣ Пассивное прослушивание (Nghe lén thụ động - Passive Eavesdropping)**

* **Tấn công không làm thay đổi dữ liệu, mà chỉ theo dõi và thu thập thông tin**.
* **Khó phát hiện** vì không gây ảnh hưởng trực tiếp đến hệ thống.

📌 **Ví dụ:** ✅ **Packet Sniffing** – Dùng Wireshark để theo dõi dữ liệu truyền trên mạng.  
 ✅ **Man-in-the-Middle (MITM)** – Chặn giao tiếp giữa hai bên mà họ không biết.  
 ✅ **Side-Channel Attack** – Phân tích dữ liệu không trực tiếp (ví dụ: đoán mật khẩu từ tiếng gõ phím).

💡 **Cách phòng chống:**

* **Mã hóa dữ liệu (TLS, VPN, SSH)** để tránh bị theo dõi.
* **Sử dụng HTTPS thay vì HTTP** khi duyệt web.

## **2️⃣ Подозрительная активность (Hoạt động đáng ngờ - Suspicious Activity)**

* **Các hành vi bất thường trong hệ thống**, có thể là dấu hiệu của một cuộc tấn công sắp xảy ra.

📌 **Ví dụ:** ✅ **Nhiều lần đăng nhập thất bại liên tục** – Dấu hiệu của Brute Force Attack.  
 ✅ **Truy vấn SQL lạ trong nhật ký máy chủ** – Dấu hiệu SQL Injection.  
 ✅ **Lưu lượng mạng tăng đột biến không rõ nguyên nhân** – Có thể là DDoS.

💡 **Cách phòng chống:**

* **Sử dụng hệ thống giám sát (SIEM, IDS/IPS)** để phát hiện hành vi bất thường.
* **Giới hạn số lần đăng nhập sai**, khóa tài khoản nếu phát hiện đăng nhập bất thường.

## **3️⃣ Бесполезное расходование вычислительного ресурса (Lãng phí tài nguyên tính toán - Resource Exhaustion)**

* **Tấn công làm cạn kiệt tài nguyên hệ thống**, khiến hệ thống không thể hoạt động bình thường.

📌 **Ví dụ:** ✅ **DDoS Attack** – Gửi lượng lớn yêu cầu giả mạo để làm sập hệ thống.  
 ✅ **Fork Bomb** – Chạy một quá trình tự nhân bản liên tục để làm cạn kiệt CPU.  
 ✅ **ZIP Bomb** – Tạo file nén nhỏ nhưng khi giải nén chiếm hàng TB dung lượng.

💡 **Cách phòng chống:**

* **Giới hạn tài nguyên hệ thống (Rate Limiting, Connection Throttling).**
* **Dùng Firewall và WAF để chặn lưu lượng bất thường.**

## **4️⃣ Нарушение навигации (Làm gián đoạn điều hướng - Navigation Disruption)**

* **Gây nhầm lẫn hoặc đánh lừa người dùng về hướng di chuyển trong hệ thống**.

📌 **Ví dụ:** ✅ **DNS Spoofing** – Chuyển hướng người dùng đến website giả mạo.  
 ✅ **Phishing Attack** – Giả mạo giao diện website để lấy thông tin đăng nhập.  
 ✅ **Clickjacking** – Dùng iframe ẩn để dụ người dùng bấm vào nút nguy hiểm.

💡 **Cách phòng chống:**

* **Sử dụng DNSSEC để bảo vệ hệ thống DNS.**
* **Kiểm tra đường link trước khi bấm vào, không nhập thông tin trên trang web lạ.**

## **5️⃣ Выведение из строя (Làm gián đoạn hệ thống - System Disruption)**

* **Tấn công làm hệ thống ngừng hoạt động hoàn toàn.**

📌 **Ví dụ:** ✅ **Tấn công DDoS mạnh (Botnet)** – Làm tê liệt máy chủ.  
 ✅ **Phá hoại vật lý (Physical Destruction)** – Phá hủy phần cứng.  
 ✅ **Wiper Malware** – Mã độc xóa toàn bộ dữ liệu trên hệ thống.

💡 **Cách phòng chống:**

* **Có hệ thống dự phòng và kế hoạch khôi phục dữ liệu (Disaster Recovery Plan).**
* **Bảo vệ vật lý (giám sát camera, kiểm soát truy cập).**

## **6️⃣ Запуск кода на объекте атаки (Thực thi mã độc trên hệ thống mục tiêu - Code Execution Attack)**

* **Chạy mã độc trên hệ thống để chiếm quyền điều khiển hoặc phá hoại dữ liệu.**

📌 **Ví dụ:** ✅ **Remote Code Execution (RCE)** – Hacker có thể chạy lệnh trên hệ thống từ xa.  
 ✅ **SQL Injection** – Cho phép hacker thực thi lệnh trên cơ sở dữ liệu.  
 ✅ **Fileless Malware** – Mã độc chạy trong bộ nhớ mà không để lại dấu vết trên ổ đĩa.

💡 **Cách phòng chống:**

* **Cập nhật hệ thống và vá lỗ hổng thường xuyên.**
* **Chặn quyền thực thi mã đối với file đáng ngờ.**

## **7️⃣ Kết luận**

🔹 **Tấn công mạng có thể thực hiện bằng nhiều cơ chế khác nhau, từ theo dõi thụ động đến làm sập hệ thống.** 🔹 **Các cuộc tấn công ngày càng tinh vi, cần biện pháp bảo vệ mạnh mẽ ở nhiều cấp độ.** 🔹 **Kết hợp Firewall, IDS/IPS, mã hóa, và giám sát bảo mật sẽ giúp giảm thiểu rủi ro tấn công.**

## **"Механизмы защиты" (Cơ chế bảo vệ an ninh mạng)**

**ba loại cơ chế bảo vệ trong an ninh mạng**, được phân loại theo **chức năng của chúng trong việc bảo vệ hệ thống trước các cuộc tấn công**.

Ba nhóm chính là:  
 1️⃣ **Превентивные (Phòng ngừa - Preventive)** 2️⃣ **Детективные (Phát hiện - Detective)** 3️⃣ **Коррективные (Khắc phục - Corrective)**

## **1️⃣ Превентивные (Cơ chế phòng ngừa - Preventive Mechanisms)**

* **Ngăn chặn các cuộc tấn công trước khi chúng xảy ra** bằng cách **bảo vệ lỗ hổng và kiểm soát truy cập**.
* Đây là **tuyến phòng thủ đầu tiên** trong an toàn thông tin.

📌 **Ví dụ về cơ chế phòng ngừa:** ✅ **Tường lửa (Firewall)** – Chặn lưu lượng độc hại trước khi vào hệ thống.  
 ✅ **Hệ thống kiểm soát truy cập (Access Control, RBAC)** – Hạn chế quyền truy cập của người dùng.  
 ✅ **Mã hóa dữ liệu (Encryption - AES, TLS, VPN)** – Ngăn chặn rò rỉ thông tin.  
 ✅ **Xác thực hai yếu tố (2FA, MFA)** – Ngăn chặn truy cập trái phép.  
 ✅ **Cập nhật phần mềm thường xuyên (Patching, Security Updates)** – Vá lỗ hổng bảo mật.

💡 **Cơ chế phòng ngừa rất quan trọng, nhưng không thể ngăn chặn 100% các cuộc tấn công!**

## **2️⃣ Детективные (Cơ chế phát hiện - Detective Mechanisms)**

* **Giúp phát hiện tấn công kịp thời** để có thể phản ứng nhanh chóng.
* **Không ngăn chặn được tấn công, nhưng giúp xác định dấu hiệu bất thường**.

📌 **Ví dụ về cơ chế phát hiện:** ✅ **Hệ thống phát hiện xâm nhập (IDS - Intrusion Detection System)** – Theo dõi lưu lượng mạng để phát hiện dấu hiệu tấn công.  
 ✅ **Giám sát nhật ký hệ thống (SIEM - Security Information and Event Management)** – Phân tích nhật ký để phát hiện hành vi đáng ngờ.  
 ✅ **Phát hiện phần mềm độc hại (Antivirus, Endpoint Detection and Response - EDR)** – Kiểm tra các tập tin hoặc tiến trình độc hại.  
 ✅ **Hệ thống giám sát hoạt động người dùng (UEBA - User and Entity Behavior Analytics)** – Phát hiện hành vi bất thường của người dùng.

💡 **Cơ chế phát hiện giúp doanh nghiệp nhận biết mối đe dọa trước khi chúng gây ra thiệt hại lớn!**

## **3️⃣ Коррективные (Cơ chế khắc phục - Corrective Mechanisms)**

* **Giúp khôi phục hệ thống sau khi bị tấn công hoặc xảy ra sự cố.**
* **Giảm thiểu hậu quả của cuộc tấn công và đảm bảo hệ thống trở lại hoạt động bình thường.**

📌 **Ví dụ về cơ chế khắc phục:** ✅ **Hệ thống sao lưu dữ liệu (Backup & Disaster Recovery Plan)** – Phục hồi dữ liệu bị mất.  
 ✅ **Phân tích nguyên nhân (Post-Incident Analysis)** – Tìm hiểu nguyên nhân vụ tấn công để cải thiện hệ thống.  
 ✅ **Cô lập hệ thống bị nhiễm mã độc (Isolation & Containment)** – Ngăn chặn lây lan phần mềm độc hại.  
 ✅ **Triển khai các bản vá khẩn cấp (Emergency Patching)** – Vá lỗ hổng sau khi bị khai thác.

💡 **Cơ chế khắc phục giúp hệ thống phục hồi nhanh chóng và ngăn ngừa tấn công lặp lại!**

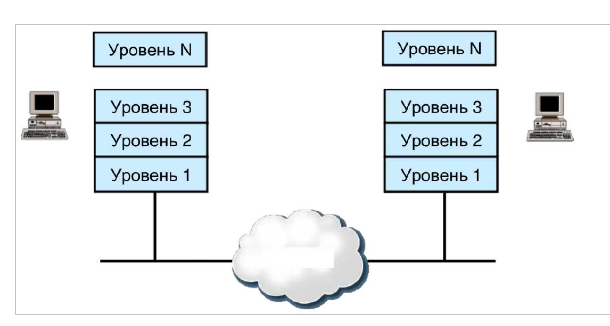
## **4️⃣ So sánh ba cơ chế bảo vệ**

| **Tiêu chí** | **Phòng ngừa (Preventive)** | **Phát hiện (Detective)** | **Khắc phục (Corrective)** |
| --- | --- | --- | --- |
| **Chức năng** | Ngăn chặn tấn công xảy ra | Phát hiện tấn công sớm | Phục hồi hệ thống sau tấn công |
| **Mục tiêu** | Bảo vệ trước tấn công | Nhận diện hành vi đáng ngờ | Giảm thiểu hậu quả, khôi phục |
| **Ví dụ** | Tường lửa, 2FA, mã hóa | IDS, SIEM, giám sát mạng | Sao lưu dữ liệu, vá lỗi khẩn cấp |
| **Hạn chế** | Không thể ngăn chặn tất cả mối đe dọa | Không tự động ngăn chặn tấn công | Không giúp ngăn chặn cuộc tấn công tiếp theo |

💡 **Hệ thống bảo mật mạnh mẽ cần KẾT HỢP cả ba cơ chế này để bảo vệ toàn diện!** 🚀

## **"Сетевое взаимодействие – многоуровневый подход" (Tương tác mạng – phương pháp nhiều lớp)**

**mô hình phân lớp trong truyền thông mạng**, phản ánh cách các hệ thống giao tiếp với nhau thông qua **nhiều tầng (уровень)**. Đây là nguyên tắc cơ bản của **mô hình tham chiếu OSI (Open Systems Interconnection Model)** và **mô hình TCP/IP**.



## **1️⃣ Giải thích mô hình nhiều lớp**

* **Mỗi hệ thống đều có các tầng khác nhau để xử lý thông tin và truyền tải dữ liệu.**
* **Dữ liệu đi qua từng lớp (tầng) trước khi được gửi qua mạng đến hệ thống khác.**
* **Hai thiết bị giao tiếp với nhau thông qua cùng một tập hợp các tầng.**

💡 **Nguyên tắc chính:** 🔹 **Giao tiếp giữa hai hệ thống luôn diễn ra theo từng tầng tương ứng.** 🔹 **Tầng thấp hơn cung cấp dịch vụ cho tầng cao hơn.** 🔹 **Mỗi tầng chỉ thực hiện các chức năng cụ thể, không can thiệp vào các tầng khác.**

## **2️⃣ So sánh với mô hình OSI và TCP/IP**

Hình ảnh minh họa một hệ thống nhiều lớp tương tự **mô hình OSI (7 lớp) hoặc TCP/IP (4 lớp)**.

📌 **Mô hình OSI (7 tầng)**:  
 1️⃣ **Tầng vật lý (Physical Layer)** – Truyền dữ liệu dưới dạng tín hiệu điện hoặc quang.  
 2️⃣ **Tầng liên kết dữ liệu (Data Link Layer)** – Định dạng khung dữ liệu, kiểm soát truy cập mạng.  
 3️⃣ **Tầng mạng (Network Layer)** – Định tuyến dữ liệu giữa các mạng khác nhau.  
 4️⃣ **Tầng vận chuyển (Transport Layer)** – Đảm bảo dữ liệu truyền tin cậy (TCP, UDP).  
 5️⃣ **Tầng phiên (Session Layer)** – Quản lý phiên giao tiếp giữa các ứng dụng.  
 6️⃣ **Tầng trình bày (Presentation Layer)** – Mã hóa, nén dữ liệu.  
 7️⃣ **Tầng ứng dụng (Application Layer)** – Giao diện giữa người dùng và hệ thống (HTTP, FTP, DNS).

📌 **Mô hình TCP/IP (4 tầng)**:  
 1️⃣ **Tầng truy cập mạng (Network Access Layer)** – Tương ứng với tầng vật lý & liên kết dữ liệu OSI.  
 2️⃣ **Tầng Internet (Internet Layer)** – Xử lý định tuyến, địa chỉ IP.  
 3️⃣ **Tầng vận chuyển (Transport Layer)** – Đảm bảo truyền dữ liệu tin cậy (TCP, UDP).  
 4️⃣ **Tầng ứng dụng (Application Layer)** – HTTP, FTP, SMTP, DNS, v.v.

## **3️⃣ Ý nghĩa của phương pháp nhiều lớp trong bảo mật mạng**

🔹 **Bảo mật theo từng tầng** – Mỗi tầng có thể có các biện pháp bảo vệ riêng, ví dụ:  
 ✅ **Tầng mạng** – Firewall để lọc lưu lượng nguy hiểm.  
 ✅ **Tầng vận chuyển** – TLS/SSL để mã hóa dữ liệu.  
 ✅ **Tầng ứng dụng** – Kiểm tra đầu vào để ngăn SQL Injection.

🔹 **Dễ dàng mở rộng hệ thống** – Mỗi tầng có thể được nâng cấp hoặc thay đổi độc lập.

🔹 **Giảm thiểu rủi ro tấn công** – Nếu một tầng bị tấn công, các tầng khác vẫn có thể bảo vệ hệ thống.

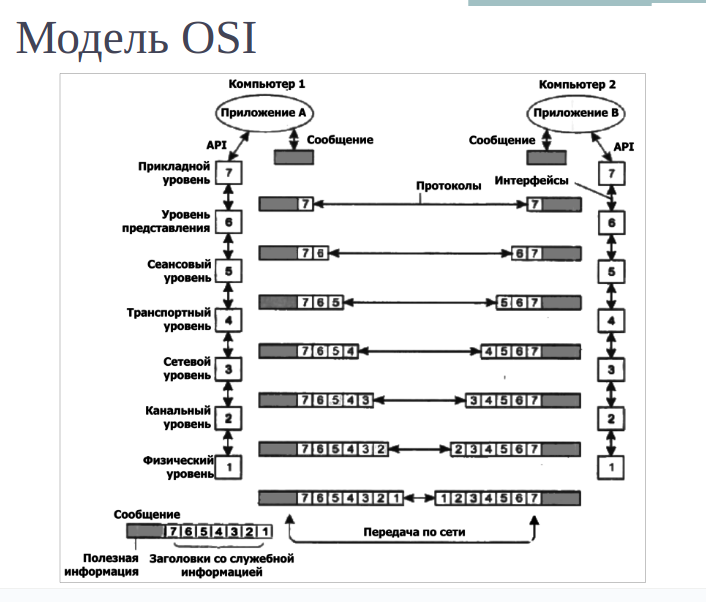
## **4️⃣ Kết luận**

🔹 **Phương pháp nhiều lớp là nguyên tắc quan trọng trong thiết kế mạng và bảo mật.** 🔹 **Dữ liệu luôn được xử lý qua nhiều tầng trước khi truyền tải đến hệ thống khác.** 🔹 **Việc bảo vệ từng tầng riêng biệt giúp nâng cao tính an toàn cho hệ thống.**

## **"Модель OSI" (Mô hình OSI)**

Hình ảnh minh họa **mô hình OSI (Open Systems Interconnection Model)**, một mô hình **7 tầng** giúp chuẩn hóa quá trình truyền thông mạng giữa các thiết bị.

📌 **Mô hình OSI giúp hiểu cách dữ liệu được truyền từ thiết bị này sang thiết bị khác** bằng cách chia nhỏ thành **7 tầng riêng biệt**, mỗi tầng có nhiệm vụ riêng.



## **1️⃣ Các tầng trong mô hình OSI**

Mô hình OSI gồm **7 tầng**, từ thấp nhất (tầng vật lý) đến cao nhất (tầng ứng dụng):

| **Tầng** | **Tên** | **Chức năng chính** |
| --- | --- | --- |
| 7️⃣ **Ứng dụng** (Application Layer) | Giao diện giữa người dùng và hệ thống mạng | HTTP, FTP, SMTP, DNS |
| 6️⃣ **Trình bày** (Presentation Layer) | Mã hóa, giải mã, nén dữ liệu | SSL/TLS, JPEG, PNG, ASCII |
| 5️⃣ **Phiên** (Session Layer) | Quản lý phiên làm việc giữa hai thiết bị | RPC, NetBIOS, SQL Sessions |
| 4️⃣ **Vận** **chuyển**(Transport Layer) | Truyền dữ liệu tin cậy giữa hai thiết bị | TCP, UDP |
| 3️⃣ **Mạng** (Network Layer) | Định tuyến, cấp địa chỉ IP | IP, ICMP, ARP, RIP, OSPF |
| 2️⃣ **Liên kết dữ liệu** (Data Link Layer) | Kiểm soát truy cập mạng, phát hiện lỗi | Ethernet, MAC Address, VLAN |
| 1️⃣ **Vật lý** (Physical Layer) | Truyền tín hiệu điện, quang | Cáp quang, Wi-Fi, Bluetooth |

💡 **Dữ liệu đi từ tầng 7 đến tầng 1 khi gửi đi, và từ tầng 1 đến tầng 7 khi nhận về!**

## **2️⃣ Quá trình truyền dữ liệu giữa hai máy tính**

Trong hình ảnh, có hai máy tính **(Компьютер 1 và Компьютер 2)** đang truyền dữ liệu qua **mô hình OSI**:

1. **Ứng dụng A trên Máy tính 1 gửi tin nhắn.**
2. Dữ liệu đi qua **các tầng OSI**, từ **tầng 7 xuống tầng 1**.
3. Ở tầng 1 (vật lý), dữ liệu được truyền qua mạng (cáp, Wi-Fi, v.v.).
4. Máy tính 2 nhận tín hiệu và **chuyển dữ liệu ngược lại từ tầng 1 lên tầng 7**.
5. **Ứng dụng B trên Máy tính 2 nhận tin nhắn.**

📌 **Nguyên tắc quan trọng:** 🔹 **Hai thiết bị giao tiếp thông qua các tầng tương ứng.** 🔹 **Dữ liệu khi truyền đi được đóng gói (Encapsulation), khi nhận về được giải nén (Decapsulation).**

## **3️⃣ Cách dữ liệu được đóng gói và giải nén**

* Khi **gửi dữ liệu**, mỗi tầng sẽ **thêm một phần header** để hướng dẫn tầng tiếp theo xử lý dữ liệu.
* Khi **nhận dữ liệu**, mỗi tầng **loại bỏ phần header** để lấy nội dung thực tế.

📌 **Ví dụ:** ✅ **Tầng ứng dụng (7)** tạo tin nhắn gốc.  
 ✅ **Tầng vận chuyển (4)** thêm thông tin TCP/UDP để đảm bảo truyền dữ liệu đúng cách.  
 ✅ **Tầng mạng (3)** thêm địa chỉ IP để định tuyến gói tin.  
 ✅ **Tầng liên kết dữ liệu (2)** thêm địa chỉ MAC để gửi dữ liệu đến đúng thiết bị.

💡 **Quá trình này đảm bảo dữ liệu đến đúng nơi và được truyền tải an toàn!**

## **4️⃣ So sánh OSI và mô hình TCP/IP**

Mô hình OSI có **7 tầng**, trong khi mô hình TCP/IP thực tế chỉ có **4 tầng**:

| **Mô hình OSI** | **Mô hình TCP/IP** |
| --- | --- |
| 7️⃣ Ứng dụng | 🟢 Ứng dụng |
| 6️⃣ Trình diễn | 🟢 Ứng dụng |
| 5️⃣ Phiên | 🟢 Ứng dụng |
| 4️⃣ Giao vận | 🟡 Giao vận (Transport) |
| 3️⃣ Mạng | 🟠 Internet |
| 2️⃣ Liên kết dữ liệu | 🔵 Mạng (Network Access) |
| 1️⃣ Vật lý | 🔵 Mạng (Network Access) |

💡 **TCP/IP thực tế hơn và đơn giản hơn so với OSI, nhưng OSI giúp hiểu sâu hơn về cách mạng hoạt động!**

## **5️⃣ Tại sao mô hình OSI quan trọng?**

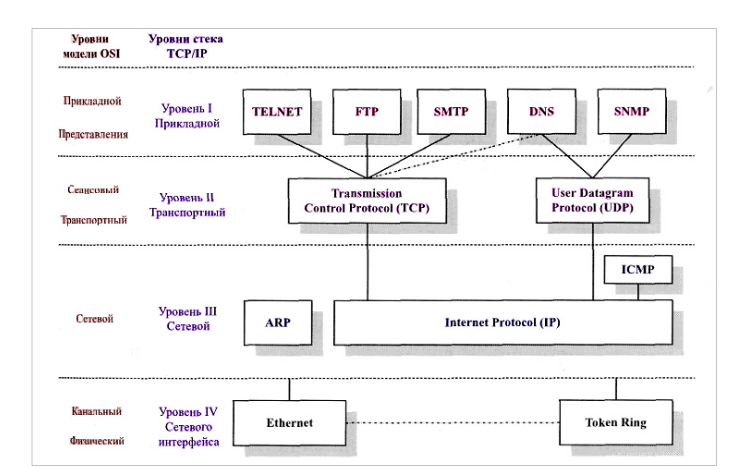
✅ **Chuẩn hóa giao tiếp mạng giữa các thiết bị khác nhau.** ✅ **Giúp các nhà phát triển và kỹ sư hiểu cách dữ liệu di chuyển qua mạng.** ✅ **Hỗ trợ chẩn đoán và khắc phục sự cố mạng theo từng tầng.**

## 

## 

## **"Структура стека TCP/IP" (Cấu trúc ngăn xếp giao thức TCP/IP)**

Hình ảnh này minh họa **cấu trúc ngăn xếp TCP/IP**, một **mô hình giao tiếp mạng thực tế** được sử dụng rộng rãi trên Internet. Mô hình TCP/IP có **4 tầng chính**, so với mô hình OSI **7 tầng**.



## **1️⃣ So sánh mô hình OSI và mô hình TCP/IP**

| **Mô hình OSI (7 tầng)** | **Mô hình TCP/IP (4 tầng)** | **Chức năng** |
| --- | --- | --- |
| 7️⃣ Ứng dụng (Application) | 🟢 Ứng dụng (Application) | Giao diện giữa người dùng và hệ thống |
| 6️⃣ Trình diễn (Presentation) | 🟢 Ứng dụng (Application) | Mã hóa, nén dữ liệu |
| 5️⃣ Phiên (Session) | 🟢 Ứng dụng (Application) | Quản lý phiên làm việc |
| 4️⃣ Giao vận (Transport) | 🟡 Giao vận (Transport) | Truyền dữ liệu tin cậy (TCP/UDP) |
| 3️⃣ Mạng (Network) | 🟠 Internet (Network) | Định tuyến, địa chỉ IP |
| 2️⃣ Liên kết dữ liệu (Data Link) | 🔵 Mạng truy cập (Network Access) | Kiểm soát truy cập mạng |
| 1️⃣ Vật lý (Physical) | 🔵 Mạng truy cập (Network Access) | Truyền tín hiệu điện, quang |

💡 **Mô hình TCP/IP thực tế hơn, đơn giản hơn, nhưng vẫn bao gồm tất cả các chức năng của OSI!**

## **2️⃣ Cấu trúc ngăn xếp TCP/IP**

Hình ảnh chia ngăn xếp TCP/IP thành **4 tầng chính**, mỗi tầng tương ứng với các giao thức khác nhau.

### **🔹 Tầng 1: Mạng truy cập (Network Access Layer)**

* Tầng thấp nhất, xử lý **kết nối vật lý** và **truyền dữ liệu trong mạng cục bộ (LAN, WAN).**
* Tương ứng với tầng **vật lý và liên kết dữ liệu của OSI**.

📌 **Giao thức quan trọng:** ✅ **Ethernet** – Giao thức kết nối phổ biến trong mạng LAN.  
 ✅ **Token Ring** – Phương thức truyền dữ liệu cũ, ít dùng hiện nay.

💡 **Chịu trách nhiệm gửi dữ liệu qua cáp mạng, Wi-Fi hoặc các phương tiện vật lý khác.**

### **🔹 Tầng 2: Internet (Network Layer)**

* Xử lý **định tuyến (routing)** và **định địa chỉ IP** để gửi dữ liệu đến đúng đích.
* Tương ứng với tầng **mạng (Network Layer) của OSI**.

📌 **Giao thức quan trọng:** ✅ **IP (Internet Protocol)** – Xử lý địa chỉ IP và định tuyến.  
 ✅ **ARP (Address Resolution Protocol)** – Dịch địa chỉ IP thành địa chỉ MAC.  
 ✅ **ICMP (Internet Control Message Protocol)** – Kiểm tra kết nối (ping, traceroute).

💡 **Đây là tầng giúp các thiết bị trên Internet tìm thấy nhau và trao đổi dữ liệu.**

### **🔹 Tầng 3: vận chuyển (Transport Layer)**

* Đảm bảo dữ liệu được truyền đi một cách **tin cậy hoặc không tin cậy**, tùy vào giao thức.
* Tương ứng với tầng **giao vận (Transport Layer) của OSI**.

📌 **Giao thức quan trọng:** ✅ **TCP (Transmission Control Protocol)** – Truyền dữ liệu **tin cậy**, có kiểm tra lỗi.  
 ✅ **UDP (User Datagram Protocol)** – Truyền dữ liệu **không tin cậy**, nhanh hơn TCP.

💡 **TCP phù hợp cho email, web, tải file. UDP phù hợp cho video, VoIP, game online.**

### **🔹 Tầng 4: Ứng dụng (Application Layer)**

* Tầng cao nhất, xử lý giao tiếp giữa **người dùng và hệ thống mạng**.
* Kết hợp **3 tầng cao nhất của OSI (ứng dụng, trình diễn, phiên).**

📌 **Giao thức quan trọng:** ✅ **TELNET** – Kết nối từ xa đến hệ thống khác.  
 ✅ **FTP (File Transfer Protocol)** – Chuyển file qua mạng.  
 ✅ **SMTP (Simple Mail Transfer Protocol)** – Gửi email.  
 ✅ **DNS (Domain Name System)** – Chuyển đổi tên miền thành địa chỉ IP.  
 ✅ **SNMP (Simple Network Management Protocol)** – Giám sát thiết bị mạng.

💡 **Các giao thức này giúp duyệt web, gửi email, tải file, quản lý mạng, v.v.**

## **3️⃣ So sánh TCP và UDP**

🔹 **TCP**: Kết nối tin cậy, chậm hơn, có xác nhận dữ liệu (ACK).  
 🔹 **UDP**: Không tin cậy, nhanh hơn, không có xác nhận dữ liệu.

| **Đặc điểm** | **TCP** | **UDP** |
| --- | --- | --- |
| **Độ tin cậy** | Cao | Thấp |
| **Tốc độ** | Chậm hơn | Nhanh hơn |
| **Có kiểm tra lỗi không?** | Có | Không |
| **Ứng dụng** | Web, email, tải file | Video, game online, VoIP |

💡 **Dùng TCP khi cần độ tin cậy cao, dùng UDP khi cần tốc độ nhanh!**

## **4️⃣ Tại sao mô hình TCP/IP quan trọng?**

✅ **Là nền tảng của Internet, tất cả thiết bị mạng đều dựa trên TCP/IP.** ✅ **Cho phép các thiết bị khác nhau giao tiếp với nhau mà không phụ thuộc vào nhà sản xuất.** ✅ **Cung cấp hệ thống định tuyến linh hoạt giúp mở rộng mạng lưới toàn cầu.** ✅ **Hỗ trợ cả truyền tải tin cậy (TCP) và truyền tải tốc độ cao (UDP).**