1. Ознакомиться с руководящими документами:

<https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/382-rukovodyashchij-dokument-prikaz-predsedatelya-gostekhkomissii-rossii-ot-4-iyunya-1999-g-n-114>

Trang web này chứa một tài liệu do Chủ tịch Ủy ban Nhà nước về Tiêu chuẩn, Đo lường và Chất lượng Nga ký vào ngày 4 tháng 6 năm 1999. Tài liệu này quy định các yêu cầu về bảo vệ thông tin trong các hệ thống thông tin.

Tài liệu bao gồm các yêu cầu về:

* Khả năng bảo mật của hệ thống thông tin: Hệ thống thông tin phải được thiết kế và triển khai để bảo vệ thông tin khỏi các mối đe dọa như truy cập trái phép, thay đổi hoặc phá hủy.
* Quản lý bảo mật: Các tổ chức phải có các quy trình và thủ tục để quản lý bảo mật thông tin.
* An ninh vật lý: Các hệ thống thông tin phải được bảo vệ khỏi các mối đe dọa vật lý như cháy nổ, thiên tai và trộm cắp.
* An ninh mạng: Các hệ thống thông tin phải được bảo vệ khỏi các mối đe dọa mạng như tấn công từ chối dịch vụ, xâm nhập và phần mềm độc hại.

Tài liệu này là một tài liệu quan trọng đối với các tổ chức ở Nga cần bảo vệ thông tin của họ.

Dưới đây là tóm tắt ngắn gọn về các yêu cầu chính của tài liệu:

* Khả năng bảo mật của hệ thống thông tin:
  + Hệ thống thông tin phải được thiết kế và triển khai để bảo vệ thông tin khỏi các mối đe dọa như truy cập trái phép, thay đổi hoặc phá hủy.
  + Các hệ thống thông tin phải được sử dụng các biện pháp bảo mật thích hợp, chẳng hạn như mã hóa, xác thực và kiểm soát truy cập.
* Quản lý bảo mật:
  + Các tổ chức phải có các quy trình và thủ tục để quản lý bảo mật thông tin.
  + Các tổ chức phải có một người chịu trách nhiệm về bảo mật thông tin.
* An ninh vật lý:
  + Các hệ thống thông tin phải được bảo vệ khỏi các mối đe dọa vật lý như cháy nổ, thiên tai và trộm cắp.
  + Các hệ thống thông tin phải được đặt trong một môi trường an toàn.
* An ninh mạng:
  + Các hệ thống thông tin phải được bảo vệ khỏi các mối đe dọa mạng như tấn công từ chối dịch vụ, xâm nhập và phần mềm độc hại.
  + Các hệ thống thông tin phải được sử dụng các biện pháp bảo mật mạng thích hợp, chẳng hạn như tường lửa, phần mềm chống vi-rút và kiểm soát truy cập mạng.
* Tiêu đề: Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей.
* Ngày ban hành: 4 tháng 6 năm 1999
* Cơ quan ban hành: Ủy ban Nhà nước về an toàn thông tin (Gostekhkomissiya Rossii)
* Nội dung: Hướng dẫn về việc phân loại phần mềm bảo vệ thông tin theo mức độ kiểm soát sự không có các khả năng không khai báo.

Nội dung chi tiết của hướng dẫn bao gồm các phần sau:

* Mục đích: Hướng dẫn này được xây dựng nhằm mục đích thống nhất và nâng cao hiệu quả công tác phân loại phần mềm bảo vệ thông tin theo mức độ kiểm soát sự không có các khả năng không khai báo.
* Phạm vi áp dụng: Hướng dẫn này áp dụng cho tất cả các tổ chức, cá nhân tham gia hoạt động phân loại phần mềm bảo vệ thông tin theo mức độ kiểm soát sự không có các khả năng không khai báo.
* Các khái niệm cơ bản: Hướng dẫn này đưa ra các khái niệm cơ bản về phân loại phần mềm bảo vệ thông tin theo mức độ kiểm soát sự không có các khả năng không khai báo.
* Các nguyên tắc phân loại: Hướng dẫn này đưa ra các nguyên tắc phân loại phần mềm bảo vệ thông tin theo mức độ kiểm soát sự không có các khả năng không khai báo.
* Các phương pháp phân loại: Hướng dẫn này đưa ra các phương pháp phân loại phần mềm bảo vệ thông tin theo mức độ kiểm soát sự không có các khả năng không khai báo.
* Các mức độ kiểm soát: Hướng dẫn này đưa ra các mức độ kiểm soát sự không có các khả năng không khai báo.
* Trách nhiệm của các bên liên quan: Hướng dẫn này quy định trách nhiệm của các bên liên quan trong việc phân loại phần mềm bảo vệ thông tin theo mức độ kiểm soát sự không có các khả năng không khai báo.

Hướng dẫn này là một tài liệu quan trọng trong lĩnh vực an toàn thông tin, giúp các tổ chức, cá nhân phân loại phần mềm bảo vệ thông tin một cách chính xác và hiệu quả.

Dưới đây là một số nội dung quan trọng trong hướng dẫn:

* Khái niệm về khả năng không khai báo: Khả năng không khai báo là khả năng của phần mềm bảo vệ thông tin có thể được sử dụng để thực hiện các hành động trái phép mà không được khai báo trong tài liệu kỹ thuật của phần mềm.
* Mục đích của phân loại phần mềm bảo vệ thông tin theo mức độ kiểm soát sự không có các khả năng không khai báo: Phân loại phần mềm bảo vệ thông tin theo mức độ kiểm soát sự không có các khả năng không khai báo nhằm xác định mức độ an toàn của phần mềm đối với các khả năng không khai báo.
* Các mức độ kiểm soát sự không có các khả năng không khai báo: Có 5 mức độ kiểm soát sự không có các khả năng không khai báo, từ thấp nhất đến cao nhất là:
  + Mức độ C: Không yêu cầu kiểm soát
  + Mức độ D: Kiểm soát cơ bản
  + Mức độ E: Kiểm soát nâng cao
  + Mức độ F: Kiểm soát cao
  + Mức độ G: Kiểm soát rất cao

- Защита от НСД термины (<https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g3> ) + **Концепция защиты от НСД - Khái niệm bảo vệ chống truy cập trái phép**

Nội dung quan trọng trong trang web https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g3 là quyết định số 136 của Chủ tịch Ủy ban Nhà nước về kỹ thuật điện tử Liên Xô (Gostekhkom USSR) về việc phê duyệt quy tắc bảo vệ thông tin bí mật nhà nước và thông tin được bảo vệ khác khỏi truy cập trái phép bằng phương tiện kỹ thuật. Quyết định này được ban hành vào ngày 30 tháng 3 năm 1992 và vẫn có hiệu lực cho đến ngày nay.

Quyết định quy định các yêu cầu đối với các hệ thống bảo vệ thông tin bí mật nhà nước và thông tin được bảo vệ khác khỏi truy cập trái phép bằng phương tiện kỹ thuật. Các yêu cầu này bao gồm:

* Các hệ thống bảo vệ phải được thiết kế và lắp đặt sao cho ngăn chặn việc truy cập trái phép vào thông tin được bảo vệ.
* Các hệ thống bảo vệ phải được bảo trì và kiểm tra thường xuyên để đảm bảo hiệu quả hoạt động.
* Các nhân viên vận hành hệ thống bảo vệ phải được đào tạo về cách sử dụng và bảo vệ hệ thống.

Quyết định cũng quy định các trách nhiệm của các tổ chức và cá nhân trong việc bảo vệ thông tin bí mật nhà nước và thông tin được bảo vệ khác. Các tổ chức và cá nhân có trách nhiệm:

* Đảm bảo rằng thông tin được bảo vệ được lưu trữ và xử lý trong các hệ thống bảo vệ phù hợp.
* Tổ chức đào tạo cho nhân viên về cách bảo vệ thông tin bí mật nhà nước và thông tin được bảo vệ khác.
* Thực hiện các biện pháp cần thiết để ngăn chặn việc truy cập trái phép vào thông tin được bảo vệ.

Quyết định số 136 của Chủ tịch Ủy ban Nhà nước về kỹ thuật điện tử Liên Xô là một văn bản quan trọng trong hệ thống pháp luật của Nga về bảo vệ thông tin bí mật nhà nước và thông tin được bảo vệ khác. Quyết định này quy định các yêu cầu đối với các hệ thống bảo vệ thông tin và trách nhiệm của các tổ chức và cá nhân trong việc bảo vệ thông tin.

Dưới đây là một số nội dung quan trọng cụ thể trong quyết định:

* **Điều 1 quy định rằng mục đích của quyết định là để xác định các yêu cầu đối với các hệ thống bảo vệ thông tin bí mật nhà nước và thông tin được bảo vệ khác khỏi truy cập trái phép bằng phương tiện kỹ thuật.**
* **Điều 2 quy định rằng các hệ thống bảo vệ phải được thiết kế và lắp đặt sao cho ngăn chặn việc truy cập trái phép vào thông tin được bảo vệ.**
* **Điều 3 quy định rằng các hệ thống bảo vệ phải được bảo trì và kiểm tra thường xuyên để đảm bảo hiệu quả hoạt động.**
* **Điều 4 quy định rằng các nhân viên vận hành hệ thống bảo vệ phải được đào tạo về cách sử dụng và bảo vệ hệ thống.**
* **Điều 5 quy định các trách nhiệm của các tổ chức và cá nhân trong việc bảo vệ thông tin bí mật nhà nước và thông tin được bảo vệ khác.**

Quyết định số 136 của Chủ tịch Ủy ban Nhà nước về kỹ thuật điện tử Liên Xô là một văn bản quan trọng và cần thiết để bảo vệ thông tin bí mật nhà nước và thông tin được bảo vệ khác khỏi truy cập trái phép bằng phương tiện kỹ thuật.

-  **Автоматизированные системы. Защита от НСД - Hệ thống tự động. Bảo vệ chống truy cập trái phép**

[**https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g**](https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g)

* Quyết định số 24/TK-TL của Chủ tịch Ủy ban Nhà nước về tiêu chuẩn và đo lường Liên bang Nga ngày 30 tháng 3 năm 1992 về việc phê duyệt "Quy tắc bảo vệ thông tin bí mật nhà nước trong hệ thống thông tin máy tính"

Quyết định này phê duyệt "Quy tắc bảo vệ thông tin bí mật nhà nước trong hệ thống thông tin máy tính" (gọi tắt là "Quy tắc"). **Quy tắc quy định các yêu cầu bảo vệ thông tin bí mật nhà nước trong hệ thống thông tin máy tính, bao gồm:**

* Các yêu cầu đối với hệ thống thông tin máy tính
* Các yêu cầu đối với việc sử dụng, bảo quản và vận hành hệ thống thông tin máy tính
* Các biện pháp bảo vệ thông tin bí mật nhà nước
* Các yêu cầu đối với hệ thống thông tin máy tính

**Quy tắc quy định các yêu cầu đối với hệ thống thông tin máy tính bao gồm:**

* Hệ thống thông tin máy tính phải được thiết kế và xây dựng theo các yêu cầu bảo mật thông tin
* Hệ thống thông tin máy tính phải được trang bị các biện pháp bảo mật thông tin cần thiết
* Hệ thống thông tin máy tính phải được vận hành, bảo dưỡng và bảo trì theo đúng quy định
* Các yêu cầu đối với việc sử dụng, bảo quản và vận hành hệ thống thông tin máy tính

**Quy tắc quy định các yêu cầu đối với việc sử dụng, bảo quản và vận hành hệ thống thông tin máy tính bao gồm:**

* Chỉ những người được phép mới được sử dụng hệ thống thông tin máy tính
* Thông tin bí mật nhà nước phải được lưu trữ và vận chuyển an toàn
* Hệ thống thông tin máy tính phải được bảo vệ khỏi các tác nhân gây hại
* Các biện pháp bảo vệ thông tin bí mật nhà nước

**Quy tắc quy định các biện pháp bảo vệ thông tin bí mật nhà nước bao gồm:**

* Biện pháp kỹ thuật
* Biện pháp tổ chức
* Biện pháp hành chính

Quyết định số 24/TK-TL của Chủ tịch Ủy ban Nhà nước về tiêu chuẩn và đo lường Liên bang Nga ngày 30 tháng 3 năm 1992 là một văn bản pháp lý quan trọng quy định các yêu cầu bảo vệ thông tin bí mật nhà nước trong hệ thống thông tin máy tính. Quy tắc này có ý nghĩa quan trọng trong việc đảm bảo an ninh thông tin bí mật nhà nước.

Ngoài ra, trang web còn chứa các nội dung quan trọng khác như:

* Các văn bản pháp luật quy định về bảo vệ thông tin bí mật nhà nước
* Các quy định kỹ thuật về bảo vệ thông tin bí mật nhà nước
* Các tài liệu hướng dẫn về bảo vệ thông tin bí mật nhà nước

Các nội dung này cung cấp thông tin hữu ích cho các cá nhân và tổ chức cần bảo vệ thông tin bí mật nhà nước.

- **Средства вычислительной техники. Защита от НСД**

**Cơ sở máy tính. Bảo vệ chống truy cập trái phép**

**(**[**https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/385-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g2**](https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/385-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g2) **)**

**Yêu cầu quan trọng nhất của quyết định này là hệ thống bảo vệ thông tin kỹ thuật phải đảm bảo an ninh, tính toàn vẹn và tính bí mật của thông tin được bảo vệ. Hệ thống bảo vệ thông tin kỹ thuật phải bao gồm các biện pháp sau:**

* **Biện pháp kỹ thuật: sử dụng các thiết bị và công nghệ bảo vệ thông tin để ngăn chặn truy cập trái phép vào thông tin, thay đổi hoặc phá hủy thông tin.**
* **Biện pháp tổ chức: xây dựng các quy trình và thủ tục bảo vệ thông tin, đào tạo nhân viên về bảo vệ thông tin.**
* **Biện pháp hành chính: quy định các trách nhiệm và chế tài đối với việc vi phạm bảo vệ thông tin.**

Quyết định số 32 của Chủ tịch Ủy ban Kỹ thuật Nhà nước Nga ngày 30 tháng 3 năm 1992 là văn bản pháp lý quan trọng nhất về bảo vệ thông tin kỹ thuật ở Nga. Văn bản này quy định các yêu cầu cơ bản đối với hệ thống bảo vệ thông tin kỹ thuật, là cơ sở để xây dựng và triển khai các hệ thống bảo vệ thông tin ở Nga.

Ngoài ra, trang web này còn có chứa các tài liệu khác liên quan đến bảo vệ thông tin kỹ thuật ở Nga, bao gồm:

* Các tiêu chuẩn quốc gia về bảo vệ thông tin kỹ thuật.
* Các hướng dẫn thực hiện bảo vệ thông tin kỹ thuật.
* Các thông tin về các sản phẩm và dịch vụ bảo vệ thông tin kỹ thuật.

Trang web này là nguồn thông tin tham khảo hữu ích cho các tổ chức và cá nhân quan tâm đến bảo vệ thông tin kỹ thuật ở Nga.

- **СВТ. Межсетевые экраны. Защита от НСД (** [**https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyulya-1997-g**](https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyulya-1997-g) **) SVT. Tường lửa. Bảo vệ chống truy cập trái phép**

* Định nghĩa về межсетевой экран (МЭ): Là một thiết bị hoặc hệ thống phần mềm nằm ở ranh giới giữa hai hoặc nhiều mạng máy tính, có chức năng kiểm soát lưu lượng mạng giữa các mạng đó.
* Mục đích của МЭ: Bảo vệ các mạng máy tính khỏi các mối đe dọa từ bên ngoài, chẳng hạn như tấn công từ chối dịch vụ (DoS), tấn công từ chối dịch vụ phân tán (DDoS), virus, phần mềm độc hại, v.v.
* Các loại МЭ: Có thể phân loại МЭ theo nhiều tiêu chí khác nhau, chẳng hạn như theo kiến trúc, theo khả năng lọc, theo vị trí, v.v.
* Các nguyên tắc bảo mật của МЭ: МЭ cần phải đáp ứng các nguyên tắc bảo mật sau để có thể bảo vệ hiệu quả các mạng máy tính:
  + Nguyên tắc kiểm soát truy cập: МЭ phải kiểm soát truy cập của các gói tin từ các mạng khác vào mạng đang được bảo vệ.
  + Nguyên tắc xác thực: МЭ phải xác thực danh tính của các gói tin từ các mạng khác trước khi cho phép chúng truy cập vào mạng đang được bảo vệ.
  + Nguyên tắc mã hóa: МЭ có thể sử dụng mã hóa để bảo vệ dữ liệu được truyền qua mạng.
* Các phương pháp lọc của МЭ: МЭ có thể sử dụng các phương pháp lọc khác nhau để kiểm soát lưu lượng mạng, chẳng hạn như lọc theo địa chỉ IP, lọc theo cổng, lọc theo ứng dụng, v.v.
* Các chỉ tiêu đánh giá МЭ: Có thể sử dụng các chỉ tiêu sau để đánh giá khả năng bảo mật của МЭ:
  + Khả năng chống tấn công: МЭ phải có khả năng chống lại các cuộc tấn công từ bên ngoài.
  + Khả năng đáp ứng yêu cầu bảo mật: МЭ phải đáp ứng các yêu cầu bảo mật của hệ thống mạng.
  + Khả năng vận hành: МЭ phải dễ dàng vận hành và quản lý.
* Các yêu cầu đối với МЭ: Các МЭ cần phải đáp ứng các yêu cầu sau để có thể được sử dụng trong các hệ thống mạng quan trọng:
  + \*\*Được thiết kế và phát triển bởi các nhà cung cấp uy tín.
  + \*\*Được chứng nhận bởi các tổ chức uy tín.
  + \*\*Được cập nhật thường xuyên để vá các lỗ hổng bảo mật.

Ngoài ra, trang web còn cung cấp một số thông tin bổ sung về МЭ, chẳng hạn như:

* Các thuật ngữ liên quan đến МЭ:
  + Firewall: Một thuật ngữ tương đương với МЭ.
  + IPS (Intrusion Prevention System): Một hệ thống có khả năng phát hiện và ngăn chặn các cuộc tấn công mạng.
  + IDS (Intrusion Detection System): Một hệ thống có khả năng phát hiện các cuộc tấn công mạng.
* Các ứng dụng của МЭ:
  + \*\*Bảo vệ mạng máy tính khỏi các mối đe dọa từ bên ngoài.
  + \*\*Bảo vệ mạng máy tính khỏi các mối đe dọa từ bên trong.
  + \*\*Bảo vệ các ứng dụng web khỏi các cuộc tấn công.

Trang web này là một tài liệu tham khảo hữu ích cho các cá nhân và tổ chức quan tâm đến bảo mật mạng máy tính.

<https://habr.com/post/311978/>