# مقدمه‌ای بر پدافند غیرعامل

# درحوزه سیستم عامل

## فهرست

## مقدمه

سیستم‌عامل نقش «روح» را در پیکره سخت‌افزاری هر رایانه ایفا می‌نماید. کلیه ابعاد فنی زیرساخت فناوری اطلاعات و ارتباطات می‌تواند تحت الشعاع انتخاب یک سیستم‌عامل قرار گیرد. به عبارتی خشت اول و زیربنای توسعه نرم‌افزاری فناوری اطلاعات و ارتباطات، توسط سیستم‌عامل پایه‌گذاری می‌شود؛ از این‌رو جهت‌گیری به سمت ایجاد و استفاده از سیستم‌عامل ملی یک راهبرد مشخص و ضرورتی اجتناب ناپذیر جهت حفظ امنیت، استقلال، خوداتکایی و بهره‌وری اقتصادی درحوزه فناوری اطلاعات و ارتباطات می باشد.

# فصل ۱

## سیستم عامل و نقش آن در جامعه اطلاعاتی

یک سامانه رایانه‌ای از یک یا چند پردازنده، حافظه اصلی، حافظه های جانبی و دستگاه‌های ورودی و خروجی نظیر صفحه کلید، صفحه نمایش، چاپگرها و واسط‌های شبکه تشکیل شده است. این اجزا در کنار یکدیگر یک سامانه پیچیده را بوجود می‌آورند. نوشتن برنامه‌هایی که تمامی این عناصر را مدیریت و از آنها بطور صحیح، بهینه و کارآمد استفاده نماید، بسیار مشکل است. اگر هر برنامه‌نویس مجبور باشد با مفاهیم گسترده‌ای نظیر نحوه عملکرد دستگاه‌های ورودی و خروجی متفاوت آشنا باشد، بسیاری از برنامه‌ها هرگز نوشته نخواهند شد. به همین دلیل، از سال‌ها قبل بوضوح مشخص بود که می بایست ازطریق روش‌هایی برنامه‌نویسان و دیگر کاربران را از درگیر شدن با این پیچیدگی‌ها دور نگه داشت. تلاش‌های گسترده، منجر به ایجاد یک لایه نرم‌افزاری روی پیکره سامانه‌های رایانه‌ای شد؛ به این لایه که همه اجزای سامانه را کنترل و مدیریت نموده و بدین ترتیب کار توسعه برنامه‌ها را امکان‌پذیر می‌نماید، سیستم‌عامل گفته می‌شود.

## وظایف سیستم عامل:

بطور کلی در هر رایانه، حداقل یک سیستم‌عامل وجود دارد که مهم‌ترین برنامه نصب شده در رایانه می‌باشد و وظایف اصلی ذیل را برعهده دارد:

- راه‌اندازی، مدیریت و بکارگیری سخت‌افزار
- برقراری ارتباطات بین کاربر، نرم‌افزار و سخت‌افزار
- مدیریت و سازماندهی ارتباط با شبکه
- مدیریت و سازماندهی برنامه‌ها، پوشه‌ها و نرم‌افزارها

از دیگر وظایف سیستم‌عامل تشخیص خطاهای محتمل می‌باشد. این خطاها می‌تواند در پردازشگر، حافظه، دستگاه های ورودی/خروجی و یا در برنامه کاربر رخ دهد. سیستم‌عامل باید برای هر نوع خطا عکس‌العمل مناسبی نشان دهد.

استفاده از سیستم عامل های متن باز می تواند بعنوان گزینه ای مناسب بمنظور افزایش توان متخصصین داخلی جهت تولید محصولات بومی مطرح باشد.

## انواع سیستم عامل:

سیستم‌عامل‌ها از نظر کاربرد بصورت ذیل تقسیم‌بندی می‌شوند:

### سیستم‌عامل کاربری:

در رایانه های شخصی استفاده می‌شود.

### سیستم‌عامل کارگزار یا شبکه‌ای:

از کنترل کننده‌های واسط شبکه[۱] و نرم‌افزارهای سطح پایین بعنوان گرداننده[۲] استفاده می‌گردد و برنامه‌های خاصی با امکانات ویژه جهت دسترسی به سامانه‌ها یا فایل‌ها، از طریق شبکه‌های گسترده رایانه‌ای بکارگرفته می‌شود.

### سیستم‌عامل توزیع‌شده:

از چندین پردازنده و سیستم مجزا و در یک محیط شبکه‌ای اجرا می‌شود و در ابررایانه‌ها و کاربردهای پردازش موازی مورد استفاده قرار می‌گیرد.

### سیستم‌عامل بلادرنگ:

بمنظور کنترل ماشین آلات صنعتی، تجهیزات علمی و سامانه‌های صنعتی استفاده می‌گردد. امکانات محدودتر در بخش رابط کاربری و برنامه‌های کاربردی خاص منظوره از ویژگی‌های این نوع سیستم‌عامل

---

[۱] network card controller

[۲] driver

می‌باشد. پاسخگویی در زمان معین در این نوع سیستم عامل ها دارای اهمیت فراوانی می باشد.

## اهمیت بومی سازی سیستم عامل:

سیستم‌عامل نرم‌افزاری مبنایی است که بعنوان یک محصول کاربردی همراه با سخت‌افزار در اختیار استفاده کنندگان قرار می‌گیرد. با توجه به رشد جدی کاربران شبکه‌های اطلاع‌رسانی و اینترنت در کشور ما، ایجاد و توسعه یک سیستم‌عامل بومی، مسئله‌ای راهبردی می‌باشد. تصمیم در خصوص انتخاب سیستم‌عامل کلیه ابعاد فنی رایانه و فناوری اطلاعات را تحت‌الشعاع قرار می‌دهد.

سیستم‌عامل کلیه منابع رایانه را کنترل و مدیریت می‌نماید. هر برنامه کاربردی برای ذخیره‌سازی داده‌ها در یک فایل یا ارسال آن از طریق شبکه، باید از سیستم‌عامل استفاده نماید. چنانچه مشخصات طراحی سیستم عامل مورد استفاده در دسترس نباشد، اطلاع از عملکرد آن امکان‌پذیر نخواهد بود.

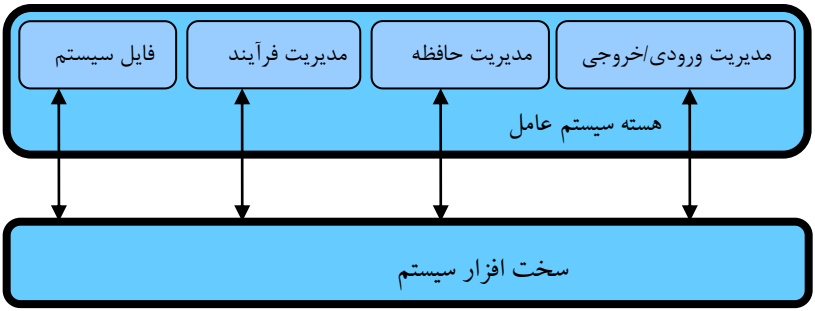
یک سیستم‌عامل بعنوان یک نرم‌افزار زیرساختی بدون انجام بررسی‌های لازم، نه از لحاظ امنیت دسترسی به اطلاعات و نه به لحاظ پایداری عملکرد، قابل اعتماد نخواهد بود. این عدم اطمینان، تهدید بزرگی است که خطرات و هزینه‌های اضافی را به دنبال خواهد داشت. از سوی دیگر ممکن است شرکت تولیدکننده از محصول خود برای آشفته کردن وضعیت بازار، گرفتار نمودن مشتری، بوجود آوردن وابستگی فنی و دسترسی محدود به اطلاعات دیجیتالی استفاده کند. در این حالت کاربران خود را در وضعیت بدی گرفتار می‌بینند که نمی‌توانند از آن نجات یابند و مجبورند برای دسترسی مجدد به اطلاعات خود که در قالب دیجیتالی ذخیره شده، محصول جدید همان تولیدکننده را خریداری نمایند.

تولیدکننده سیستم‌عامل می‌تواند، با وارد کردن برنامه‌های ویژه‌ای، باعث بوجودآمدن اختلال در عملکرد برنامه‌های کاربردی تولیدکنندگان دیگر شود. اینگونه رقابت ناعادلانه به نفع تولیدکنندگان سیستم‌عامل بوده و امکان بوجود آمدن امتیاز انحصاری را افزایش می‌دهد.

# فصل ۲

## معماری کلان سیستم عامل

شکل ذیل ساختار کلی یک سیستم‌عامل را نشان می‌دهد. در اینجا مؤلفه‌های سیستم‌عامل که در بخش هسته آن قرار می گیرند، نشان داده شده است. هر کدام از آن‌ها با استفاده از توابع خاصی با سخت‌افزار ارتباط برقرار می کنند. مشکل اصلی این معماری عدم وجود انعطاف لازم برای اعمال سیاست‌های امنیتی می‌باشد. این موضوع پیاده‌سازی مکانیزم‌های امنیتی را در حالت کلی مشکل می کند. بنابراین نیاز به وجود یک معماری امن و منعطف در طراحی سیستم‌عامل احساس می‌شود.




معماری کلان سیستم عامل

## مؤلفه‌های سیستم‌عامل

در نگاه کلی مؤلفه‌های اصلی سیستم‌عامل شامل بخش‌های ذیل می‌باشد:

### فایل‌سیستم[1]

وظایف اصلی فایل‌سیستم عبارتند از ایجاد و حذف فایل‌ها، ایجاد و حذف شاخه‌ها، انجام عملیات کپی، انتقال و تغییرات روی فایل‌ها و شاخه‌ها، ذخیره‌سازی و مدیریت قرارگیری فایل‌ها بر روی رسانه‌ها و مدیریت دسترسی‌های مختلف به فایل‌های مشترک. از نظر امنیتی، مدیریت و کنترل دسترسی به فایل‌ها مهم‌ترین بخش از وظایف سیستم‌عامل می‌باشد. تهدید مهم در مورد امنیت فایل‌سیستم استفاده از پروتکل‌های رمزنگاری آسیب پذیر یا غیرقابل اعتماد می‌باشد. بمنظور حفظ امنیت می‌بایست حتی‌الامکان از پروتکل‌های رمزنگاری طراحی و تولید شده داخلی در فایل‌سیستم استفاده شود. همچنین سیستم‌عامل باید دارای قابلیت تعریف مالکیت‌های جداگانه با سطوح دسترسی متفاوت و قابل کنترل برای هر فایل باشد. در این راستا کنترل نحوه دسترسی به این فایل‌ها بسیار مهم است؛ ضعف در قسمت کنترل دسترسی، تهدید بزرگی برای سامانه بشمار می‌آید.

### مدیریت فرآیندها[2]

بطور کلی در سیستم‌عامل‌ها، به یک برنامه در حال اجرا فرآیند گفته می‌شود. برای انجام هر کاری در یک رایانه باید یک یا چند فرآیند اجرا شود. با توجه به تعریف فرآیند و سیستم‌عامل، که وظیفه

---

[1] File System

[2] Process Management

مدیریت منابع سامانه را برعهده دارد؛ مدیریت فرآیندها یکی از مهم‌ترین و حساس‌ترین وظایف هر سیستم‌عامل می‌باشد. سیستم‌عامل با توجه به سیاست‌های مدیریتی خود، بر فرآیندها نظارت و مدیریت کرده و به آن‌ها اجازه اجرا شدن می‌دهد و یا از اجرای آن‌ها ممانعت می‌نماید. امکان اجرای فرآیندها توسط هر یک از مؤلفه‌ها و دسترسی بدون قید و شرط به منابع سخت‌افزاری سامانه، می‌تواند بسیار خطرناک باشد؛ یکی از خطراتی که سیستم‌عامل ناامن را تهدید می‌کند، از دست رفتن کنترل سامانه می‌باشد. در معماری‌های امن سیستم‌عامل، بخشی با نام کنترل امنیت به مؤلفه‌های سیستم‌عامل اضافه می‌شود که وظیفه بررسی فرآیندها و صدور مجوز اجرا برای آن‌ها را برعهده دارد. کنترل امنیت در این معماری‌ها خود از دو بخش تشکیل شده است:

۱. «کارگزار امنیتی» که حاوی سیاست‌های امنیتی سیستم‌عامل می‌باشد.

۲. «سازمان دهنده اشیاء» که پس از دریافت درخواست اجرای فرآیند، با مراجعه به کارگزار امنیتی امکان اجرا شدن فرآیند مذکور را بررسی کرده و در نهایت مجوز اجرا را برای آن فرآیند صادر و یا درخواست مذکور را رد می‌نماید.

## مدیریت حافظه[۱]

سیستم‌عامل در رابطه با مدیریت حافظه دو عملیات اساسی انجام می‌دهد :

۳. تخصیص حافظه مورد نیاز و اختصاصی به هر فرآیند برای اجرا

۴. استفاده از انواع حافظه در سامانه و مدیریت آن‌ها بمنظور اجرای فرآیندها با بالاترین سطح کارایی

تهدیدات اصلی مرتبط با مدیریت حافظه شامل عدم کنترل صحیح مقادیر ورودی‌های توابع سیستمی، فضاهای آدرس‌دهی و یا حجم اطلاعات ورودی می‌باشد که ممکن است سبب بروز مشکلات اساسی مانند سرریز شدن بافر[۲] شود. چنین مشکلاتی می‌تواند مقدمات برخی حملات به سیستم‌عامل را فراهم نماید.

## مدیریت ورودی‌ها و خروجی‌ها[۳]

ورودی/خروجی‌های یک سامانه رایانه‌ای از طریق تبادلات شبکه‌ای و یا دستگاه‌های جانبی امکان‌پذیر می‌باشد.

---

[۱] Memory Management

[۲] Buffer over flow

[۳] I/O Management

## معماری امن سیستم‌عامل

بطور کلی یک سیستم‌عامل امن نتیجه بهره‌گیری از معماری امن می‌باشد. عدم وجود یک معماری امن باعث می‌شود سیستم‌عامل از نظر امنیت و پایداری قابل اتکا نبوده و درنتیجه، احتمال نفوذ و وقوع تهدیدات امنیتی بالا می‌رود. در عین حال ساختار یک سیستم‌عامل باید فرآیندها و مکانیزم‌های لازم بمنظور پشتیبانی از انواع سیاست‌های امنیتی را داشته باشد زیرا با توجه به شرایط و محیط‌های مختلف، می بایست سیاست‌های امنیتی متفاوتی تعریف شوند؛ یک معماری مناسب باید با این سیاست‌ها تطبیق پذیر باشد و در عین حال توانایی پشتیبانی از سیاست‌های جدید را نیز داشته باشد، چرا که سیاست های امنیتی عموماً حالت ایستا ندارند.

با توجه به نکات فوق در معماری هدف می بایست یک سامانه مدیریتی که وظیفه بررسی فرآیندها و اعطای مجوز به آن‌ها برای اجرا شدن را بر عهده دارد به مجموعه مؤلفه‌های سیستم‌عامل اضافه گردد. در حقیقت با استفاده از این بخش که متشکل از دو مؤلفه کارگزار امنیتی و سازمان دهنده اشیاء است، می‌توان سیاست‌های امنیتی را پیاده‌سازی نمود.

## ارزیابی امنیتی سیستم عامل

در پی احساس نیاز به محصولات امن و پایدار، عرصه جدیدی برای طراحان و توسعه دهندگان سامانه‌های اطلاعاتی بوجود آمد. بخش بزرگی از شرکت‌های غیرمتخصص در زمینه امنیت، با مشاهده وضعیت موجود، اقدام به ارائه برخی محصولات امنیتی فاقد ارزش نمودند و کاربران آن محصولات با اطمینان به آن‌ها دچار مشکلات بزرگتری شدند.

خریداران و متقاضیان محصولات نرم‌افزاری، همواره نیازمندند که با استفاده از معیارهایی اطمینان حاصل نمایند که فرآیندهای طراحی، پیاده‌سازی و ارزیابی محصولاتی که قصد خرید و استفاده از آن‌ها را نموده‌اند، در چارچوبی کاملاً مشخص و استاندارد انجام شده است. لذا دولت‌ها سعی نمودند با ایجاد ساختارهایی به ارزیابی امنیتی محصولات و درجه‌بندی آن‌ها بپردازند.

بر اساس تحقیقات انجام گرفته در این راستا تعدادی استاندارد و معیار ارزیابی ارائه شده‌اند که فرآیندهای طراحی، پیاده‌سازی و ارزیابی محصولات نرم‌افزاری را از لحاظ امنیتی ارزیابی می‌کنند و به محصولات ارزیابی شده، سطحی از اطمینان را تخصیص می‌دهند. برخی از این استانداردها در این قسمت مورد بررسی قرارگرفته اند.

- **استاندارد TCSEC**

استاندارد TCSEC در سال ۱۹۸۵ توسط وزارت دفاع آمریکا برای اولین بار برای ارزیابی امنیتی محصولات نرم‌افزاری ارائه شد. استاندارد TCSEC پس از ارزیابی یک محصول، آن را از لحاظ امنیتی در یکی از سطوح اطمینان بخشی C۱، C۲، B۱، B۲، B۳ و A۱ قرار می‌دهد.

- **استاندارد ITSEC**

در سال ۱۹۹۰ کشورهای انگلیس، فرانسه و آلمان براساس معیار ارزیابی امنیتی TCSEC، معیاری برای ارزیابی امنیتی محصولات فناوری اطلاعات ارائه نمودند. پس از بررسی‌های فراوانی که توسط مجامع بین‌المللی بر روی معیار ارزیابی مذکور صورت پذیرفت، نسخه ۱.۲ این معیار توسط اتحادیه کشورهای اروپایی برای

بکارگیری عملی در زمینه ارزیابی امنیتی محصولات فناوری اطلاعات تهیه و به دنیا ارائه شد. این استاندارد در حقیقت تکمیل شده و توسعه یافته استاندارد TCSEC بوده و دارای ۶ کلاس ارزیابی می‌باشد.

### استاندارد CC

پس از استاندارد ITSEC، اولین نسخه از معیار ارزیابی CC در سال ۱۹۹۴ به دنیا عرضه شد. این معیار ارزیابی نیز برپایه TCSEC، ITSEC و تعدادی معیار ارزیابی بومی‌سازی شده دیگر نظیر CTCPEC، بنیان گرفته بود.

مؤسسه استانداردهای بین‌المللی ISO در سال ۱۹۹۰ کار خود را برای تدوین استانداردهای ارزیابی امنیت در بازار صنعت فناوری اطلاعات شروع کرد که نتیجه آن ارائه ۱۵۴۰۸ ISO بود. در حقیقت CC پس از گذراندن مراحلی، از سوی مؤسسه استانداردسازی ایزو به عنوان استانداردی برای ارزیابی امنیتی محصولات نرم‌افزاری شناخته شد و از آن پس با نام ۱۵۴۰۸ ISO مطرح گردید. تعدادی از مفاهیم پایه‌ای که در استاندارد CC وجود دارند عبارتند از:

- هدف مورد ارزیابی(TOE[۱]):

  محصول یا خدماتی است که با استفاده از این استاندارد می‌خواهیم آن را از لحاظ امنیتی مورد ارزیابی قرار دهیم.

- هدف امنیتی (ST[۲]):

---

[۱] Target of Evaluation

[۲] Security Target

مشخص‌کننده انتظارات امنیتی از محصول مورد نظر

- نمایه حفاظتی (PP[1]):

مشخص‌کننده نیازمندی‌های امنیتی به زبان سطح بالا

- سطوح اطمینان بخشی ارزیابی (EAL[2]):

مشخص می‌کند که در ارزیابی انجام شده، چه میزان از نیازمندی‌های اطمینان بخشی برآورده شده‌است.

## مقایسه استانداردهای امنیتی

در جدول ذیل استانداردهای معرفی شده در بخش‌های گذشته از حوزه های مختلف مورد مقایسه و بررسی قرار گرفته است.[سند ملاحظات پدافند غیرعامل در طراحی و تولید سیستم عامل بومی-۱۳۸۶]

بررسی و مقایسه استانداردهای امنیت نرم افزار

| حوزه / استاندارد | ISO۱۵٤۰۸(CC) | ITSEC |
|---|---|---|
| پذیرش توسط مؤسسه‌های استاندارد بین‌المللی معتبر( نظیر ISO و IEEE ) | خوب | متوسط |
| میزان بکارگیری توسط طراحان، تولیدکنندگان و خریداران | زیاد و در حال افزایش | متوسط |
| میزان انطباق با نیازهای روز جامعه اطلاعاتی | زیاد | متوسط |
| انعطاف پذیری با کاربردهای متنوع | زیاد | متوسط |

[1] Protection Profile

[2] Evaluation Assurance Level

## پیشنهاد بومی‌سازی استانداردهای ارزیابی امنیتی

همان‌طور که در تعریف استاندارد CC گفته شد، یکی از مفاهیم پایه‌ای این استاندارد، نمایه حفاظتی است که مصرف کننده[1] توسط آن، نیازمندی‌های خود را بیان می‌کند. به عبارت دیگر، استاندارد CC به گونه‌ای طراحی شده است که قابلیت بومی‌سازی شدن در آن به صورت نهادینه قرار گرفته است و کارشناسان می‌توانند با تعریف نمایه حفاظتی و سطوح امنیتی براساس نیازهای خود، این استاندارد را بومی کنند.

با تعریف نمایه حفاظتی جدید بر اساس نیازهای امنیتی کشور، بخش زیادی از فعالیت بومی‌سازی استاندارد سیستم‌عامل انجام خواهد شد.

ارزیابی سیستم‌عامل از لحاظ امنیتی توسط مراکز مشخصی صورت می‌گیرد، این مراکز برای ارزیابی امنیتی سیستم‌عامل باید کد منبع سیستم‌عامل و جزئیات مربوط به طراحی و پیاده‌سازی آن را در اختیار داشته باشند. در صورتی که چنین مراکز ارزیابی در داخل کشور وجود نداشته باشد، برای ارزیابی امنیتی سیستم‌عامل ملی ناچار خواهیم شد که تمامی اطلاعات و جزئیات طراحی و پیاده‌سازی آن را در اختیار مراکزی که در سایر کشورها قرار دارند، بگذاریم؛ که این امر تهدیدات فراوانی را برای کشور بهمراه خواهد داشت و به هیچ وجه توصیه نمی‌شود. کشور یا مرکز مقصد به دلیل موقعیت استراتژیک ایران در منطقه و با توجه به موقعیت جنگ تمام عیار اطلاعاتی فعلی، با دانستن اطلاعات فنی سیستم‌عامل ملی و نقاط آسیب‌پذیر آن می‌تواند برنامه‌های تخریبی را در حوزه‌های مختلف به اجرا درآورده و

[1] خریدار سیستم عامل یا فرد یا نهادی که متقاضی سیستم عامل است.

زمینه تهدید تمامی زیرساخت‌های اطلاعاتی کشور را در شرایط خاص فراهم نماید. دارندگان کد می‌توانند نسبت به انجام حملات مختل کننده خدمات فناوری اطلاعات اقدام کرده و اطلاعات زیرساخت‌ها را تخریب نمایند.

با توجه به تهدیداتی که در این زمینه متوجه کشور خواهد شد، ضروری است که مرکزی برای ارزیابی امنیتی سیستم‌عامل در داخل کشور راه‌اندازی شود.

در صورت استفاده از سیستم‌عامل‌های کدبسته، تضمینی برای عدم دستیابی تولیدکننده سیستم‌عامل به اطلاعات شخصی و محرمانه ذخیره شده روی رایانه، وجود ندارد.

# فصل ۳

## ملاحظات پدافند غیرعامل در طراحی سیستم عامل

در این فصل از کتابچه به بیان برخی از مهمترین ملاحظات پدافند غیرعامل در حوزه طراحی سیستم عامل خواهیم پرداخت:

- کد منبع سیستم‌عامل مورد استفاده در کشور بایستی در دسترس متخصصان ذیربط قرار داشته باشد و مورد بررسی قرار گیرد. عدم دسترسی به کد سامانه و عدم امکان بررسی باعث می‌شود تا تولیدکننده سیستم‌عامل بتواند با وارد نمودن برنامه‌های ویژه‌ای در سامانه هدف نفوذ کرده و موجب جاسوسی، شنود هوشمندانه و بوجود آمدن اختلال در عملکرد برنامه‌های کاربردی شود.
- انجام بررسی‌های لازم بر روی کد منبع سیستم‌عامل از لحاظ امنیت دسترسی به اطلاعات و ثبات عملکرد در آزمایشگاه‌های امنیت سیستم عامل در داخل کشور ضروری است.
- طراحی و استفاده از یک معماری امن برای داشتن یک سیستم‌عامل امن ضروری است.

- در طراحی و پیاده‌سازی سیستم‌عامل باید یک سامانه ثبت وقایع با قابلیت ثبت نوع درخواست، شناسه کاربر و اجرای برنامه وجود داشته باشد.
- در فایل‌سیستم امن می‌بایست قابلیت کنترل مجوز دسترسی در خصوص سطح دسترسی، مالکیت و مجوزهای اعمال تغییرات روی فایل‌ها وجود داشته باشد.
- از فایل‌های اصلی حاوی اطلاعات مهم کاربری مانند کلمه عبور باید حفاظت به عمل آورد و تنها کاربر ریشه به آن‌ها دسترسی داشته باشد.
- می بایست مکانیزم‌های کنترلی خاص در طراحی سامانه مدیریت فرآیند، ایجاد و پیاده‌سازی گردد؛ بطوریکه فرآیندهای مخاطره آمیز مسدود و اطلاعات آنها و کاربران اجرا کننده ثبت و گزارش شود.
- سرویس‌های غیر ضرور، هنگام ارائه محصول به کاربر نهایی می‌بایست غیرفعال باشند.
- در دستگاه‌های ورودی/خروجی برای ایجاد مکانیزم‌های محافظتی باید برای دسترسی هر کاربر، رمز ورود تقاضا شده و متناسب با هر سطح دسترسی، امکانات معینی از سامانه در اختیار کاربر قرار گیرد.
- سیستم عامل ملی می‌بایست دارای سطح قابل قبولی از امنیت ذاتی در برابر نرم‌افزارهای مخرب باشد، این نوع از امنیت بیشتر در سیستم‌عامل‌های چند کاربره مطرح است.
- در طراحی سیستم‌عامل ملی می‌بایست امکانات و قابلیت‌های لازم جهت پشتیبانی از استانداردها و پروتکل‌های امن‌سازی سیستم‌عامل پیش بینی شود.
- برای هر سیستم‌عامل مورد استفاده در مراکز کشور باید نمایه حفاظتی متناسب با اهمیت آن مرکز تعریف شود و سیستم‌عامل بکارگیری شده از منظر امنیتی توسط یک نهاد معتبر و مطمئن، ارزیابی و تائید گردد.

- سیستم‌عامل از نظر تداوم اجرا می‌بایست متناسب باشد؛ به بیان دیگر در شرایط از کار افتادن برخی از قسمت‌های سامانه، سیستم‌عامل مورد استفاده باید قادر باشد توابع و عملکردهای اصلی سامانه را همچنان قابل استفاده نگه‌دارد.
- طراحی سیستم‌عامل باید به ترتیبی باشد که بسامد بروز شکست یا خطای ناشی از عیوب سیستم‌عامل تا حد ممکن پایین باشد.
- عواملی همچون توانایی بازگرداندن خدمات سیستم‌عامل به سطح کارایی تعیین شده، توانایی بازگرداندن داده‌هایی که مستقیماً تحت تأثیر خرابی بوده‌اند و زمان لازم و تلاش مورد نیاز برای انجام این کارها؛ تاثیر بسزایی در افزایش زمان برپابودن[۱] سامانه می‌گذارد، مجموعه این نکات همواره می‌بایست جزء اصلی‌ترین مؤلفه‌های طراحی یا انتخاب یک سیستم‌عامل قرار گیرد.
- قابلیت پایداری سیستم‌عامل شامل قابلیت تداوم اجرا[۲]، تحمل در برابر عیب و خطای ناشی از طراحی سامانه[۳]، میزان بلوغ[۴] و قابلیت بازگرداندن[۵] داده‌ها و خدمات به حالت عادی (مورد اشاره در ملاحظات قبل)، عاملی کلیدی محسوب می‌شود که باید مورد توجه قرار گیرد.
- پیش از استفاده می‌بایست میزان کارایی سیستم‌عامل هدف از نظر زمان و مدیریت منابع در یک آزمایشگاه مجهز و مطمئن، ارزیابی و تعیین شود.

---

[۱] Uptime

[۲] Survivability

[۳] Fault Tolerance

[۴] Maturity

[۵] Recoverability

- بروزرسانی منظم، دقیق و متناسب با اهمیت کارکردی سیستم‌عامل، فرآیندی است که مرتباً باید انجام پذیرد.
- تشکیل تیم‌های متعدد فنی، زبده و مجرب برای ارائه خدمات سریع، صحیح و مطمئن به سیستم‌عامل‌های مستقر در مراکز کشور جهت تضمین پایداری کل سامانه کامپیوتری و تشکیل مراکز پشتیبانی ضروری است.
- ویژگی‌های قابلیت بکارگیری (شامل چگونگی نصب و راه‌اندازی، میزان کاربرپسندی[1]، میزان شناسایی سخت‌افزارهای کامپیوترهای سازمان، میزان یکپارچگی و سازگاری با بستر سخت‌افزاری موجود، امکانات نرم‌افزاری همراه و یکپارچه با سیستم‌عامل، تعداد و نوع قالب‌ها و پروتکل‌های استاندارد پشتیبانی شده توسط سیستم‌عامل) در طراحی، پیاده‌سازی و ارزیابی سیستم‌عامل کامپیوترهای شخصی سازمان‌ها و مراکز مهم باید مورد توجه خاص قرار گیرد.
- استفاده از قالب فایل‌ها و پروتکل‌های ارتباطی استاندارد یا استانداردسازی آن‌ها، به منظور کاهش هزینه‌ها، افزایش قابلیت همکاری سامانه‌ها، افزایش کیفیت خدمات و نهایتاً نظارت بر حسن عملکرد سامانه‌ها، لازم است.

---

[1] User-Friendly

# پیوست ۱

## مسیر تحول سیستم عامل ها

اهم اقدامات انجام شده در زمینه نگارش و توسعه سیستم‌های عامل و رخدادهای مربوطه در داخل و خارج از کشور بشرح ذیل ارائه می‌گردد:

خانواده UNICS  خانواده Windows  خانواده Mac  خانواده Linux

| تاریخ | اقدام/رخداد |
|---|---|
| ۱۹۶۸ | شروع پروژه تولید سیستم‌عامل چند کاربره توسط آزمایشگاه Bell در شرکت AT&T |
| ۱۹۶۹ | تولید سیستم‌عامل تک کاربره UNICS[۱] |

[۱] Uniplexed Information and Computing System

| تاریخ | اقدام/رخداد |
|---|---|
| ۱۹۷۰ | اضافه نمودن ابزاری ابتدایی به UNICS جهت حمایت از چند پردازنده |
| ۱۹۷۱ | نگارش اولین نسخهٔ یونیکس به زبان اسمبلی در انحصار آزمایشگاه Bell در شرکت AT&T |
| ۱۹۷۲ | انتشار نسخهٔ دوم یونیکس در ماه ژوئن به زبان B (مبتنی بر زبان BCPL[۱]) |
| ۱۹۷۳ | بازنویسی و انتشار نسخه سوم یونیکس به زبان C |
| ۱۹۷۵ | انتشار نسخهٔ ششم یونیکس[۲] |
| ۱۹۸۱ | انتشار سیستم‌عامل تک کاربره DOS[۳] توسط شرکت مایکروسافت |
| ۱۹۸۴ | انتشار سیستم‌عامل Mac توسط شرکت اپل |

[۱] Basic Combined Programming Language

[۲] این نسخه برای اولین بار خارج از AT&T مورد استفاده قرار گرفت. طبق قوانین فدرال، شرکت AT&T Bell از فروش سخت‌افزار و نرم‌افزار منع شده بود، به همین دلیل، یونیکس را تحت حق کپی آموزشی به دانشگاه‌ها و موسسات آموزشی پیشنهاد نمود.

[۳] Disk Operating System

| تاریخ | اقدام/رخداد |
| --- | --- |
| ۱۹۸۵ | ارائه سیستم‌عامل ویندوز نسخه۱ توسط شرکت مایکروسافت |
| ۱۹۹۲ | تولید سیستم‌عامل ویندوز نسخه ۳.۱ توسط شرکت مایکروسافت |
| ۱۹۹۰ | انتشار سیستم۴ (نسخهٔ پیشرفته‌ای از یونیکس) |
| ۱۹۹۱ | انتشار نسخهٔ ۰.۱۱ لینوکس در سال ۱۹۹۱ روی شبکهٔ اینترنت |
| ۱۹۹۳ | ارائه سیستم عامل BSD توسط شرکت AT&T |
| ۱۹۹۳ | تولید سیستم‌عامل ویندوز NT۴ توسط شرکت مایکروسافت |
| ۱۹۹۳ | آغاز پروژه دبیان و ارائه توزیع لینوکس آن توسط شرکت دبیان |
| ۱۹۹۴ | آغاز پروژه لینوکس ردهت و عرضه توزیع آن توسط این شرکت |

| تاریخ | اقدام/رخداد |
| --- | --- |
| ۱۹۹۴ | آغاز پروژه لینوکس سوزه و عرضه توزیع آن توسط شرکت ناول |
| ۱۹۹۵ | تولید سیستم‌عامل ویندوز ۹۵ توسط شرکت مایکروسافت |
| ۱۹۹۸ | تولید سیستم‌عامل ویندوز ۹۸ توسط شرکت مایکروسافت |
| ۲۰۰۰ | تولید سیستم‌عامل Mac X توسط شرکت اپل |
| ۲۰۰۰ | تولید سیستم‌عامل ویندوز ۲۰۰۰ توسط شرکت مایکروسافت |
| ۲۰۰۰ | تولید سیستم‌عامل ویندوز ME توسط شرکت مایکروسافت |
| ۲۰۰۱ | تولید سیستم‌عامل ویندوز XP توسط شرکت مایکروسافت |

| تاریخ | اقدام/رخداد |
| --- | --- |
| ۲۰۰۱ | پیشنهاد فارسی سازی لینوکس به شورای انفورماتیک از سوی مرکز فناوری اطلاعات شریف |
| ۲۰۰۲ | شروع طرح ملی لینوکس فارسی توسط مرکز فناوری اطلاعات شریف- شورای عالی انفورماتیک |
| ۲۰۰۳ | تولید سیستم‌عامل ویندوز ۲۰۰۳ توسط شرکت مایکروسافت |
| ۲۰۰۳ | آغاز پروژه لینوکس فدورا و عرضه توزیع آن توسط شرکت ردهت |
| ۲۰۰۴ | آغاز پروژه لینوکس اوبونتو و عرضه توزیع آن توسط شرکت کانونیکا |
| ۲۰۰۴ | ارائه نسخه اولین توزیع لینوکس فارسی (شبدیکس) از سوی مرکز فناوری اطلاعات شریف و شورای عالی انفورماتیک |
| ۲۰۰۵ | آغاز پروژه کارآمد و ارائه توزیع لینوکس آن توسط شرکت داده پردازی |

| تاریخ | اقدام/رخداد |
| --- | --- |
| ۲۰۰۵ | آغاز پروژه پارسیکس و ارائه توزیع لینوکس آن مبتنی بر توزیع دبیان توسط آلن باغومیان |
| ۲۰۰۶ | ارائه توزیع لینوکس شریف توسط شرکت فارسی وب شریف |
| ۲۰۰۶ | تولید سیستم‌عامل ویندوز ویستا توسط شرکت مایکروسافت |
| ۲۰۰۸ | تولید سیستم‌عامل ویندوز سرور ۲۰۰۸ توسط شرکت مایکروسافت |
| ۲۰۰۹ | تولید سیستم‌عامل ویندوز ۷ توسط شرکت مایکروسافت |
| ۲۰۰۹ | ارائه توزیع لینوکس کوثر با حمایت انجمن صنفی کاربران نرم افزارهای آزاد/متن باز |