

امنیت فضای مجازی و دفاع الکترونیکی

جلسه نهم

فصل دوم : امنیت فضای مجازی

۹۴/۱۰/۲۴

خلاصه : فصل اول: کلیات و مفاهیم

- ۱,۱. فضای مجازی
- ۱,۲. مفهوم امنیت، مؤلفات و اقسام آن
 - ۱,۲,۱. ضرورت امنیت
 - ۱,۲,۲. معنای لغوی امنیت
 - ۱,۲,۳. معنای اصطلاحی امنیت
 - ۱,۲,۴. امنیت ملی و امنیت‌های مضاف
 - ۱,۲,۵. سیر تطور مفهوم امنیت ملی
 - ۱,۲,۶. مؤلفات امنیت ملی
 - ۱,۲,۷. اقدامات تأمینی برای امنیت ملی

فصل دوم: «امنیت فضای مجازی»

- ۲.۱. تعریف امنیت فضای مجازی
- ۲.۲. تهدیدهای امنیتی فضای مجازی
- ۲.۳. تدبیرهای امنیتی فضای مجازی

تعریف اصطلاحی امنیت:

حفاظت و مقاومت هر دارایی ارزشمند و آسیب‌پذیر در برابر تهدیدها

تعریف امنیت فضای مجازی: (امنیت رایانه / امنیت فناوری اطلاعات):

«حفاظت و مقاومت سخت‌افزارها، نرم‌افزارها، شبکه، اطلاعات، خدمات،

و کاربران در برابر تهدیدهای فضای مجازی.»

تعریف دارایی‌های فضای مجازی:

۱- سخت‌افزارها

ابزارهایی ملموس هستند شامل رایانه‌ها، چاپگرها، تلفن‌ها، نمایشگرها، سرورها، سونیچ‌ها، آنتن‌های ارتباطاتی، و اجزاء آنها و مانند آن که به صورت مکانیکی، مغناطیسی، الکترونیکی و یا الکتریکی کار می‌کنند.

تعریف دارایی‌های فضای مجازی:

مثال: قفل الکترونیکی درب اتاق هتل‌ها، سخت‌افزاری است که با استفاده از یک کارت مغناطیسی که از روی برنامه‌ای رایانه‌ای شماره اتاق مربوط به آن داده شده است، و با استفاده از نیروی مکانیکی که با اتصال به نیروی الکتریکی حرکت می‌کند، درب اتاق مربوط را باز می‌کند.



تعریف دارایی‌های فضای مجازی:

۲- نرم‌افزارها

برنامه‌هایی که روی سخت‌افزارها راه‌اندازی می‌شوند تا عملیات یک سخت‌افزار را هدایت کنند یا کاربرد اطلاعات یا خدمات را ساماندهی کنند. مثال :

۱- سیستم‌های عامل برای مدیریت و هدایت عملیات یک سخت‌افزار طراحی می‌شوند مانند سیستم عامل ویندوز یا سیستم عامل اپل یا سیستم عامل اندروید

۲- برنامه‌های کاربردی برای مدیریت اطلاعات و خدمات نوشته می‌شوند مانند برنامه‌های نور و برنامه‌های شرکت مایکروسافت و گشتارهای شبکه مثل کروم، اینترنت اکسپلورر و فایرفاکس.

تعریف دارایی‌های فضای مجازی:

۳- شبکه

طرق ارتباط و اتصال بین سخت‌افزارها برای مبادله اطلاعات و خدمات به صورت بی‌سیم یا باسیم
مثال:

شبکه اینترنت،

شبکه‌های زیرساختی کشور،

شبکه تلفن‌های معمولی و همراه،

شبکه‌های اینترنتی سازمانی و ساختمانی،

شبکه سیم مسی،

شبکه فیبر نوری،

شبکه وای فای شهری،

شبکه بی‌سیم

و ...

تعریف دارایی‌های فضای مجازی:

۳- شبکه

شبکه شامل شبکه اینترنت، شبکه‌های زیرساختی کشور، شبکه تلفن‌های معمولی و همراه، شبکه‌های اینترنتی سازمانی و ساختمانی، شبکه سیم مسی، شبکه فیبر نوری، شبکه وای فای شهری، شبکه بی‌سیم و مانند آن می‌شود.

تعریف دارایی‌های فضای مجازی:

۳- شبکه

در برخی تعاریف شبکه را بخشی از سخت‌افزارها در نظر می‌گیرند ولی ما در اینجا به دو دلیل آن را از سخت‌افزار جدا کردیم

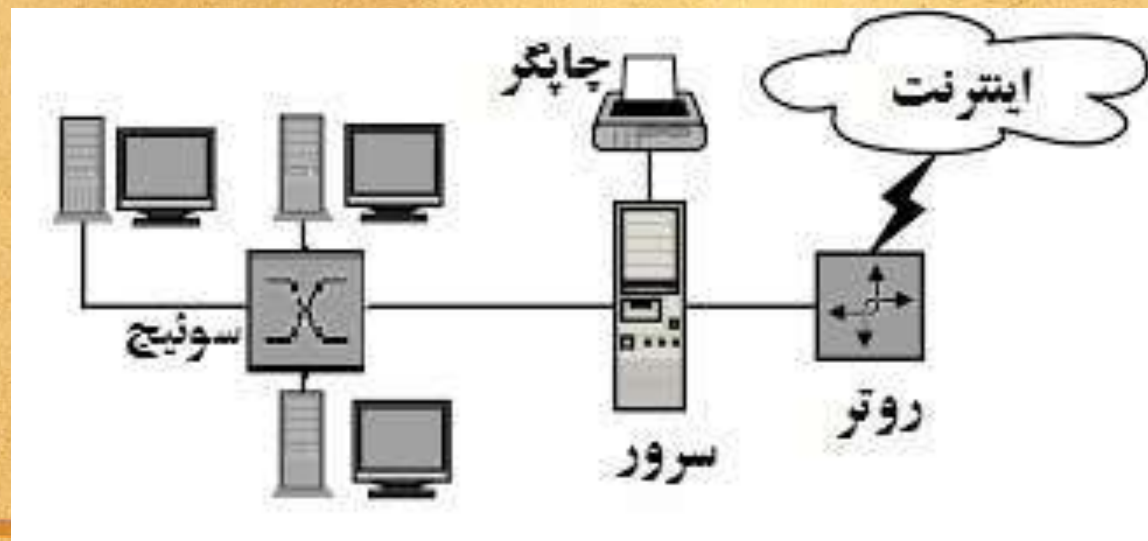
اول این که این رشته دانشگاهی مستقل از سخت‌افزار و نرم‌افزار است و مباحث سخت‌افزاری و مباحثی نرم‌افزاری را هم شامل می‌شود.

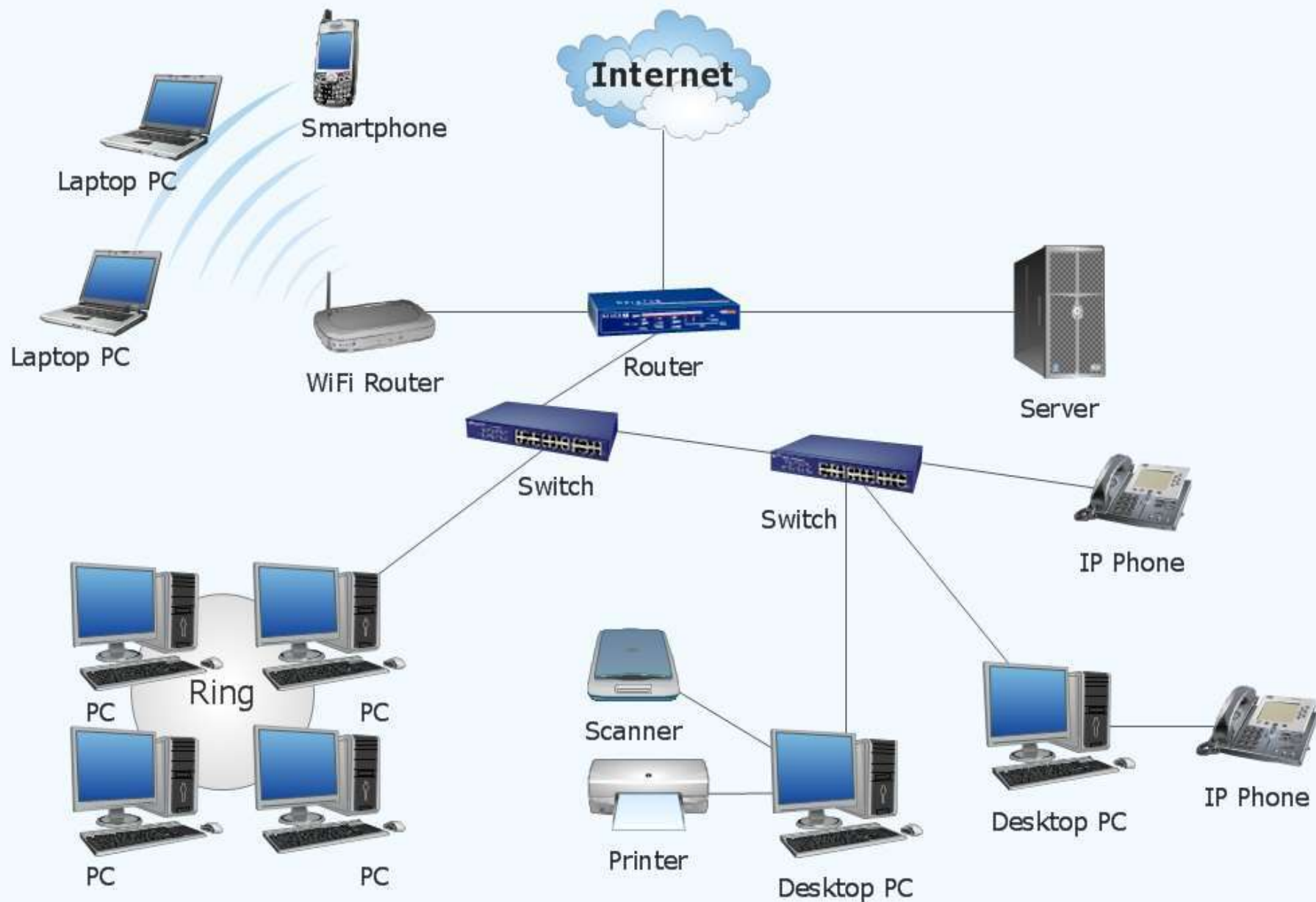
دوم این که امنیت شبکه مستقل از امنیت سخت‌افزار و نرم‌افزار دارای مباحثی مهم و مستقل است.

یک شبکه پیچیده معمولاً از چند دستگاه رایانه به همراه تعدادی سوئیچ و روتر تشکیل شده که وظیفه ارسال بسته‌های اطلاعاتی و اتصال رایانه‌ها به یکدیگر و به شبکه‌های دیگر مثل شبکه اینترنت برعهده دارند.

سوئیچ‌ها وظیفه انتقال بسته‌های اطلاعاتی را از یک رایانه مشخص به رایانه مشخص دیگر برعهده دارند.

روترها که معمولاً واسطه بین دو شبکه است، وظیفه انتقال بسته‌های اطلاعاتی را به شبکه‌های دیگر برعهده دارند مثلاً بسته اطلاعاتی را از یک شبکه داخلی به شبکه اینترنت می‌فرستد.





۴- اطلاعات =

کلیه داده‌هایی که مراحل مختلف فرایندهای رایانه‌ای به صورت ورودی، خروجی، ذخیره‌ای یا انتقالی روی آنها صورت می‌گیرد و به کمک سخت‌افزارها و نرم‌افزارها قابل پردازشند.

۵- خدمات =

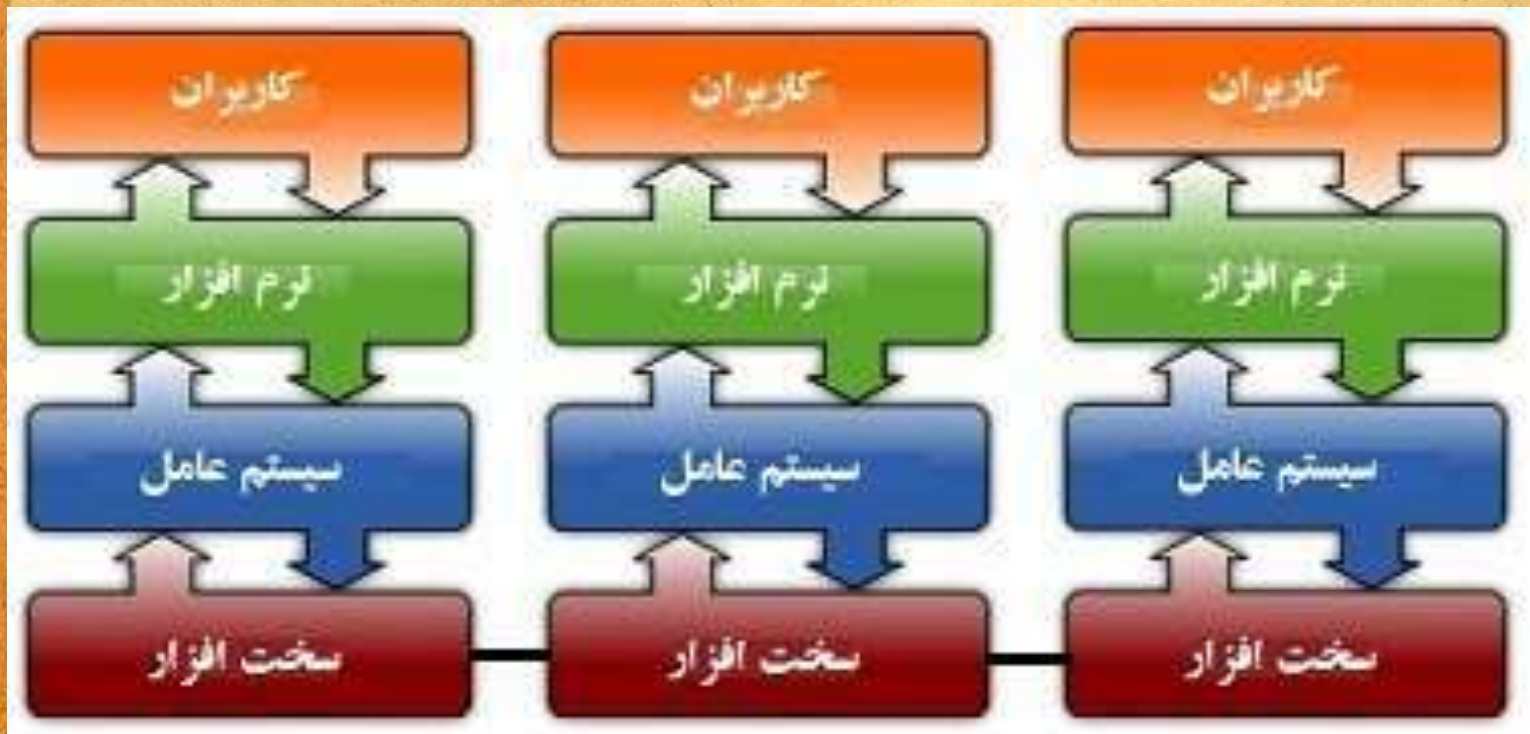
هر فعالیت انسانی که برای مساعدت به دیگری و با استفاده از سخت‌افزارها و نرم‌افزارها انجام می‌گیرد.

۶- کاربران =

کسانی که از اطلاعات و خدمات عرضه شده با این سخت‌افزارها، نرم‌افزارها و یا شبکه‌ها استفاده می‌کنند.

امنیت فضای مجازی

هر چه اعتماد جوامع به فضای مجازی بیشتر شود، اهمیت امنیت فضای مجازی بیشتر می‌شود و باید به تهدیدهایی که امنیت را در فضای مجازی به خطر می‌اندازد توجه جدی‌تری کرد. اینک بینیم چه نوع تهدیدهایی در فضای مجازی وجود دارند.



۲.۲. تهدیدهای امنیتی فضای مجازی

گفتیم که دارایی‌های شش‌گانه در حوزه امنیت عبارتند از سخت‌افزارها، نرم‌افزارها، شبکه، اطلاعات، خدمات و کاربران. مهمترین تهدیدهایی که ممکن است مربوطه به یک یا چند مورد از این شش حوزه باشند، عبارتند از: سرقت، دست‌رسی، جعل، تغییر، تخریب، و اخلال به صورت نامجاز صورت گرفته و ممکن است عمدی یا سهوی باشند.

اگر برخی از این افعال بر روی یک یا چند مورد از آن دارایی‌های شش گانه تحقق یابد امنیت فضای مجازی نقض شده است. حاصل تقاطع هر یک از این دارایی‌های شش گانه در هر یک از تهدیدهای مذکور ماتریسی از موضوعات را بدست می‌دهد که باید در هر خانه آن مباحث لازم فقهی را بررسی کرد.

امنیت فضای مجازی

اخلال	تخریب	تغییر	جعل	دسترسی	سرقت	
						سخت افزار
						نرم افزار
						شبکه
						اطلاعات
						خدمات

در هر خانه دو بحث مد نظر است یکی که مربوط به تهدیدهای آن خانه است و مباحث فقهی که این فعل انسانی به عنوان تهدید داراست و دوم بحثی که مربوط به تدبیرهای آن خانه است و مباحث فقهی که این فعل انسانی به عنوان تدبیر دارد. در این فصل مبحث اول و در فصل بعد مبحث دوم را بررسی خواهیم کرد.

والحمد لله رب العالمين