دانشگاه آزاد اسلامی واحد نراق

امنیت فناوری اطلاعات
حقوق و جرایم سایبری

ارائه شده برای درس سیستم‌های اطلاعاتی مدیریت پیشرفته

دکتر شفیعی نیک‌آبادی

تهیه و تنظیم:

حسن رضایی

علیرضا عبدالهی

امنیت فناوری اطلاعات

مقدمه
امنیت فناوری اطلاعات
نفوذگران و اهداف حمله به شبکه‌های رایانه‌ای
دسته‌بندی نفوذگران از حیث رفتاری
دسته‌بندی نفوذگران از حیث شخصیتی
سطوح مهارت نفوذگران
دسته‌بندی تهدیدات امنیت
فرآیند توسعه‌ی امنیت

مقدمه

با گسترش روز افزون فناوری اطلاعات، موضوع تهدیدات امنیتی در این حوزه و چگونگی مقابله با آن‌ها از اهمیت فوق‌العاده‌ای یافته است. استفاده از شبکه‌های رایانه‌ای با وسعت زیاد برای تبادل اطلاعات مهم بین نقاط گوناگون جهان، در کنار مزایای بسیاری که به همراه دارد، عرصه‌ی گسترده‌ای را برای سوء استفاده پدیدآورده است. بنابراین یکی از مباحث مهم در حوزه‌ی فناوری اطلاعات، امنیت آن است.

امنیت فناوری اطلاعات

فناوری اطلاعات شامل فناوری‌هایی است که درخدمت ذخیره‌سازی، پردازش، انتقال و مدیریت اطلاعات است اما امنیت اطلاعات به استفاده ایمن از این فناوری و اطمینان از وجود محیطی عاری از هرگونه تهدید باز می گردد.

امنیت فناوری اطلاعات:

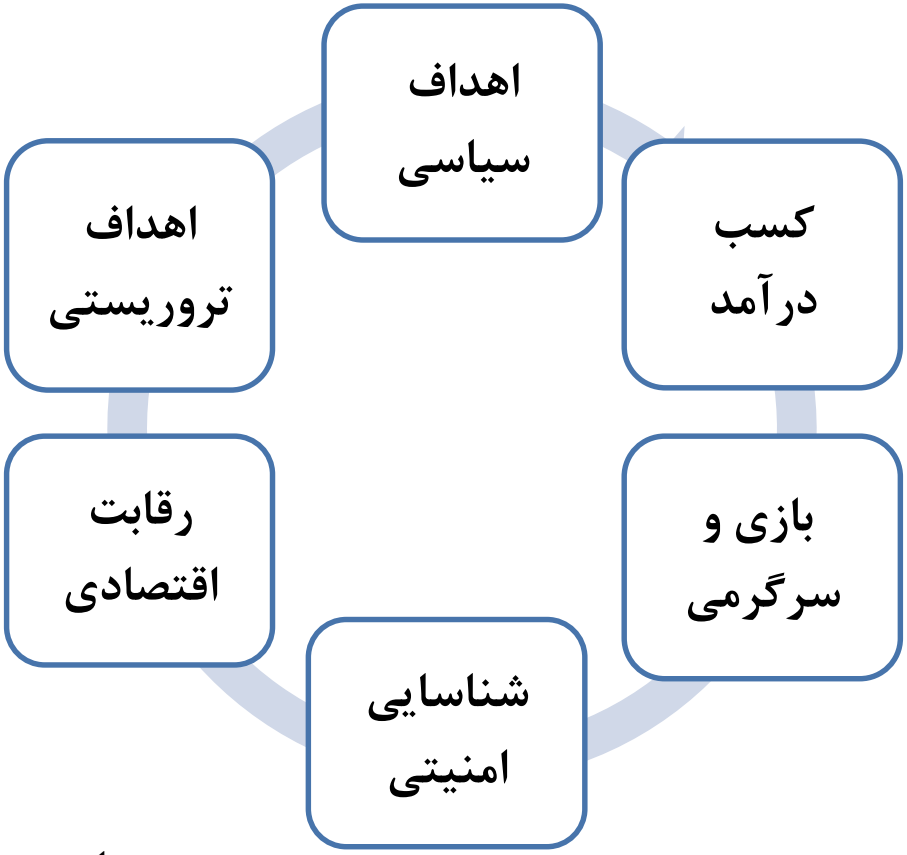
۱- امنیت کامپیوتر (Computer Security):

هدف از امنیت کامپیوتری نگهداری از منابع اطلاعاتی در مقابل استفاده غیرمجاز و یا نادرست و همچنین حفاظت از اطلاعات در مقابل صدمات عمدی یا غیرعمدی، افشا یا تغییر است.

۲- امنیت ارتباطات (Communication Security)

به حفاظت از اطلاعات در طی انتقال بین سیستم‌های کامپیوتری و شبکه‌ها باز می‌گردد.

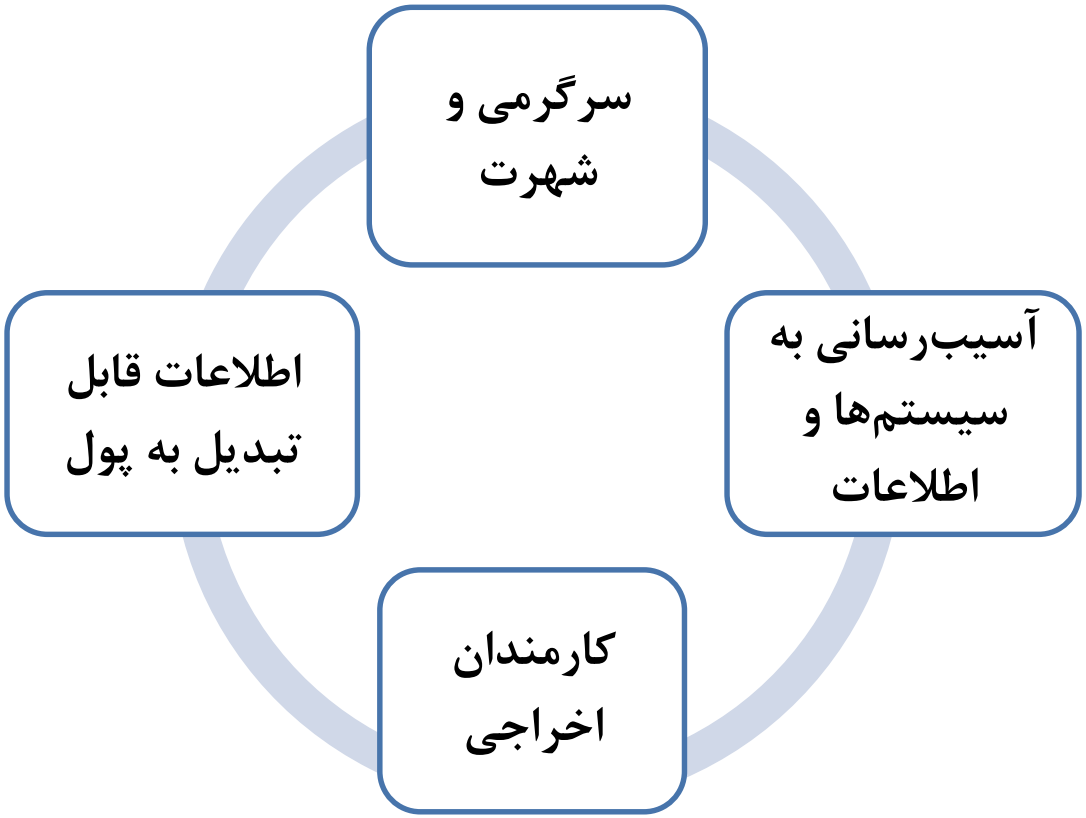
نفوذگران و اهداف حمله به شبکه‌های رایانه‌ای



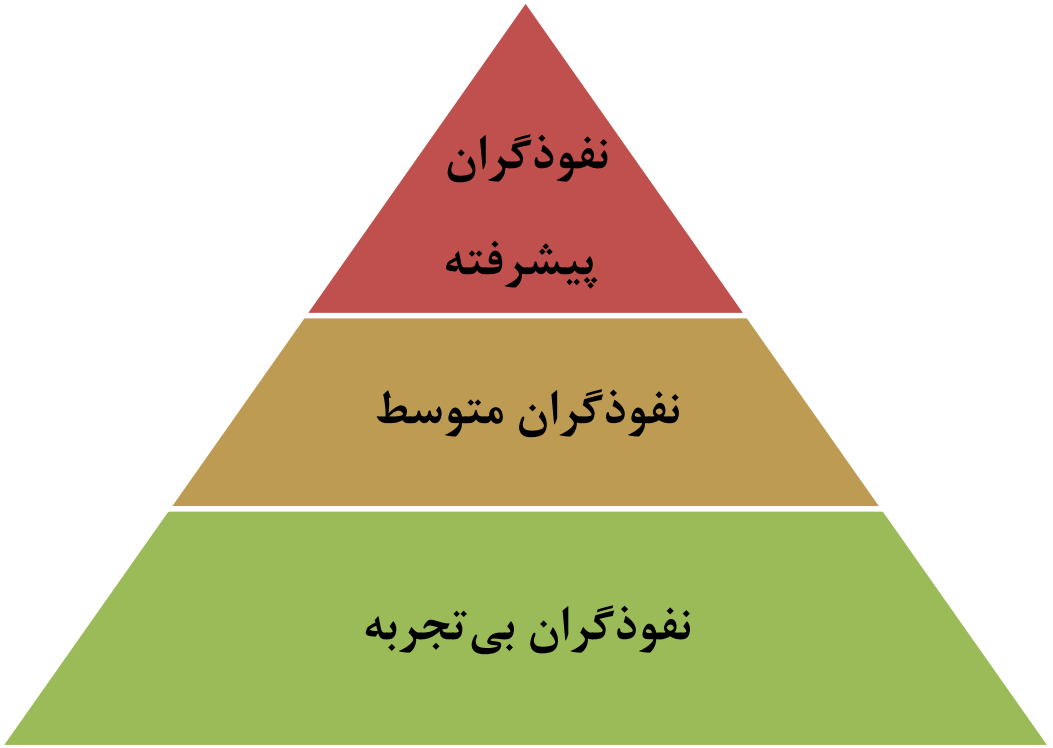
دسته‌بندی نفوذگران از حیث رفتاری

- ✓ **هکر:** شخصی است که از مهارت زیاد در زمینه برنامه‌نویسی و شبکه‌های کامپیوتری برخوردار بوده و به منظور شناسایی ویژگی‌های امنیتی سیستم‌های کامپیوتری در آن‌ها رخنه می‌کند، لیکن نقش تخریبی ندارد.
- ✓ **کراکر:** شخصی است که برای بهره‌برداری غیرمجاز، سرقت و یا تخریب اطلاعات در سیستم‌های کامپیوتری نفوذ می‌نماید.
- ✓ **واکر:** نفوذگران مزاحمی را گویند که شبیه کراکرها در پی خرابه کاری یا سرقت اطلاعات نمی‌باشند.

دسته‌بندی نفوذگران از حیث شخصیتی

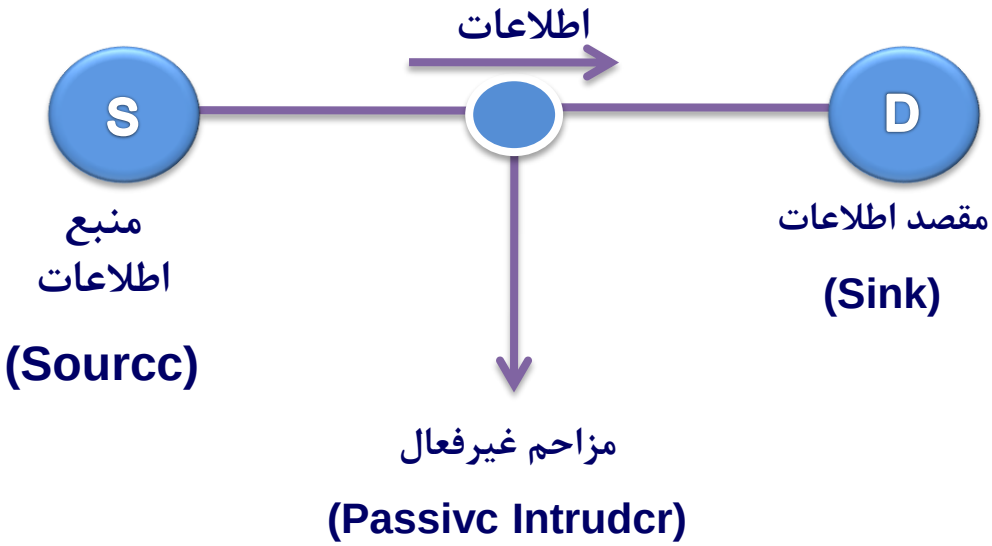


سطوح مهارت نفوذگران



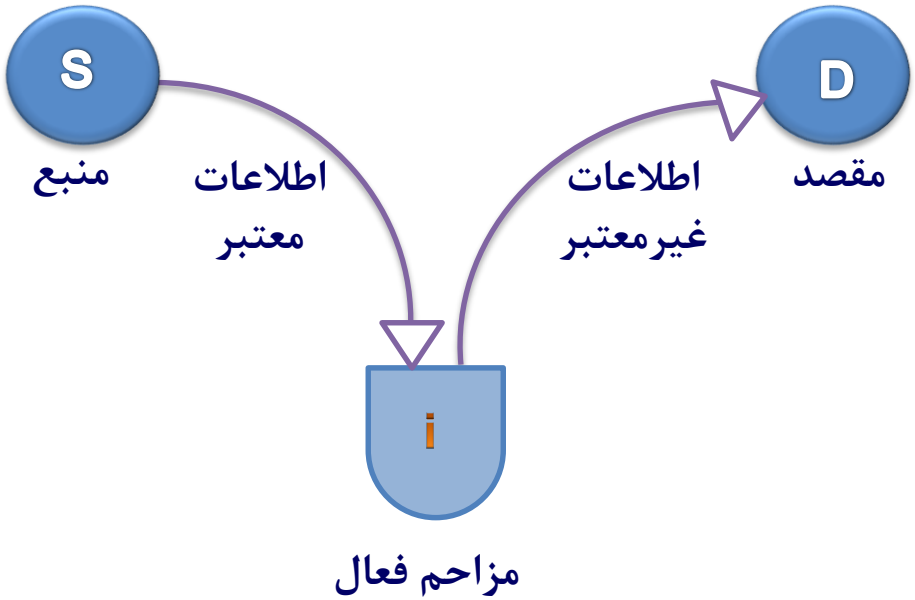
دسته‌بندی تهدیدات امنیت

- ✓ تهدیدات غیرفعال



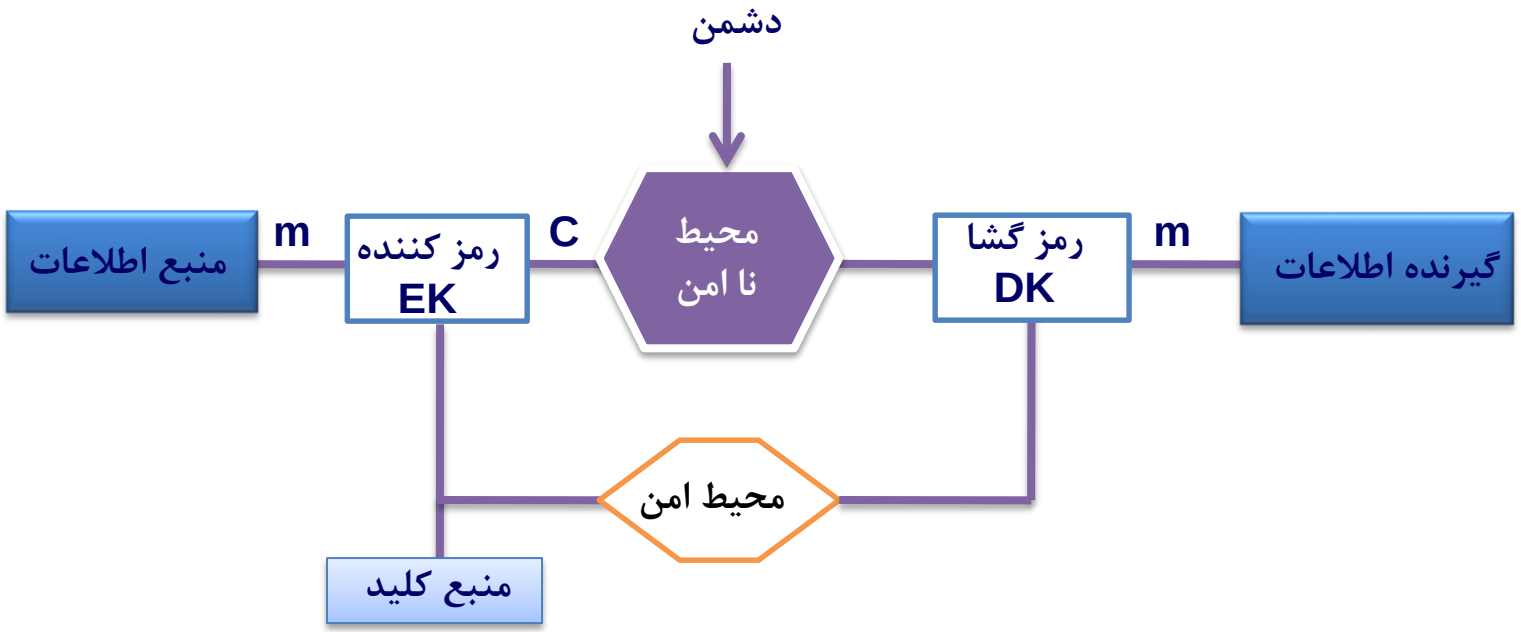
دسته‌بندی تهدیدات امنیت

- ✓ **تهدیدات فعال**



دسته‌بندی تهدیدات امنیت

جلوگیری از تهدیدات با استفاده از رمزگذار پیغام



دسته‌بندی تهدیدات امنیت

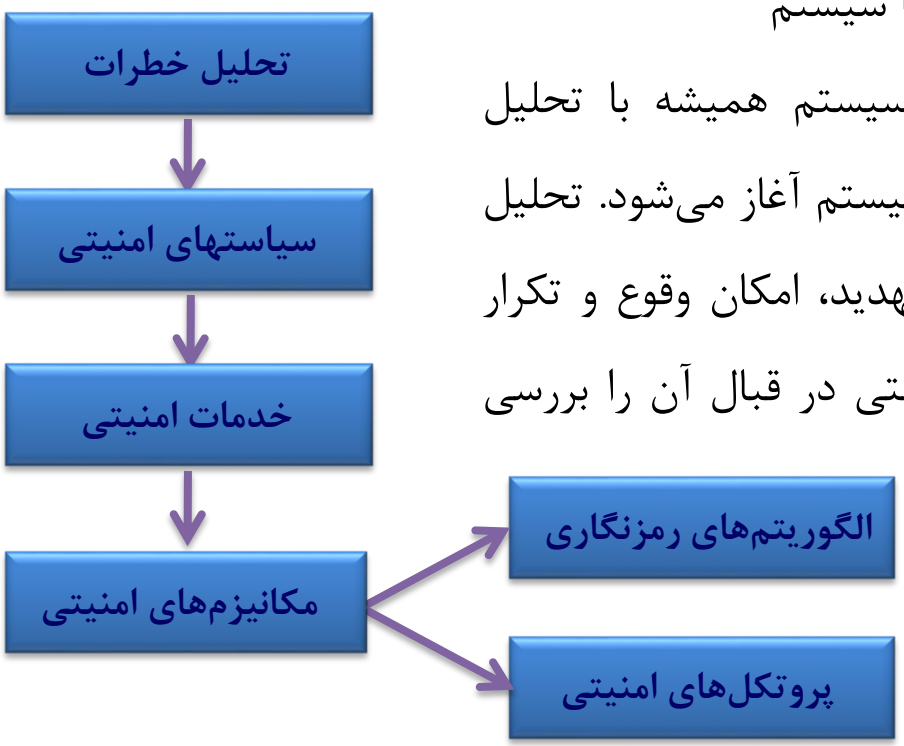
طبقه‌بندی جزئی‌تر تهدیدات و حملات امنیتی:

- ✓ استراق سمع (Eavesdropping)
- ✓ تغییر قیافه (Masquerading)
- ✓ مداخله در پیام (Message Tampering)
- ✓ ارسال مجدد (Replaying)
- ✓ تحلیل ترافیک (Traffic Analysis)
- ✓ انکار یا تکذیب سرویس (Denail Of Service)

فرآیند توسعه‌ی امنیت

۱- تحلیل خطرات مطرح در سازمان یا سیستم

فرآیند توسعه عملکرد امنیتی یک سیستم همیشه با تحلیل حملات محتمل و آسیب پذیری آن سیستم آغاز می‌شود. تحلیل ریسک، رابطه بین خطرآفرینی یک تهدید، امکان وقوع و تکرار آن و هزینه ایجاد مکانیزم‌های محافظتی در قبال آن را بررسی می‌کند.



فرآیند توسعه‌ی امنیت

تحلیل خطر برای تهدیدات امنیتی

میزان خطرآفرینی	احتمال وقوع تهدید		
	به‌ندرت	گاه و بی‌گاه	اغلب
تا حدودی جدی	۱	۲	۳
جدی	۴	۵	۶
خیلی جدی	۷	۸	۹

فرآیند توسعه‌ی امنیت

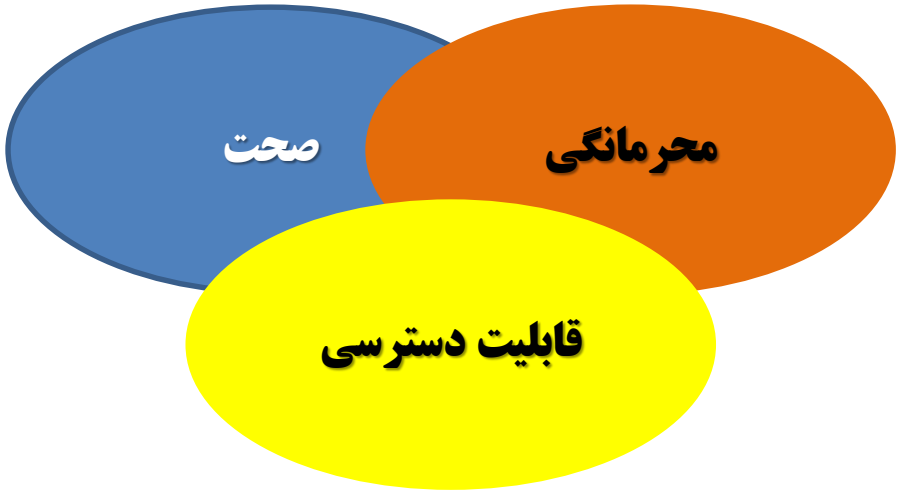
۲- تدوین سیاست ها و خدمات امنیتی

سه مولفه اصلی (CIA):

۱- محرمانگی (Confidentiality)

۲- صحت یا یکپارچگی (Integrity)

۳- قابلیت دسترسی (Availability)



فرآیند توسعه‌ی امنیت

سازمان بین المللی ISO

۱- احراز هویت (Authentication)

۲- کنترل دستیابی (Access Control)

۳- محرمانگی داده (Data Confidentiality)

۴- یکپارچگی یا اصالت داده (Data Integrity)

۵- عدم انکار(Nonrepudiation)

فرآیند توسعه‌ی امنیت

۳- تعیین مکانیزم‌های امنیتی

- ✓ مکانیزیم رمزگذاری
- ✓مکانیزم امضای دیجیتال
- ✓ مکانیزیم کنترل دستیابی
- ✓ مکانیزیم صحت داده
- ✓ مکانیزیم تبادل احراز هویت
- ✓ مکانیزیم پوشش ترافیک
- ✓ مکانیزیم کنترل مسیریابی
- ✓ مکانیزیم تایید توسط عامل سوم

حقوق و جرایم سایبری

مقدمه
تاریخچه جرایم رایانه‌ای
تعریف جرم رایانه‌ای
شاخه‌های حقوق و جرایم سایبری
ماهیت جرایم سایبری
طبقه‌بندی جرایم سایبری

مقدمه

امروزه بسیاری از مردم از شبکه اینترنت یا اینترانت برای مبادله پیام یا فعالیت‌های دیگر استفاده می‌کنند. این شبکه‌ها فاصله زمانی و مکانی را از بین برده و قدرت زیادی در اختیار بشر قرار داده است. چون این فناوری فضای اشتراکی ایجاد کرده و مفاهیم جدیدی چون حاکمیت سایبری و غیره را به منصه ظهور رسانده است، برای استفاده از آن نیازمند تدوین قوانین جدیدی هستیم که «**حقوق سایبری**» نام دارد. از طرفی این فضا شرایط سوء استفاده را برای افراد بزهکار فراهم کرده است. از این رو در این فضا نیز ممکن است انسان مرتکب جرم شود. چون چنین جرمی در فضای اینترنتی روی می‌دهد آن را جرم الکترونیکی یا سایبری نام می‌نهند.

تاریخچه جرایم رایانه‌ای

اولین مورد جرم کامپیوتری توسط « الدون رویس » حسابدار یک شرکت اتفاق افتاد. به زعم وی شرکت حق او را پایمال کرده بود، بنابراین با تهیه برنامه‌ای قسمتی از پول‌های شرکت را به خود اختصاص داد. انگیزه رویس در این کار انتقام‌گیری بود. رویس در مدت ۶ سال توانست بیش از یک میلیون دلار برداشت کند. چون برنامه وی مکانیزمی برای توقف نداشت نمی‌توانست آن را متوقف کند از این رو خود را به مراجع قانونی معرفی کرد و به ده سال زندان محکوم شد.

تعریف جرم رایانه‌ای

متخصصین وحقوقدانان تعریف‌های مختلفی ازجرم کامپیوتری (سایبری) ارائه کرده‌اند. بعضی از این تعاریف در ذیل آمده است:

- ✓ سوء استفاده از کامپیوتر به عنوان هر رفتار غیرقانونی، غیر اخلاقی یا غیرمجاز مربوط به پردازش خودکار و انتقال داده‌ها.
- ✓ هر فعل مثبت غیرقانونی که در آن رایانه ابزار یا هدف جرم است. به عبارت دیگر ابزارها یا هدفی که تأثیرگذار بر عملکرد رایانه است.
- ✓ هرگونه رخداد توأم و انجام شده با فناوری رایانه که موجب شده بزه‌دیده متحمل ضرر بالقوه یا بالفعل شود و مرتکب عامداً توانسته یا خواهد توانست چیزی کسب کند.
- ✓ هر عمل مجرمانه‌ای که رایانه وسیله ارتکاب یا برای ارتکاب باشد.

شاخه‌های حقوق و جرایم سایبری

اینترنت فضای جدیدی برای ارتباط و استفاده از منابع اطلاعاتی در اختیار بشر قـرار داده اسـت که قوانین حقوقی جدیدی می‌طلبد. شاخه‌های حقوق سایبری عبارتند از:

الف – حقوق جزا (جرایم سایبری)

ب – حقوق خصوصی در فضای سایبر شامل:

- ✓ حقوق مدنی شامل قراردادهای انفورماتیک، ادله اثبات دیجیتالی، مسئولیت در شبکه‌های برخط و مالکیت فکری سایبری
- ✓ حقوق تجارت الکترونیک

شاخه‌های حقوق و جرایم سایبری

ج – حقوق عمومی در فضای سایبر شامل:

- ✓ حمایت از داده (حریم خصوصی)
- ✓ جریان آزاد اطلاعات شامل دموکراسی الکترونیکی، رأی گیری، الکترونیک و پارلمان الکترونیکی

د – حقوق بین المللی درفضای سایبر شامل:

- ✓ اصول حقوق بین الملل
- ✓ حاکمیت سایبری
- ✓ روش های حل اختلاف
- ✓ داوری
- ✓ تابعیت سایبری
- ✓ ازدواج اینترنتی
- ✓ قانون محل وب سرور
- ✓ قانون الکترونیک
- ✓ اقامتگاه سایبری
- ✓ روش های همکاری

ماهیت جرایم سایبری

چون جرایم رایانه‌ای و سایبری ناشی از فناوری مدرن است از این روی آثار جـالبی دارد کـه در ادامه بررسی می‌شود:

۱- جرایم کامپیوتری تصنعی هستند.

۲- تأثیر وجدانی اندکی برفاعل دارند.

۳- عنصر مادی جرایم سایبری مشابه است (شکل یکسان ارتکاب).

۴- زمان ارتکاب جرم به حداقل رسیده است.

۵- مکان ارتکاب بین المللی شده است.

۶- بزه دیده به جای انسان ماشین است.

طبقه‌بندی جرایم سایبری

یکی از مشکلات برخورد قضایی و پلیسی با جرم‌های سایبر چگونگی طبقه بنـدی آن هـا اسـت. کشورهای مختلف به علت سنت های حقوقی متفاوت، رویه های مختلفی را به رویکردهـا فنـی، حقوقی در ارتباط با جرم کامپیوتری دنبال کرده اند. از این روی طبقه بندی های متفـاوتی نیـز ارائه داده اند که بعضی از آن ها عبارتند از :

۱- طبقه بندی OECD

۲- طبقه بندی شورای اروپا

طبقه‌بندی جرایم سایبری

جرایم کامپیوتری از دیدگاهی دیگر به سه گروه زیر تقسیم می شوند :

۱- جرایم اقتصادی مربوط به کامپیوتر مثل کلاهبرداری، جاسوسی کامپیوتری و خرابکاری کامپیوتری

۲- جرایم مربوط به رایانه علیه حقوق فردی، خصوصاً علیه حق حریم خصوصی شهروندان با توجه به شیوه‌های مختلف نقض حریم خصوصی

۳- جرایم مربوط به رایانه علیه منافع جمعی مثل جرایم علیه امنیت ملی، علیه کنترل جریان فرامرزی داده‌ها، علیه تمامیت رویه‌های رایانه‌ای و شبکه‌های داده

مراجع

- مبانی و مدیریت فناوری اطلاعات / تألیف: دکتر محمد فتحیان و مهندس سید حاتم مهدوی‌نور

پرسش و پاسخ