Session1

مؤلفه هاي اكوسيستم اقتصاد ديجيتال :

محصولات و خدمات (Product & Service) : بسياري از محصولات و خدمات بصورت ديجيتالي ارائه مي شود. شبيه مستندات كاغذي، كتابها ، اطلاعات صوتي و تصويري، بليط ها، رزرو هتلها، آموزش، حراجها ، پزشكي و ...

مصرف كنندگان (Consumer) :

جمعيت كثيري كه در فضاي وب به جستجوي نياز خود مي پردازند (كشف نياز از طريق وب)

فروشندگان (Seller) :

فروشگاههاي الكترونيكي روي وب كه محصولات و خدمات خود را تبليغ مي كنند.

واسطه ها (Intermediary) :

ارائه كننده خدمات اينترنتي هستند بعنوان مثال ايجاد و مديريت بازارهاي الكترونيكي را بعهده دارند اين واسطه ها معمولا سيستم هاي رايانه اي هستند كه تحت عنوان واسطه هاي الكترونيكي ناميده ميشوند.

خدمات پشتيباني (Support Service) :

ايجاد و پشتيباني فضاي ديجيتال شبيه صدور گواهينامه، خدمات ايجاد اعتماد

سازمانهاي مرتبط با ايجاد زيرساخت (Infrastructure Companies) :

هزاران سازمان تدارك سخت افزار و نرم افزارهاي مورد نياز EC را به عهده دارند .

سازندگان محتوا(Content Creators) :

سازمانهايي كه عهده دار ايجاد محتواي مناسب در EC هستند مثلا صفحات وب

شركاي كسب و كار (Business Partners) :

در كنار فروشندگان و خريداران سازمانهايي هستند كه در روي اينترنت به همكاري مي‌پردازند

بازارهاي الكترونيكي (Electronic Marketplaces) :

بازارهايي نظير بازارهاي چند به چند (چند فروشنده و چند خريدار)، يا يك به چند (Sell-Side or Buy-Side).

تعريف EDI (Electronic Data Interchange)

و اجزاي اصلي آن :

- تعريف رسمي EDI عبارتست از :مبادله الكترونيكي اطلاعات ساختار يافته بين كامپيوترهاي سازمانهاي مختلف به شكل پيامهاي استاندارد .
- و بر طبق تعريف كنفرانس بين المللي تجارت و عمران سازمان ملل متحد EDI عبارتست از انتقال كامپيوتر به كامپيوتر اطلاعات تجاري واداري بااستفاده ازاستانداردموردتوافق ساختار يافته.

عناصر مورد نياز و ضروري براي استفاده از سيستم EDI عبارتند از :

- سخت افزار
- مخابرات و شبكه‌هاي مخابراتي
- نرم افزارهاي ارتباطي و نرم افزارهاي مترجم

تجارت الكترونيكي چيست؟ (E_Commerce)

تعاريف مختلف :

تجارت الكترونيكي بر پردازش وانتقال الكترونيكي داده‌ها،شامل متن،صداوتصوير مبتني مي‌باشد و شامل فعاليتهاي گوناگوني از قبيل مبادله الكترونيكي كالاها و خدمات،تحويل فوري مطالب ديجيتالي و انتقال الكترونيكي مي‌شود.

تجارت الكترونيكي فرايند خريد،فروش يا تبادل‌محصولات،خدمات واطلاعات از طريق شبكه‌هاي كامپيوتري و اينترنت است.

تجارت الكترونيكي به معني انجام تجارت كالا و خدمات با استفاده از ارتباطات راه دور و ابزارهاي مبتني بر آن مي‌باشد

تعريف تجارت الكترونيكي از ديدگاههاي مختلف:

- Communications(تحويل كالاها ، خدمات و ...)
- Business process(اتوماسيون تراكنشهاي كسب و كار)
- Service(ابزار كاهش هزينه خدمات و ارتقاي كيفيت)
- Online(توانايي خريد و فروش مبتني بر اينترنت)
- Collaborations(ايجاد ارتباطات درون و برون سازماني)
- Community(گردهم آوري اعضاي جامعه براي يادگيري وارتباط)

كسب و كار الكترونيكي چيست؟ (E_Business)

- كسب و كار الكترونيكي از معناي وسيعتري نسبت به تجارت الكترونيكي برخوردار است كه نه تنها شامل خريدوفروش است بلكه شامل ارائه خدمات به مشتريان،همكاري با شركاي بنگاه و اجراي معاملات در يك سازمان مي‌باشد.
- كسب وكار الكترونيكي واژه‌اي است كه به معني اجراي كسب و كار با استفاده از ارتباطات راه دور (telecommunications) و همچنين مبتني بر ارتباطات دوربرد مي باشد. بعنوان مثال فرآيند ثبت و صدور مجوز،نام‌نويسي دانشجويان يا اداره يك دادگاه از جمله مواردي هستند كه در مقوله كسب و كار الكترونيكي قرار مي‌گيرند و در ارتباط با تجارت الكترونيكي قلمداد نمي‌گردند.

تاريخچه تجارت الكترونيكي

- از اواخر دهه ۱۹۷۰ كاربردهاي EC مورد توجه قرار گرفته است. نظير EFT ، Electronic Fund Transfer (انتقال الكترونيكي سرمايه) در اين دوره كاربردها بيشتر در سازمانهاي بزرگ و انستيتوهاي مالي مطرح بود.
- سپسEDI (Electronic Data Interchange) مطرح شدكه كاربردهاي غير مالي را هم اضافه كرد.
- در دهه ۱۹۹۰ با افزايش نرخ كاربري اينترنت تجارت الكترونيكي به معني فعلي مطرح شد.

انواع سازمانها از حيث ميزان بهره مندي از EC:

- سازمانهاي brick-and-mortar : سازمانهاي كاملا سنتي (رويه هاي فيزيكي)
- سازمانهاي click–and-mortar:برخي ازفعاليتهاي آنهابا بهره‌گيري ازتجارت الكترونيكي است.
- سازمانهاي Virtual: كاملا مبتني بر تجارت الكترونيكي خالص Pure

انواع تجارت الكترونيكي(از حيث تراكنش هاي مختلف) (بسيار مهم)

الف ـ ارتباط بنگاه و بنگاه(B2B(Business _ to _ Business الگويي از تجارت الكترونيكي را گويند كه طرفين معامله شركتها يا بنگاهها مي باشند.بعنوان مثال ارتباط تجاري بين سازندگان قطعات خودرو و خودروسازان از اين نوع است.

ب ـ ارتباط بنگاه و مصرف‌كننده (B2C(Business_to_Consumer الگويي از تجارت الكترونيكي را گويندكه بسيارمتداول بوده وارتباط تجاري مستقيمابين شركتها ومشتريان يا مصرف‌كنندگان برقرار مي‌شود ج ـ ارتباط مصرف‌كنندگان و شركتها(C2B(Consumer _to_ business در اين حالت اشخاص حقيقي به كمك اينترنت فرآورده‌ها يا خدمات خود را به شركتها مي‌فروشند.

انواع تجارت الكترونيكي

د- ارتباط مصرف‌كننده با مصرف كننده(C2C(Consumer _to_ consumer در اين حالت ارتباط خريدوفروش بين مصرف‌كنندگان است.مزايده‌ها و مناقصه‌هاي كالا از طريق اينترنت در اين مقوله مي‌گنجد. (p2p نوع خاص آن است)

هـ - ارتباط بين بنگاهها و سازمانهاي دولتيB2A (Business _to_ Administration) شامل كليه تعاملات تجاري بين شركتها و سازمانهاي دولتي است.پرداخت مالياتها و عوارض از اين قبيل تعاملات محسوب مي‌گردد.اين حالت به عنوان ارتباط بنگاهها و دولت(Business _to _Government) (B2G) نيز ناميده مي‌شود.

و- ارتباط بين دولت و شهروندان(G2C(Government _to _citizens الگويي از تجارت الكترونيكي است كه در آن ارتباط بين دولت و آحاد مردم كه شامل بنگاههاي اقتصادي،مؤسسات دولتي و كليه شهروندان مي‌باشد با استفاده از فناوري اطلاعات و ارتباطات برقـرار مي گردد از اين الـگو تحت عـنـوان دولـت الـكتـرونيـكيE_ government نيز ياد مي شود.

ز- ارتباط بين بنگاهها و كارمندان(B2E(Business _to_ Employee الگويي از تجارت الكترونيكي است كه در آن يك سازمان خدمات،محصولات يا اطلاعات مورد نياز را به كاركنان خود تحويل مي‌دهد.

ح - فعاليت‌هاي تجاري سيار(MC(Mobile Commerce شامل تعاملات تجاري است كه در يك محيط بي‌سيم به صورت سيار انجام مي‌پذيرد.ضمنا آن دسته از معاملات تجاري سياركه متوجه افرادمعين در مكانها و زمانهاي مشخص مي‌باشد را(LC) يا Location Commerce گويند.

ط - تجارت الكترونيكي درون سازماني(Intra business) شامل كليه فعاليتهاي درون سازماني در رابطه با مبادله كالا،خدمات يا اطلاعات بين واحدها و كاركنان مختلف يك سازمان مي‌باشد.

ي - ارتباط بين دولتها(G2G(Government _to_ Government اين الگو شامل ارتباط تجاري بين دولتها در زمينه‌هايي شبيه صادرات و واردات مي‌باشد.

ك - تجارت مشترك (CC(Collaborative Commerce الگويي از تجارت الكترونيكي است كه در آن افراد يا گروهها بصورت پيوسته(Online) با يكديگر همكاري و تشريك مساعي مي‌نمايند.

سهم تجارت الكترونيكي از طريق B2C و B2Bبيش از حالات ديگر گزارش شده است

قواعد تجاري(اسلايد ۳۱)

قواعد تجاری در مدلهاي مختلف متفاوت است مثلا:

در معاملات بين شركتها (B2B) عمليات بصورت رسمي همراه با ارتباط مستقيم مصرف‌كننده و خريدار و توأم با مذاكرات پيچيده است همچنين تسويه‌حساب پس از دريافت كالا يا خدمات توسط خريدار انجام مي‌شود.

در تبادلات بين شركتها و مصرف‌كنندگان (B2C) كه به صورت خرده‌فروشي (Retail)انجام مي‌پذيرد عمليات بصورت غير رسمي و با مذاكره ساده همراه با ارتباطات غير مستقيم مصرف‌كننده و خريدار است ضمنا ابتدا عمليات پرداخت انجام شده و سپس تحويل كالا يا خدمات صورت مي‌پذيرد .

چرخه تجارت (Trade cycle)

چرخه تجارت گوياي مجموعه تبادلاتي است كه بين عرضه‌كننده كالا يا خدمات و خريدار انجام مي‌پذيرد كه شامل مراحل ذيل است:

الف ـ فعاليتهاي پيش از خريد (pre _ sales):

اين فعاليتها شامل جستجو وانتخاب عرضه‌كننده مناسب،انجام مذاكرات لازم و توافق در رابطه با شرايط و چگونگي معامله است.

ب ـ انجام معامله (Execution):

دراين مرحله خريدار كالا يا خدمات مورد نياز خود را انتخاب و سفارش(order) خريد انجام مي‌پذيرد و فروشنده نيز اقدام به تحويل (Delivery) موارد نياز خريدار مي‌نمايد.

ج ـ تسويه حساب(Settlement) :

در اين مرحله عمليات ارسال صورتحساب توسط فروشنده و پرداخت توسط خريدار انجام مي‌شود.

د ـ خدمات پس از فروش (After _ sales) :

مرحله آخر از چرخه تجارت است كه شامل خدماتي از قبيل رسيدگي به شكايات و نارضايتي مشتريان و تعمير و نگهداري مي‌باشد.

تجارت الكترونيكي Partial و Pure(خالص)

اگر چرخة تجارت الكترونيكي بصورت كاملا (مبتني بر وب) ديجيتال صورت گيرد آن حالت را Pure و در غير اينصورت Partial (ناقص)گويند.(شبيه فروش محصولات فروشگاه شهروند)

مراحل بهره‌برداري از تجارت الكترونيكي (الگوي ساده B2C)

الف ـ ايجاد فروشگاه الكترونيكي با تواناييهاي مورد نياز(يك سايت وب با آدرس مشخص شبيه WWW. Amazon. Com و بصورت مشتري پسند)

ب ـ انجام تبليغات (Advertisement) مثلا با بهره گيري از موتورهاي جستجو يا ...

ج ـ سفارش خريد بصورت الكترونيكي با استفاده از سبد مجازي، ارسال نامه به روش پست الكترونيكي يا تكميل و ارسال فرمهاي الكترونيكي

د ـ پرداخت (توسط كارت اعتباري يا بدون استفاده از كارت اعتباري)

به منظور استفاده از كارت اعتباري وجود يك حساب ويژه تجارت الكترونيكي(Merchant Account) در يكي از بانكهاي مشخص براي فروشگاه مورد نظر ضروري است.(توجه به روشهاي امنيتي مثل SSL,SET)

هـ ـ تحويل كالا يا خدمات (بصورت فيزيكي و يا براي محصولات ديجيتال بوسيله اينترنت)

و ـ خدمات پس از فروش

امنيت در تجارت الكترونيك

- يكي از دغدغه هاي اصلي درEC امنيت است. خريداران به فرستادن اطلاعات خصوصي خود بر روي اينترنت حساس هستند وفروشندگان به سيستمها و داده‌هاي استراتژيك خود اهميت مي دهند.

انجمن ملي امنيت كامپيوتري امريكا(مهم –شايد سوال امتحانی) (NSCA) چهار جنبه را براي امنيت در تجارت الكترونيك بيان مي‌كند:

- احراز هويت Authentication : فرستنده (سرويس دهنده يا سرويس گيرنده) پيغام همان كسي است كه وي ادعا مي‌كند.
- خصوصي بودن (محرمانه بودن) Confidentiality : محتواي يك پيغام سري بوده و تنها براي فرستنده و گيرنده مورد نظر مشخص است.
- يكپارچگي Integrity: محتواي يك پيغام در حين انتقال چه عمداً و چه سهواً تغيير داده نمي‌شود.
- عدم انكار(عدم تكذيب) Non Repudiation: فرستنده پيغام نمي تواند فرستادن آن را انكار نمايد.

مزاياي تجارت الكترونيك

- امروزه بسياري از صنايع شامل مسافرت, استخدام, معاملات املاك, بانكداري, خدمات مالي و انتشارات در حال استفاده از تجارت الكترونيك هستند. اين نوع تجارت مزاياي زيادي براي شركتها, مصرف كنندگان و جامعه دارد.

✓ **مزاياي تجارت الكترونيك براي شركتها عبارتند از :**

- توسعه بازارها و تبديل آنها به بازارهاي ملي و بين المللي
- كاهش هزينه بوجود آوردن, پردازش, توزيع, ذخيره سازي و بازيابي اطلاعات كاغذي
- منجر به كاهش موجوديها و اموال و هزينه هاي سر بار از طريق مديريت تأمين زنجيره‌اي كارآمد مي‌شود.
- همه گير شدن و عمومي شدن كالاها و خدمات
- كاهش زمان بين هزينه كردن سرمايه و دريافت درآمد

✓ **مزاياي تجارت الكترونيك براي مصرف كنندگان عبارتند از :**

- قادر ساختن آنها به خريد و ديگر فعاليتهاي تجاري در طول ٢٤ ساعت, از هر مكاني
- در اختيار گذاشتن انتخابهاي بيشتر
- تأمين كالاها و خدمات ارزانترازطريق امكان خريد دربسياري مكانها و انجام مقايسه سريع
- تحويل سريع كالا و خدمات, به خصوص در مورد محصولات ديجيتالي
- تأمين اطلاعات مرتبط و مفصل در چند ثانيه در عوض چند روز و چند هفته
- امكان شركت در مزايده‌هاي مجازي
- مجاز ساختن مشتريان براي تعامل با ديگر مشتريان در مجامع الكترونيكي و تبادل عقايد و مقايسه تجارب

✓ **در نهايت مزاياي تجارت الكترونيك براي جامعه عبارتست از :**

- امكان كار براي افراد بيشتري در خانه و انجام سفرهاي كمتري براي خريد كه منجر به كاهش ترافيك در جاده ها و كاهش آلودگي هوا مي‌شود.
- امكان فروش رفتن برخي محصولات با قيمت پائين‌تر كه قدرت خريد افراد كم بضاعت‌تر را افزايش مي‌دهد.
- تسهيل تحويل خدمات عمومي با هزينه‌اي كمتر

✓ **مزاياي تجارت الكترونيكي(براي سازمانها، مشتريان و جامعه)**

برخي از مزاياي تجارت الكترونيكي عبارتست از:

- گسترش بازارها به بازارهاي ملي و بين‌المللي
- دسترسي سريع به اطلاعات دقيق تجاري و حذف تلفات زماني
- كاهش هزينه‌هاي تبليغات و سربار
- ارتقاي رفاه عمومي مردم
- افزايش رقابت و ارتقاي كيفيت محصولات و خدمات
- افزايش سرمايه‌گذاري و درآمد
- كاهش هزينه‌هاي توليد،پردازش،توزيع،ذخيره‌سازي و بازيابي اطلاعات
- ايجاد فرصتهاي شغلي جديد
- امكان خريد محصولات و خدمات از سراسر جهان ودر مدت‌زمان محدود
- گسترش فضاي انتخاب براي مشتريان
- افزايش سرعت تحويل محصولات و خدمات بويژه فرآورده‌هاي ديجيتالي و بهبود زنجيره عرضه
- امكان شركت در حراجهاي مجازي(مبتني بر شبكه‌هاي رايانه‌اي)
- امكان ارتباط مشتريان در فضاي الكترونيكي و تبادل ايده و انتقال تجربيات تجاري
- كاهش هزينه‌هاي رفت‌وآمد شهري و مسافرت براي خريد،و نتيجتا آلودگي محيطي و ترافيك كمتر
- بهينه‌سازي ارتباط خريداران و فروشندگان از طريق حذف واسطه‌ها

معايب تجارت الكترونيكي

برخي از معايب تجارت الكترونيكي را ميتوان بصورت ذيل بيان نمود:

- مشكلات امنيتي تعاملات تجاري از طريق شبكه‌هاي رايانه‌اي
- كاهش حجم فروش و سطح درآمد مردم
- تضعيف بازارهاي داخلي و انتقال فوري تقاضاهاي داخلي به رقباي خارجي
- كاهش نيروي شاغل و افزايش نرخ بيكاري

محدوديتهاي تجارت الكترونيكي

ازجمله محدوديتهاي مطرح در استفاده از تجارت الكترونيكي كه لازم است مد نظر قرار گيرد عبارتند از:

- لزوم وجود بانكداري الكترونيكي توانمند و دقيق
- فقدان استانداردها و قواعد پذيرفته شده جهاني در مورد امنيت،كيفيت و قابليت اعتماد
- پهناي باند ارتباطي ناكافي
- ضعف ابزارهاي نرم‌افزاري در رابطه با كاربردهاي مختلف تجارت الكترونيكي
- حفظ امنيت اطلاعات و محرمانه بودن اطلاعات شخصي
- توسعه محيط حقوقي لازم به منظور اجراي تجارت الكترونيكي
- روشهاي مطمئن و كارا براي تائيد احراز هويت خريدار و فروشنده
- فقدان اعتماد و مقاومت مشتريان و نبود فرهنگ تجارت On line

Session2

اینترانت و اکسترانت :

دو نمونه از مهمترین گستره های اینترنت، **" اینترانت ها و اکسترانت ها"** هستند.

- اینترانت، شبکه داخلی سازمانی است که از طریق آن امکان **دسترسی به داده های یک شرکت و سازمان برای افراد داخل سازمان** بوجود می آید. دسترسی به آن **محدود** است و فقط در داخل سازمان مورد استفاده قرار می گیرد.
- اینترانت همان مفاهیم و تکنولوژیهای اینترنت را مورد استفاده قرار می دهد ولی **برای ارتباط از بستر اینترنت استفاده نمی شود** و در صورت نیاز به اتصال به اینترنت لزوماً اینترانت را پشت یک **fire wall** یا دیواره آتشین قرار می دهند تا از خطر ها در امان باشد.

مزایای اینترانت :

- ارزان
- قابل گسترش و یا کوچک شدن
- از طریق بیشتر رایانه ها دسترس پذیر
- محیط اطلاعاتی غنی تر و پاسخگوتر
- ایجاد محیطی درون سازمانی برای ذخیره اطلاعات که در هر زمان می توان آن را روزآمد ساخت
- ایجاد محیط همکاری
- اشتراک اطلاعات
- افزایش تشریک مساعی کارمندان
- دسترسی کارمندان سازمان به اطلاعات صرف نظر از محل
- بهبود روشهای تصمیم گیری و به کارگیری اطلاعات
- کاهش هزینه ها از جمله چاپ و توزیع کاغذ، آموزش کارمندان، فروش و بازاریابی و حسابداری، تولید ، دسترسی و توزیع سریع تر اطلاعات،انتقال اطلاعات به شخص یا اشخاص مورد نظر در سازمان بدون اتلاف وقت در کمترین زمان

اکسترانت :

- اکسترانت ها به **اینترانتهای خصوصی که در اختیار کاربران بیرون از سازمان یا شرکت نیز قرار می گیرند گویند.** تا حد بسیار زیادی شبیه اینترانت است با این تفاوت که اکسترانت به منظور دسترسی به تعدادی از شرکای تجاری ، مشتریان خاص و مواردی که به عنوان جزئیات اصلی یک شرکت تلقی می شوند، گسترش می یابد.
- اکسترانت ها برای دسترسی **نیازمند یک نام کاربری و یک کلمه عبور بوده** و از طرفی هویت کاربر قسمتهایی از اکسترانت را که می تواند مرور کند، تعیین می کند.

مزایای اکسترانت :

- اشتراک اطلاعات با مشتریان، تامین کنندگان محصولات و سایر شرکای تجاری
- توسعه و گسترش اطلاعات
- تبادل اطلاعات میان مشتریان
- ایجاد امکان استفاده از اطلاعات منتخب برای افراد بیرون از سازمان
- کاهش هزینه ها
- بهبود فرآیندهای تجاری و کاری
- بهبود و گسترش موقعیت رقابتی شرکت

مقایسه اینترانت و اکسترانت :	*اینترانت*	*اکسترانت*
پهنای باند	زیاد	کم
پروتکل	پروتکل های اینترنت	پروتکل های اینترنت
امنیت	معمولی به زیاد	کم به معمولی
دامنه	ساختمان ومجموعه ساختمان ها	شهر وکشور

SVN یک معماری صحیح امنیتی (Secure Virtual Network)

- مجموعه توانایی های زیر را در یک قالب مدیریتی مشترک ارائه می دهد:

firewall security,
VPNs,
IP address management
Etc...

و نیز یک خط مشی امنیتی واحد را با توجه به تمام جنبه های امنیتی تعریف می نماید.

مؤلفه های کلیدی معماری SVN (Secure Virtual Network)

- کنترل دسترسی
- احراز هویت کاربر
- ترجمه آدرس شبکه NAT
- شبکه خصوصی مجازی
- دسترس پذیری بالا
- امنیت محتوا
- حسابرسی و گزارش دهی
- مدیریت کاربر بر پایه LDAP

احراز هویت

- احراز هویت کاربر
  - اعطای دسترسی بر پایه کاربر
- احراز هویت میزبان
  - اعطای دسترسی بر پایه میزبان
  - پس از احراز هویت اجازه ارتباط فقط برای IP های خاص داده می شود.
- احراز هویت جلسه
  - نیاز به احراز هویت برای هر ارتباط
- قوانین پنهان سازی:
  - قوانین باید بمنظور جلوگیری از خواندن آسان آنها پنهان شوند.
  - سایر قوانین می توانند آشکار باشند اما بهرحال شماره آنها تغییر می کند.
- احراز هویت کاربر:
  - احراز هویت کاربر توسط سرورهای امنیتی بر روی درگاه مهیا می شود.
  - پس از احراز هویت کاربر سرور امنیتی متناظر درخواست می شود TELNET, FTP, HTTPو RLOGIN .
  - در صورت احراز هویت موفقیت آمیز سرور امنیتی ارتباط جداگانه ای را به سرور هدف برقرار می سازد.

چرا VPN ؟(کلا مباحث مربوط به vpn مهم است)

- برای برقراری **ارتباطی سریع، ایمن و مطمئن بین نقاطی دور از هم،** براي يك شركت بزرگ كه داراي شعب مختلف در نقاط مختلف يك كشور و يا در نقاط مختلف دنيا است، بايستي يك شبكه‌ي گسترده‌ي خصوصي بين شعب اين شركت ايجاد گردد .
- اما **استفاده از خطوط استیجاری هزینه بالا و در عین حال عدم انعطاف پذیری به همراه دارد و هزینه مواقعی که از منابع استفاده نمی شود، نیز باید پرداخت شود.**
- يكي از راه حل هاي اتصال مستقيم به كامپيوتر مقصد به كمك مودم است كه در اينجا علاوه بر مودم ، پيكر بندي كامپيوتر به عنوان سرويس دهنده RAS نيز لازم خواهد بود . از اين گذشته ، هزينه ارتباط تلفني راه دور براي مودم هم قابل تامل است.

چرا VPN ؟

Solutions	Cost	Security	QOS	Flexibility
Leased Line	Very High Dependent To Distance	High	Absolute	Very Low
Dial Up PSTN	High Dependent To Distance	Medium	Absolute	Medium
Internet	Low	Low	Best Effort	Very High
VPN	Medium	Very High	Best Effort	High

- VPN در يك تعريف كوتاه **شبكه‌اي از مدارهاي مجازي** براي انتقال ترافيك شخصي است. در واقع پيادەسازي شبكەي خصوصي يك شركت يا سازمان را روي يك شبكه عمومي، VPN گويند.
- بنا بر تعريف استاندارد (Internet Engineering Task Force) IETF، VPN تقلیدی از WAN با استفاده از **امکانات عمومی یا اشتراکی پروتکل IP** همانند اینترنت می باشد.
- به تعبیری دیگر VPN توسعه یک شبکه اینترانت خصوصی در یک شبکه عمومی همانند اینترنت است که یک ارتباط امن و کم هزینه را بین دو پایانه ارتباطی برقرار می کند. این توسعه به کمک تونل های مفهومی خصوصی میسر می شود.

سیر تکاملی VPN(۲۸)

- VPN یک فناوری جدید نمی باشد، بر خلاف باور عمومی مفهوم VPN مربوط به ۱۵ سال قبل میشود و نسل های گوناگونی را تاکنون پشت سر گذاشته است.
- **نسل اول** اواخر دهه ۸۰ ،توسط AT&T به نام *Software Defined Networks* (SDNs) ایجاد شد.
- **نسل دوم** با تلفیق فناوری های X.25 و ISDN در دهه ۹۰ بوجود آمدند. هر دو این فناوری ها اجازه انتقال رشته ای از بسته ها را در یک شبکه عمومی می دادند.
- **نسل سوم** با ادغام فناوری های ATM و Frame Relay بوجود آمد.
- **نسل چهارم** با رشد تجارت الکترونیک در اواسط دهه ۹۰، سازمان ها راه حلی را می خواستند که **براحتی قابل پیاده سازی، مقیاس پذیر، مدیریت آسان، دارای دسترسی جهانی و دارای امنیت بسیار بالا باشد** نسل کنونی که بر پایه IP می باشد با استفاده از فناوری تونل کشی کلیه این نیاز ها را برآورده می سازد.

مزایای VPN از راه دور

- عدم نیاز به RAS و مودم
- عدم نیاز به پرسنل پشتیبانی
- عدم نیاز به ارتباط از راه دور Dial-up
- ارائه خدمات Dial-up ارزان به کاربران از راه دور
- نرخ انتقال بالای داده ها بدلیل استفاده از مودم در ارتباطات محلی
- ارائه دسترسی بهتر به منابع سازمانی

معایب VPN از راه دور

- عدم تضمین کیفیت خدمات QoS
- امکان بالای **از دست دادن داده ها** و بعلاوه تحویل تکه تکه و بدون ترتیب بسته ها
- بدلیل استفاده از الگوریتم های دقیق رمز نگاری **سربار پروتکل** بطور قابل ملاحظه ای افزایش می یابد. که منجر به تأخیر در فرایند احراز هویت خواهد شد. بعلاوه فشرده سازی داده ها برپایه PPP و IP بسیار کند و ضعیف خواهد بود.
- بدلیل استفاده از بستر اینترنت در انتقال داده ها، در هنگام انتقال داده های چند رسانه ای، **تأخیر قابل ملاحظه ای** بوجود خواهد آمد و توان عملیاتی کاهش خواهد یافت.

VPN های اینترانت

- در صورتیکه سازمانی دارای **یک و یا بیش از یک محل (راه دور) بوده** و تمایل به الحاق آنها در یک شبکه اختصاصی باشد ، می توان یک اینترانت VPN را بمنظور برقرای ارتباط هر یک از شبکه های محلی با یکدیگر ایجاد نمود .

مزایای VPN های اینترانت

- کاهش هزینه ها بدلیل حذف روتر هایی که در ستون فقرات WAN استفاده می شوند.
- کاهش قابل ملاحظه پرسنل پشتیبانی
- امکان **پشتیبان گیری کم هزینه** با استفاده از تونل های VPN بهمراه فناوری سوئیچینگ سریع مانند Frame Relay

معایب VPN های اینترانت

- بدلیل استفاده از تونل کشی در شبکه عمومی حملاتی از نوع انکار خدمات **DoS** تهدیدی جدی محسوب می شوند.
- امکان بالای **از دست دادن داده ها**
- بدلیل استفاده از بستر اینترنت در انتقال داده ها، در هنگام انتقال داده های چند رسانه ای، **تأخیر قابل ملاحظه ای** بوجود خواهد آمد و توان عملیاتی کاهش خواهد یافت.
- عدم تضمین کیفیت خدمات **QoS**

VPN های اکسترانت

- در مواردیکه سازمانی در تعامل اطلاعاتی بسیار نزدیک با سازمان دیگر باشد ، می توان یک اکسترانت VPN را بمنظور **ارتباط شبکه های محلی هر یک از سازمانها** ایجاد کرد. در چنین حالتی سازمانهای متعدد قادر به فعالیت در یک محیط **اشتراکی** خواهند بود .

مکانیزمهای امنیتی VPN(هم بالا مهم هم ازین به بعد)

- تونل کشی
- رمز نگاری
- احراز هویت
- سطوح دسترسی (تفویض اختیار)

تونل کشی

- تونل کشی تکنیکی است که در آن بسته داده ها در پروتکل های تونل کشی IPSec, PPTP , یا L2TP کپسول می شوند و**درنهایت در بسته های IP بسته بندی می شوند. بسته نهایی با استفاده از اطلاعاتIP به طرف شبکه مقصدمسیریابی می شود.**بدلیل اینکه بسته اصلی ازهر نوعی می تواند باشد، تونل کشی **از پروتکل های گوناگونی** مانند ATM و IP, ISDN, Frame Relay پشتیبانی می نماید.

پروتکهای تونل کشی VPN IP Security (IPSec)

- **رشته ای** از پروتکلهاست که برای ایجاد VPN مورد استفاده قرار می گیرند. مطابق با تعریف IETF پروتکل IPSec به این شکل تعریف می شود:
- یک پروتکل امنیتی در **لایه شبکه** است تا خدمات امنیتی رمزنگاری را تامین کند. خدماتی که به صورت منعطفی به پشتیبانی ترکیبی از **احراز هویت ، صحّت ، کنترل دسترسی و محرمانگی بپردازد.**
- **تنها به ترافیک مبتنی بر IPاجازه بسته بندی و رمزنگاری می دهد** ودرصورتی که ترافیک غیر IP نیزدرشبکه وجودداشته باشد،بایداز پروتکل دیگری مانند GRE در کنار IPSec استفاده کرد.
- IPSec به استاندارد de facto در صنعت برای ساخت VPN تبدیل شده است. بسیاری از فروشندگان تجهیزات شبکه ، IPSec را پیاده سازی کرده اند و لذا امکان کار با انواع مختلف تجهیزات از شرکتهای مختلف،IPSec رابه یک انتخاب خوب برای ساختVPN مبدل کرده است.

پروتکهای تونل کشی VPN Point-to-Point Tunneling Protocol (PPTP)

- يك مكانيزم تونل‌كشي **نقطه به نقطه** است كه براي دسترسي راه دور به كارگزار سخت‌افزاري Ascend و ويندوز NTتوسط مايكروسافت، 3COM و Ascendطراحي شده است.در اين قرارداد، **امكان رمزنگاري وجود دارد** و ازقرارداد **PPP**براي بسته‌بندي اطلاعات استفاده مي كند. قراردادPPTP در كاربردهاي **كوچك** و كاربردهايي كه نياز به امنيت خيلي بالايي ندارند، استفاده مي‌شود.راه‌اندازيVPN با استفاده از قرارداد PPTP در اين محيطها **كم‌هزينه و مقرون بصرفه** است. قرارداد PPTP داراي قابليت پياده‌سازيVPN شبكه‌ي محلي-به‌شبكه‌ي محلي نيز ميباشد.
- اين پروتكل امكان رمزنگاري ٤٠ بيتي و ١٢٨ بيتي را دارا بوده و از مدل هاي احراز هويت كاربر كه توسط PPP حمايت شده اند ، استفاده مي نمايد.

پروتکهای تونل کشی VPN

Layer 2 Tunneling Protocol (L2TP)(۵۷بسیار مهم و سوال دارد)

- پروتکل فوق توسط IETF ایجاد شده است .پروتکل فوق از ویژگی های PPTP و L2F استفاده کرده است . پروتکل L2TP بصورت کامل IPSec را حمایت می کند. از پروتکل فوق **بمنظور ایجاد تونل بین موارد زیر استفاده می گردد :**
- سرویس گیرنده و روتر
- NASو روتر
- روتر و روتر
- Layer 2 Forwarding(L2F)پروتکل فوق توسط سیسکو ایجاد شده است . در پروتکل فوق از مدل های احراز هویت کاربر که توسط PPP حمایت شده اند ، استفاده شده است .

ترجمه آدرس شبکه NAT(۶۱مهم)

(Network Address Translation)

- NAT کامپیوترهای داخلی را از شبکه های خارجی **پنهان** می سازد امنیت شبکه را بالا می برد.
- یک میزبان داخلی می تواند به یک میزبان داخلی یا خارجی متصل شود، ولی برای میزبان ناشناخته خارج از شبکه اینگونه نیست.
- بر دو نوع **ایستا و پویا** می باشد.(مهم)

NAT ایستا

- آدرسهای خصوصی IP داخلی را به آدرس عمومی خارجی ترجمه می کند.

NAT پویا(مهم . از تغییر پورت هم استفاده میکند)

- کلیه آدرسهای خصوصی داخلی پشت یک آدرس عمومی خارجی پنهان می شوند و با استفاده از **انتساب پویای شماره های پورت** بین آنها تمایز قائل می شود.

احراز هویت و سطوح دسترسی(۶۶مهم)

- احراز هویت بسته ها و کاربران جهت شناسایی آنان و تعیین مجوز دسترسی آنان به منابع شبکه. مدل **Authentication Authorization Accounting (AAA)** مثالی از یک سیستم جامع احراز هویت کاربران می باشد. این مدل بمنظور ایجاد امنیت بالا در محیط های VPN از نوع " دستیابی از راه دور " استفاده می گردد. زمانیکه کاربران به سیستم متصل می گردند ، سرویس دهنده AAA درخواست آنها را اخذ و عملیات زیر را انجام خواهد داد :
  - شما چه کسی هستید؟ (تایید ، Authentication)
  - شما مجاز به انجام چه کاری هستید؟ (مجوز ، Authorization)
  - چه کارهائی را انجام داده اید؟ (حسابداری ، Accounting)

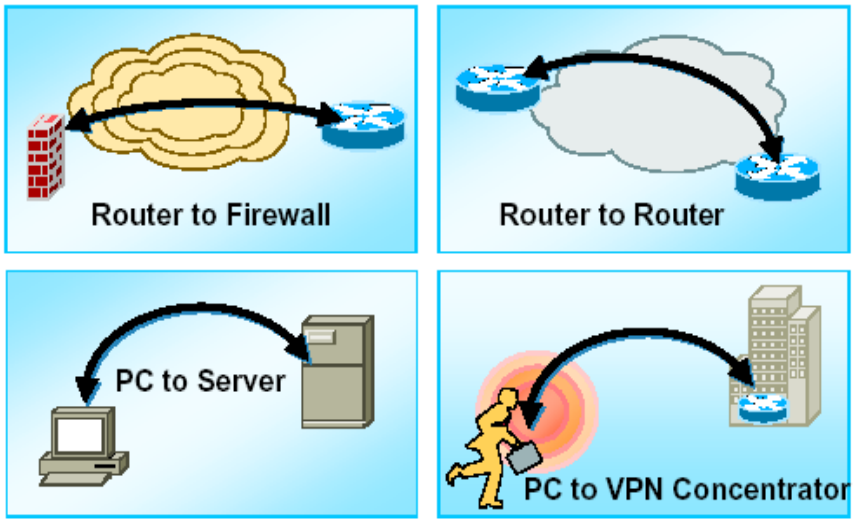
پیاده سازی VPN

- یک پیاده سازی کامل VPN از هر سه نوع گفته شده پشتیبانی می کند و نیز نیازمند سه مؤلفه حیاتی زیر می باشد:
  - امنیت
    - کنترل دسترسی
    - احراز هویت
    - رمزنگاری
  - QoS
    - شامل کنترل ترافیک، مدیریت پهنای باند و سرعت VPN
  - مدیریت و کارایی

تکنولوژی های VPN(۶۹مهم)

با توجه به انواع VPN دستیابی از راه دور و یا سایت به سایت، بمنظور ایجاد شبکه از عناصر خاصی استفاده می گردد :

- نرم افزارهای مربوط به کاربران از راه دور
- سخت افزارهای اختصاصی نظیر یک " کانکتور "VPN و یا یک فایروال PIX
- سرویس دهنده اختصاصی VPN بمنظور سرویس های Dial-up
- سرویس دهنده NAS که توسط ISP بمنظور دستیابی به VPN از نوع "دستیابی از را دور" استفاده می شود .
- شبکه VPN و مرکز مدیریت سیاست ها.



- **کانکتور VPN** : سخت افزار فوق توسط شرکت سیسکو طراحی و عرضه شده است. کانکتور فوق در مدل های متفاوت و قابلیت های گوناگون عرضه شده است . در برخی از نمونه های دستگاه فوق امکان فعالیت همزمان ۱۰۰ کاربر از راه دور و در برخی نمونه های دیگر تا ۱۰,۰۰۰ کاربر از راه دور قادر به اتصال به شبکه خواهند بود .

- **روتر مختص VPN** : روتر فوق توسط شرکت سیسکو ارائه شده است . این روتر دارای قابلیت های متعدد بمنظور استفاده در محیط های گوناگون است . در طراحی روتر فوق شبکه های VPN نیز مورد توجه قرار گرفته و امکانات مربوط در آن بگونه ای بهینه سازی شده اند .

- **فایروالPIX** : فایروال (Private Internet eXchange) PIX قابلیت هائی نظیر NAT ، سرویس دهنده Proxy ، فیلتر نمودن بسته ای اطلاعاتی ، فایروال و VPN را در یک سخت افزار فراهم نموده است.

دو نوع اصلی از VPN ها به طور مشخص شناخته شده اند:

۱- VPNهای مبتنی بر تجهیزات مربوط به مشتری یا Customer Premise Equipment (CPE)

۲- VPN های مبتنی بر شبکه.

دسترس پذیری و قابلیت اطمینان

- **دسترس پذیری بمعنی کل زمان مؤثر استفاده از شبکه است**. در شبکه های خصوصی و اینترانت ها این زمان نسبتاً بالاست زیرا که کل زیرساخت اختصاصی بوده و تحت کنترل کامل سازمان می باشد. با این وجود VPN از یک زیر ساخت عمومی همانند اینترنت و یا PSTN استفاده می کند. بنابراین بسیار وابسته به این نوع شبکه هاست. فاکتور دسترس پذیری در VPN بسیار وابسته به ISP مورد استفاده می باشد.
- بطور کلی ISP ها دسترس پذیری را در قالب *Service Level Agreement* (*SLA*) تضمین می کنند. **SLA توافقی است مابین ISP و سازمان که کل زمان مؤثر استفاده از شبکه را تضمین می کند. با این که گران است ولی بعضی از ISP ها تا توان ۹۹% این امکان را فراهم میکنند.**
- اگر سازمانی به دنبال دسترس پذیری بالا باشد باید به جستجوی ISP که یک زیر ساخت با کیفیت بالا را ارائه می دهد باشد. که شامل موارد زیر می شود:

- **قابلیت مسیر یابی نیرومند که امکان میدهد** در هنگامی که مسیر های اصلی شلوغ و یا بسته است مسیر های جایگزینی را پیدا نماید.

- **فراوانی خطوط دسترسی**. که امکان میدهد تا در هنگام افزایش تقاضا و یا خرابی، برای پهنای باند خود را با شرایط جدید تطبیق دهد.

قابلیت اطمینان

- قابلیت اطمینان، دیگر نیاز اصلی VPN است که بطور کامل در درون فاکتور دسترس پذیری نهفته است. قابلیت اطمینان تراکنشها در VPN **تحویل پایان به پایان داده ها** را در کلیه وضعیتها **تضمین** می نماید. همانند سایر شبکه ها اگر مسیری و یا دستگاهی خراب شود، این امکان با سوئیچ کردن بسته ها به مسیر های گوناگون تضمین می شود. این فرایند برای کاربر نهایی کاملاً شفاف است و با افزایش مسیر ها و سخت افزار لازم بدست خواهد آمد.

کیفیت خدمات QoS

- QoS از دو بعد حیاتی تشکیل شده است: **تأخیر Latency و توان عملیاتی**.

- همانند دسترس پذیری QoS نیز وابسته به SLA می باشد. به کمک SLA سرویس دهنده **یک سطح مشخص از تأخیر و توان عملیاتی را به اعضاء خود ارائه می دهد**. اگر در هر زمان از این سطح توافق شده SLA کمتر شود، نقض توافق خواهد بود. به این ترتیب سازمان مطمئن می شود که به سطح وعده داده شده از خدمات خواهد رسید.
- وابسته به سطح تأخیر و توان عملیاتی وعده داده شده از سرویس دهنده ،QoS به سه دسته زیر تقسیم می شود:
- QoS بهترین تلاش. این کلاس از خدمات در واقع بیانگر فقدان QoS می باشد زیرا ارائه دهنده خدمات نه تأخیر و نه توان عملیاتی را تضمین می نماید. به همین علت ارزان ترین کلاس از خدمات می باشد و برای ترافیک با پهنای باند زیاد و حساس به تأخیر مناسب نمی باشد.
(کاربران معمولی اینترنت)
- QoS نسبی. این کلاس از خدمات قادر است تا ترافیک داده ها را اولویت دهی کند. بنابراین حداقل، توان عملیاتی تضمین خواهد شد. با این وجود این اطمینان کامل نیست و وابسته به بار شبکه و درصد ترافیکی که نیاز به اولویت دهی در هر زمان دارد، می باشد. بعلاوه این سطح از خدمات هیچ تدارکی برای کاهش تأخیر نمی بیند. این کلاس از خدمات برای کاربردهای متقاضی پهنای باند قیمت مناسبی دارد. (اکسترانت ها و دسترسی های از راه دور)
- QoS مطلق. این کلاس هم توان عملیاتی و هم کاهش تأخیر را گارانتی می نماید. بنابراین گران ترین کلاس خدمات محسوب می شود. تراکنشهای صوتی و تصویری

سازگاری

بعلت استفاده از اینترنت، VPN باید قادر به استفاده از آدرس دهی IP و کاربردهای IP باشد. برای اطمینان از سازگاری با زیرساخت IP، روشهای زیر می توانند مکمل VPN باشند:

- استفاده از درگاه های IP gateways
- استفاده از تونل کشی
- استفاده از مسیر یابی IP مجازی Virtual IP Routing (VIPR)

مزایا و معایب VPN

- **مزایای VPN**

  - گسترش محدوه جغرافيائي ارتباطي
  - کاهش هزینه پیاده سازی
  - کاهش هزینه مدیریت و کارکنان از طریق واگذاری به سرویس دهندگان
  - افزایش اتصال بین دفاتر و کاربران راه دور
  - امنیت تراکنشها (با استفاده از فناوری تونل کشی)
  - استفاده کارا از پهنای باند در برابر اتلاف آن در روشهایی نظیر خطوط اجاره ای
  - افزایش مقیاس پذیری و تطبیق با تغییرات آینده

- **معایب VPN**

  - وابستگی زیاد به اینترنت و عدم تضمین کارایی در مقابل خطوط اجاره ای
  - کمبود پشتیبانی از پروتکلهای قدیمی و سازمانهایی که هنوز بر پایه سیستمهای قدیمی فعالند.
  - تردید نسبت به اطلاعات دریافت شده
  - استفاده از منابع غیرموثق
  - تفسیر بد از اطلاعات دریافت شده
  - سرقت ایده ها
  - نبود مهارتهاي حرفه اي در کار با اطلاعات
  - فروش اطلاعات یا استفاده نابجا از اطلاعات
  - عدم اطمينان از کارايي سرويس و تأخير در ارتباطات

Session7

پول و نقش آن در تجارت - نقشهای اساسی پول

- واسطه مبادله

- ذخیره ارزش
- واحد محاسبه (پایه ارزش)
- وسیله پرداختهای آتی

ویژگیهای مطلوب پول

- قابل حمل بودن
- با دوام بودن - Durability
- قابلیت تقسیم پذیری - Divisibility
- یکسان و متحدالشکل بودن - Standardizability
- قابلیت تشخیص - Recognizability

انواع تقسیم بندی پول

- پول کالایی - Commodity Standard
  - پول کالایی عبارت است از کالاهای مادی که کاربرد پولی هم دارند. مانند نمک و احشام در رم باستان.
- پول اعتباری یا اسکناس بدون پشتوانه – Fiat Money
  - نوعی پول اعتباری که بدون پشتوانه مالی توسط بانکها و موسسات مالی ایجاد می گردد.
- پول بانکی یا تحریری

نوعی پول اعتباری که با پشتوانه مالی توسط بانکها و موسسات مالی ایجاد می گردد.

پیدایش نظام بانکداری الکترونیکی

- دوره اول : اتوماسیون پشت باجه – Back Office Automation
- دوره دوم : اتوماسیون جلوی باجه – Front Office Automation
- دوره سوم : متصل کردن مشتریان به حسابهایشان
- دوره چهارم : یکپارچه سازی سیستمها و مرتبط کردن مشتری با تمامی عملیات بانکی

اتوماسیون پشت باجه(اسلاید ۷ – سوال داریم)

- شروع دوره به سال ۱۹۶۰ بر می گردد.

- نقطه آغازین کاربرد کامپیوتر در نظام بانکداری می باشد.
- در این دوره اطلاعات و اسناد به صورت دسته ای به مرکز ارسال و شبانه پردازش بر روی آنها انجام می گردید.
- سیستمهای کامپیوتری در این دوره تاثیری در جهت رفاه مشتریان بانکها بر جای نگذاشت و تنها تاثیر این سیستمها در آن دوره ایجاد دقت و سرعت در موازنه حسابها بود.

اتوماسیون جلوی باجه

- آغاز این دوره به اواخر دهه ۱۹۷۰ میلادی بر می گردد.
- در این دوره کارمند شعبه در حضور مشتری عملیات بانکی را به صورت الکترونیکی ثبت و دنبال می کرد.
- در این دوره کارمندان شعبه قادر شدند به صورت پیوسته به حسابهای جاری دسترسی داشته باشند و بانکها برای نیل به اتوماسیون جلوی باجه، از شبکه های محابراتی موجود که در اختیار و انحصار شرکتهای دولتی بود و استفاده از آنها نه تنها از نظر فناوری محدود، بلکه به لحاظ هزینه ای بسیاری گزاف بود، استفاده نمایند.
- شبکه های مخابراتی، ترمینالهای بانکی شعب را به مراکز رایانه ای متصل می ساخت.
- در این دوره اتوماسیون، هیچ تاثیری در کاهش کارمندان بانکی نداشت.
- نرم افزارها و سیستم های بکارگرفته شده همچنان غیر یکپارچه و جزیره ای بودند.

متصل کردن مشتریان به حسابهایشان

- آغاز این دوره به اواسط دهه ۱۹۸۰ میلادی بر می گردد.

- در این دوره مشتریان از طریق ابزارهایی همچون تلفن و دستگاه های ATM به حسابهایشان دسترسی پیدا می کردند.
- دراین دوره در کنار عملیات دریافت و پرداخت، مشتریان خود می توانستند به صورت الکترونیکی به نقل و انتقال وجوه بپردازند.
- در این دوره شعب بانکها به تدریج خالی از صفهای طولانی مراجعین می شود و آن دسته از کارمندانی که در جلوی باجه به امور دریافت و پرداخت حسابهای مشغول بودند به بخشهای دیگر منتقل می گردند.
- مهمترین ویژگی های این دوره که آنرا از دوره های قبل متمایز می سازد عبارتند از توسعه جزیره ای سیستمهای مکانیزه در جلوی باجه و پشت باجه و همچنین توسعه سیستمهای ارتباطی مشتریان با حسابهایشان همچون خودپرداز، تلفن بانک، فکس بانک و ...
- در این دوره تمام عملیات بانکی الکترونیکی نشده و همچنان نیروی انسانی در ایجاد ارتباط میان سیستمهای جزیره ای نقش حیاتی ایفا می کند.

یکپارچه سازی سیستمها و مرتبط سازی مشتری با کلیه عملیات بانکی

- در این دوره کلیه خدمات بانکی که در دوره های قبل از جلوی باجه ارائه می گردید، با حذف کارمند باجه به صورت الکترونیکی از طریق شبکه های کامپیوتری فراهم می گردد.
- تمام رویه ها و متدهای سنتی مرسوم در نظام بانکداری در این دوره با معادل های الکتورنیکی خود جایگزین می گردند. همچون پول، سکه، چک، سفته و ...
- یکپارچگی سیستمهای بانکی و ظهور تکنولوژیهایی همچون شبکه اینترنت و شبکه Mobile موجب ظهور پدیده هایی همچون بانکداری تلفن همراه یا Mobile Banking، بانکداری اینترنتی، بانکداری خانگی یا Home Banking و بانکداری مجازی یا Cyber Banking گردیده است.
- تحولات و پیشرفتها در این دوره همچنان ادامه دارد.

مقایسه بانکداری سنتی و بانکداری الکترونیکی

بانکداری نوین (الکترونیکی)	بانکداری سنتی
بازار نا محدود	بازار محدود

ارائه خدمات گسترده	ارائه خدمات محدود
هزینه سرمایه گذاری کم	هزینه سرمایه گذاری زیاد
هزینه توسعه کم	هزینه توسعه زیاد
کسب درآمد از طریق ارزش افزوده	کسب درآمد از طریق حاشیه سود
نامحدود	محدود به ساعات اداری
ارتباطات یکپارچه	عدم وجود ارتباط بین بانکی
نیروی کار کم و پر بازده	نیروی شاغل زیاد و غیر بازده

انتقال الکترونیکی وجوه – Electronic Funds Transfer (EFT)(اسلاید ۱۴ – حتما سوال داریم)

سیستم انتقال وجه به مجموعه ای از فعالیتها اطلاق می شود که بوسیله بانک ها و موسسات دیگر از قبیل اتاق پایاپای جهت انتقال وجه بین بانکها صورت می پذیرد. حال اگر این فعالیتها بر مبنای کاغذ استوار باشد به آن انتقال دستی وجوه و اگر مبتنی بر شبکه های کامپیوتری به صورت الکترونیکی انجام گیرد به آن انتقال الکترونیکی وجوه می گویند.

بی شک امروزه یکی از مهمتریت وظایف بانکها و موسسات مالی انتقال وجه می باشد. امروزه در کشورهای توسعه یافته از اسکناس و سکه تنها برای پرداختهای خرد و کوچک استفاده می گردد. در حال حاضر شکل رایج انتقال وجه در ایران به صورت دستی است.

شروع بکارگیری و توسعه سیستمهای انتقال الکترونیکی وجوه به دهه ۶۰ میلادی در آمریکا و اروپا بر می گردد. در این دوران در سطحی محدود جهت بهره گیری از کارتهای اعتباری، مکانیزم های جدید اتاق پایاپای الکترونیکی به وجود آمد.

گسترش فراکیر سیستمهای انتقال الکترونیکی وجوه به دهه ۹۰ میلادی با ظهور اینترنت بر می گردد.

هنوز اتفاق نظری در خصوص محدوده تعریف *EFT* شکل نگرفته است. بعضی آنرا بخشی از بانکداری الکترونیکی می دانند در حالیکه بعضی دیگر بانکداری الکترونیکی را در دل *EFT* می دانند.

انتقال الکترونیکی وجوه – Electronic Funds Transfer (EFT)

- تعریف مندرج در قوانین بازرگانی آمریکا: انتقال الکترونیکی وجوه عبارت است از یک شبکه انتقال، اطاق پایاپای خودکار و سایر نظامهای ارتباطی اطاق پایاپای که از آن طریق یک دستور پرداخت بانکی، به بانک مخاطب مخابره و ارسال می گردد.

- تعریف دیگر: انتقال الکترونیکی وجوه عبارت است از هر نوع انتقال وجه به غیر از شیوه های سنتی مثل چک، وجه نقد و سایر ابزارهای کاغذی مشابه، که از طریق یک ترمینال الکترونیکی، تلفن، کامپیوتر، نوارهای مغناطیسی به منظور سفارش، اطلاع و صدور مجوز به موسسه مالی برای بدهکاری و بستانکاری یک حساب صورت می گیرد.
- تعریف دیگر: انتقال الکترونیکی وجوه شامل انتقال وجه بین حسابها، بانکها و سایر موسسات مالی با استفاده یا بدون استفاده از اتاق پایاپای خودکار (*Automatic Clearing House*)، از طریق بکارگیری ترمینال الکترونیکی، تلفن، کامپیوتر، دستگاه های *POS* (*Point of Sale*)، دستگاه های *ATM* و یا هر وسیله الکترونیکی دیگر می گردد.

مزایا و ویژگیهای EFT

- امنیت
- سرعت
- سادگی و تسهیل انتقال
- هزینه پایین
- حذف اشتباهات انسانی
- بهره وری و کارایی
- بهبود مدیریت وجوه و نقدینگی
- بهبود روابط با مشتریان

روشهای انتقال وجه :

- **انتقال اعتبار:**

عبارتست از روشی که در آن وجوه از طریق فرستنده انتقال برای گیرنده انتقال ارسال می شود. اگر هر دو دارای حساب بانکی باشند، فرستنده به بانک خود دستور می دهد تا حساب او را بدهکار و حساب گیرنده را در بانک طرف گیرنده بستانکار نماید. اگر فرستنده دارای حساب نباشد، پول را نقدا پرداخت می کند و اگر گیرنده دارای حساب نباشد، بانک طرف گیرنده متعهد می شود تا پول را نقدا در اختیار گیرنده قرار دهد.

- **انتقال بدهکار:**

انتقال بدهکار که گاهی به آن جمع آوری مطالبات نیز گفته می شود عبارت است از اخذ اعتبار بوسیله گیرنده ار انتقال دهنده. در این مکانیزم، گیرنده به بانک طرف خود دستور می دهد تا مبلغ خاصی را از حساب انتقال دهنده به حساب او انتقال دهد.

بانکداری الکترونیکی(۲۱ مهم هم فارسی هم واژه های انگلیسی اش- تست دارد)

- بانکداری الکترونیکی مصرف کننده
  - ماشین خودپرداز – ATM

- پایانه فروش – Point of Sale (POS)
- بانکداری تلفنی – Telephone Banking
  - واکنش صوتی – Voice Response
  - تشخیص صدا – Voice Recognition
  - تلفن های قابل برنامه ریزی – Programmable Telephone
- بانکداری اینترنتی – Internet Banking یا بانکداری خانگی / دفتری – Home/Office Banking

بانکداری الکترونیکی بین بانکی

- شبکه بین بانکی بین المللی SWIFT - Society for World Wide Interbank Financial Telecommunications
- شبکه بین بانکی CHIPS در آمریکا – Clearing House Interbank Payment System
- شبکه بین بانکی CHAPS در انگلستان – Clearing House Interbank Payment System
- شبکه بین بانکی RENTAS در مالزی – Real-Time Electronic Transfer of Fund and Securities

شبکه سوئیفت - SWIFT (۲۳ مهم تست دارد)

- مبادلات و پرداختهای بین المللی حداقل از دو طریق صورت می گیرد :
  - کارت های بانکی بین المللی
  - شبکه سوئیفت
- سوئیفت یک شبکه بین المللی ارتباط مالی بین بانکی است که تسهیلات و خدمات ویژه ای را از طریق مراکز رایانه ای در سراسر دنیا ارائه می دهد. سیستم مزبور به صورت چند کاربره بوده و موسسه آن به صورت شرکت تعاونی اداره می شود و بانکهای عضو در آن دارای سهام بوده و در سود موسسه سهیم هستند.

مزایای و اهمیت شبکه سوئیفت

- **استاندارد بودن** پیش از پیدایش این شبکه پیغامهای مالی توسط تلکس ارسال می گردید که از استاندارد مشخصی برخوردار نبود.
- **سرعت ارسال** پیامهای مالی در کمتر از چند ثانیه.

- **<u>قابلیت اطمینان</u>** کلیه الگوریتم های مربوط به رمزنگاری و رمز گشایی در شبکه تعبیه شده است.
- **<u>گستردگی تعداد</u>** ۲۸۰۰ بانک و ۶۰۰۰ موسسه مالی تا سال ۲۰۰۰ در این موسسه عضو بوده اند و به طور متوسط ارزش پیامهای مالی آن در روز به بیش از ۵ تریلیون دلار می رسد.
- **<u>هزینه کم</u>** هزینه مخابره هر پیام در شبکه سوئیفت برای ایران در حدود ۸ فرانک بلژیک است که در حدود یک سوم هزینه ارسال پیام از طریق تلکس است.
- **<u>امنیت</u>** سوئیفت با بهره گیری از شبکه های خصوصی مجازی بستر امنی را برای ارتباطات فراهم کرده است و تاکنون گزارشی مبنی بر سوء استفاده از این شبکه منتشر نشده است.

پرداخت الکترونیکی – Electronic Payment(۲۸ عناصر اصلی مهم)

پرداخت الکترونیکی عبارتست از انجام پرداخت از سوی یک شخص به شخص دیگر از طریق شبکه های رایانه ای بدون اینکه نیاز به دیدار طرفین باشد.

عناصر اصلی در پرداخت الکترونیکی

- بانک یا موسسه تحصیل دار Acquirer Bank
- بانک یا موسسه گشایشگر Issuer Bank
- موسسه صادر کننده کارت
- مشتری یا پرداخت کننده یا خریدار Buyer/Customer/Payer
- بازرگان یا دریافت کننده یا فروشنده Payee/Seller/Merchant
- قانون گذار یا Regulator

اعتماد در پرداخت الکترونیکی(۲۹ – مهم – انکارناپذیری مهمتر)

- *Privacy* به معنای محرمانگی و وجود حریم شخصی می باشد. بعضی اوقات تحت عنوان *Confidentiality* نیز مطرح می شود و به معنای آن است که گروههای درگیر در پرداخت باید مطمئن باشند که جزئیات معاملات بین آنها کاملا محرمانه می ماند و برای کاربردهای دیگر استفاده نمی شود.
- *Authentication* به معنای هویت شناسی است و بدین معنا ست که خریداران، فروشندگان و واسطه های دیگر مطمئن باشند که مشارکت کنندگان در فرآیند پرداخت الکترونیکی همان کسانی هستند که ادعا می کنند و باید هویت آنها تایید شود.

- *Integrity* به معنای یکپارچگی (صحت) بوده و مفهوم آن است که داده ها و اسناد پرداخت الکترونیکی توسط افراد غیر مجاز قابل دستکاری نباشند.
- *Non repudiation* انکارناپذیری به مفهوم آن که هیچ کدام از دست اندرکاران پرداخت الکترونیکی نمی توانند معاملات خودشان را انکار یا شانه خالی کنند.
- ویژگیهای سیستمهای پرداخت الکترونیکی
- *Ease of use* یا راحتی استفاده توسط کاربر راحت بتوان از آن استفاده نمود.
- *Scalability* یا مقیاس پذیری زیر ساخت نرم افزاري و سخت افزاري مقیاس پذیر باشد و با افزایش تعداد مشتریان کارايي سیستم پائین نیاید.
- *Transaction Fees* یا دستمزد انجام معاملات زمانی که از کارت اعتباری برای پرداخت الکترونیکی استفاده می شود، فروشنده باید حدود۳% قیمت فروش کالا یا خدمت را به عنوان دستمزد به بانک واسط یا بانک فروشنده ،موسسه کارت اعتباری وموسسه گشایشگر ... پرداخت کند.
- *Trackability* یا قابلیت ردگیری بسادگي بتوان جریان پول را ردگیري کردکه امکان تقلب کمتر می شود.

روشهای انتقال پول در پرداخت الکترونیکی

- **پرداخت از طریق حسابهای بانکی** که به واسطه بانک فعال می گردد و به دو روش زیر می باشد
  - **پیش پرداخت مشتری** قبلا پولی را به حساب خودش می ریزد و در موقع انجام معامله از آن پول کسر می گردد
  - **پرداخت به شیوه اعتباری مشتري به جای پول**، اعتباری در بانک دارد که با آن اعتبار معامله انجام می شود و بانک پرداخت را انجام داده سپس صورت حساب را ارسال می کند تا مشتري با مراجعه به بانك بپردازد
- **پرداخت به صورت مستقیم** که مشتری مستقیم با خود فروشنده ارتباط دارد مثلا اعتبار را مستقیم از فروشنده خريد مي‌كند.

روشهای پرداخت الکترونیکی

- کارتهای الکترونیکی یا *E-CARDS* که عبارتند از:
  - کارتهای اعتباری *Credit Cards* مانند *Visa Card , Master Card*

- شارژکارتها *Charge Cards* مانند *American Express*
- کارتهای بدهی *Debit Cards*

- کارتهای خرید یا *Purchase Cards*
- پول الکترونیکی یا *E-cash , Digital Money , Digicash*
- پرداخت های شخص به شخص یا *P2P*
- چک های الکترونیکی یا *E-checking* مانند *ECheckSecure.Com*
- صورتحساب الکترونیکی یا *E-billing*
- انتقال الکترونیکی وجوه یا *Electronic funds transfer*

پول الکترونیکی یا E-Cash

در پرداختهای خرد بدلیل حق العمل بالای کارتهای اعتباری، استفاده از کارتهای اعتباری مقرون به صرفه نیست.

براي مواردی است که قیمت پایین است و پرداختها خرد است که ابتدا خریدار مبلغی پول الکترونیکی را خرید کرده و مورد استفاده قرار مي‌دهد.

از مزایای پول الکترونیکی می توان به عدم محدودیت در استفاده از آن اشاره نمود.

ردیابی مالیاتی در پول الکترونیکی سخت است.

نمونه های پول الکترونیکی:

- ECoin.Net
- Stored-Value Cards
- VISA CASH
- DigiCash
- CyberCoins

کیف پول الکترونیکی یا E-Wallet

اگر خریدار اطلاعات کارت اعتباری خود را شبیه نام، آدرس، اطلاعات کارت اعتباری و ... را برای هر یک از خریدهای خودش به صورت مکرر وارد کند خسته کننده است. ۲ روش براي جلوگيري از مشکل وجود دارد :

- فروشندگان یک بار اطلاعات خریدار را دریافت کرده و روی Server خود نگهداری می کنند تا برای استفاده های بعدی لزومی به ورود مجدد نباشد. مثلا در سایت Amazon.com سرویس One Click این کار را انجام می دهد.
- از نرم افزار E-wallet استفاده شود که بر روی کامپیوتر خریدار نصب می شود و خریدار یک بار اطلاعات خودش را وارد می کند و برای خریدهای الکترونیکی بعدي این نرم افزار مورد استفاده قرار می گیرد. این نرم‌افزار توسط فروشنده نیز باید مورد قبول واقع شود.
- کیف پول الکترونیکي در VISA.COM, MASTERCARD.COM, YAHOO.COM

کارت هوشمند Smart Card

کارتي پلاستیکي با ابعاد تقریبي ۵/۵ در ۸/۵ سانت که روي آن یا در بین لایه‌هاي کارت تراشه‌اي قرار داده شده‌است که قابلیت ذخیره سازي/ پردازش اطلاعات را دارد.

انواع کارت هوشمند

- **<u>از حیث نحوه ارتباط کارت با کارتخوان</u>**
  - کارت هوشمند تماسي یا *Contact Card*
  - کارت هوشمند غیر تماسي یا *Contactless Card*
    - کارتهاي فعال یا *Active* (فاصله عملکرد تا چند متر)
    - کارتهاي غیر فعال یا *Passive*
      - *Closed Couple* (فاصله کمتر از يك سانت)
      - *Proximity* (فاصله حدود چند سانتي متر)
      - *Vicinity* (حدود يك متر)
  - کارت هوشمند ترکیبي یا *Combi Card*
- **<u>از حیث نوع تراشه بکار رفته در کارت</u>**
  - کارت با حافظه ساده *(PROM و EEPROM)*
  - کارت با حافظه هوشمند
  - کارت هوشمند میکروکنترلی
  - کارت هوشمند کریپتوکنترلی

نواحي مختلف حافظه کارت هوشمند

- ناحیه آزاد
- ناحیه محرمانه

- ناحيه سري

سيستم عامل كارت هوشمند

برنامه‌اي است با حجم كم چند كيلوبايتي كه وظايف ذيل را انجام مي‌دهد

- انتقال داده‌ها از/ به كارت هوشمند
- كنترل اجراي دستورات
- مديريت فايلها
- مديريت و اجراي الگوريتم‌هاي رمزنگاري

نمونه هايي از سيستم عامل كارت هوشمند

- Microsoft Windows For Smart Card
- JavaCard
- MST(IBM)
- MIKADO
- OSCAR

مزاياي كارت هوشمند نسبت به ساير كارتها

- اندازه كوچك
- امنيت
- حجم اطلاعات قابل حمل نسبت به كارتهاي مغناطيسي
- انعطاف‌پذيري
- طول عمر و دوام زياد

كاربردهاي كارت هوشمند

- كاربردهاي شناسايي شبيه‌كارتهاي كنترل تردد، كارتهاي عضويت، و..
- كاربردهاي مالي شبيه كارتهاي اعتباري، كارتهاي تلفن همگاني، كارتهاي پرداخت شبكه تلويزيوني و..

- کاربردهاي نگهداري اطلاعات شبيه کارتهاي گواهينامه هوشمند، کارتهاي درمان، ..

مقدمه ای بر امنیت سیستمهای پرداخت

مشکلات امنیتی در سیستمهای پرداخت سنتی

- تولید پول تقلبی
- جعل امضاء
- برگشت چک

مسائل امنیتی در سیستمهای پرداخت الکترونیکی

- تولید پول تقلبی
- جعل امضاء
- برگشت چک
- کپی اسناد دیجیتال
- ردیابی فعالیتهای مالی افراد

نگرانیهای رایج در سیستم های پرداخت الکترونیکی

- هکرهای غیر فعال که به شنود اطلاعات مالی افراد می پردازند.
- هکرهای فعال که از طریق حملات فعال سعی در وارد آوردن صدمه به کاربران را دارند.
- وجود عناصر متقلب در سیستمهای پرداخت الکترونیکی.

دسته بندی سرویسهای امنیتی در سیستمهای پرداخت الکترونیکی

- سرویسهای امنیتی تراکنشهای پرداخت – Payment Transaction Security Services
- سرویسهای امنیتی کارت الکترونیکی – Electronic Cards Security Services
- سرویسهای امنیتی پول الکترونیکی - Digital Money Security Services
- سرویسهای امنیتی چک الکترونیکی – ecking Security Services

Session10

تعاریف سازمانهای بین المللی(۳ مهم – همه کشورها مهم – بخصوص ژاپن و آمریکا- سوال داریم)

- سازمان همکاری و توسعه اقتصادی(OECD): ۱۹۸۳ تعریف سوء استفاده رایانه ای:

" سوء استفاده رایانه ای عبارتست از هر رفتار غیر قانونی، غیر اخلاقی یا غیر مجاز مربوط به پردازش خودکار و انتقال داده ها."

کنوانسیون جرم سایبر

- کنوانسیون جرم سایبر یک سند بین المللی است که موضوع آن جرم رایانه ای است.
- در سال ۲۰۰۱ با حضور ۲۴ کشور عضو شورای اروپا، آمریکا، ژاپن، کانادا، و آفریقای جنوبی در بوداپست
- عبارت کلی تر جرم *سایبر* مطرح شد که جرم *رایانه ای* یکی از زیر مجموعه های آن است.

تعاریف نظامهای حقوقی کشورهای مختلف

تعریف جرم رایانه ای در آمریکا

- اشکال ارتکاب جرم رایانه ای(جیمز رابینسون ۲۰۰۰):
  - رایانه بعنوان هدف و موضوع جرم، مثل سرقت اطلاعات، هک کردن
  - رایانه بعنوان وسیله ارتکاب جرم، مثل کلاهبرداری رایانه ای، جعل رایانه ای و هرزه نگاری
  - گاهی رایانه هدف و یا وسیله ارتکاب جرم نیست بلکه بهمراه یک جرم در مسیر حرکت مجرمانه قرار میگیرد.
- تعریف وزارت دادگستری آمریکا: " جرم رایانه ای عبارتست از هر اقدام غیر قانونی که برای ارتکاب، پی جوئی، یا پیگرد قضائی آن، بهره برداری از دانش فناوری رایانه ای رایانه ای ضروری است. "

تعریف جرم رایانه ای در کانادا

- " جرم رایانه ای عبارتست از هر نوع فعالیت مجرمانه ای که در برگیرنده کپی، استفاده، جابجائی، ملاحظه، دسترسی یا سوء استفاده از سیستمهای رایانه ای، عملکرد رایانه، عملکرد رایانه ها، داده ها یا برنامه های رایانه ای است."

تعریف جرم رایانه ای در آلمان

- " جرم رایانه ای همه شرایطی را که پردازش الکترونیکی داده ها وسیله یا موضوعی برای ارتکاب جرم یا تخلف باشد و بیانگر دلایلی برای ظن به ارتکاب جرم است، در بر می گیرد."

تعریف جرم رایانه ای در ژاپن

- تعریف رسمی کارگزاری پلیس ملی ژاپن: " جرم رایانه ای عبارتست از جرمهای در برگیرنده اعمال همراه با بی مبالاتی یا حوادثی که عملکرد یک سیستم رایانه ای را مختل کرده یا از آن استفاده غیر قانونی می کند."
- جرمهائی که تا ۱۹۹۰ پلیس ژاپن شناخته است:
  - تخریب سخت افزار
  - تخریب نوارها و دیسکت ها
  - کذب سازی یا محو داده ها
  - استفاده غیر قانونی از سخت افزار
  - سرقت داده ها و برنامه ها
- چهار دسته جرم کامپیوتری در ژاپن:
  - سرقت داده های رایانه ای
  - سوء استفاده از داده های رایانه ای
  - استفاده غیر مجاز از رایانه
  - خرابکاری رایانه ای

تعریف جرم رایانه ای در هلند

- "رفتاری که بطور بالقوه آسیب رسان است و به واسطه هائی که برای ذخیره سازی، پردازش یا انتقال داده ها از رایانه کمک می گیرند، مربوط می شود."
- پلیس این جرمها را به دو دسته تقسیم کرده است:
  - زمانی که رایانه به منزله هدف جرم باشد.
  - زمانی که رایانه بمنزله وسیله جرم باشد.

تعریف جرم رایانه ای در فرانسه

- تقسیم بندی تحلیلی از جرم رایانه ای(از نظر نتیجه عمل)
  - جرمها علیه اشخاص (آسیب به آزادیها و حقوق خصوصی)
  - جرمهای علیه اموال (جرمهای علیه تجهیزات الکترونیکی و اطلاعات)

طبقه بندی جرمهای رایانه ای

طبقه بندی OECD

- وارد کردن، تغییر دادن، پاک کردن یا متوقف سازی داده ها یا برنامه های رایانه ای که بطور عمدی و با قصد:
  - انتقال غیر قانونی وجه یا هر چیز با ارزش دیگر
  - ارتکاب جعل
  - جلوگیری از عملکرد سیستم رایانه ای و مخابراتی

صورت بگیرد

- تجاوز به حقوق انحصاری ثبت شده مالک یک برنامه رایانه ای حمایت شده به قصد بهره برداری تجاری و ارائه آن به بازار
- دستیابی یا شنود آگاهانه در سیستم رایانه ای یا ارتباطی به طور آگاهانه و بدون کسب مجوز از افراد سیستم مزبور، اعم از آنکه با تخطی از تدابیر امنیتی صورت بگیرد یا با هدف غیر شرافتمندانه.

طبقه بندی شورای اروپا

<u>الف) فهرست حداقل در توصیه نامه (R89)</u>

۱. کلاهبرداری رایانه ای
۲. جعل رایانه ای
۳. وارد کردن خسارت به داده ها یا برنامه های رایانه ای
٤. خرابکاری رایانه ای
٥. دستیابی غیر مجاز رایانه ای
٦. شنود غیر مجاز رایانه ای
۷. تکثیر غیر مجاز برنامه حمایت شده رایانه ای
۸. تکثیر غیر مجاز یک نیمه هادی

<u>ب) فهرست اختیاری در توصیه نامه (R89)</u>

۱. تغییر داده ها یا برنامه های رایانه ای
۲. جاسوسی رایانه ای
۳. استفاده غیر مجاز از رایانه

٤. استفاده غیر مجاز از یک برنامه حمایت شده رایانه ای

اینترپل(۲۰ مهم)

- دسترسی غیر مجاز
  - نفوذ غیر مجاز
  - شنود غیر مجاز
  - سرقت زمان رایانه
- تغییر داده های رایانه ای از رهگذر
  - بمب منطقی
  - اسب تراوا
  - ویروس
  - کرم
- کلاهبرداری رایانه ای
  - سوء استفاده از خودپردازها
  - جعل رایانه ای
  - سوء استفاده از ماشینهای بازی
  - دستکاری در مرحله ورودی و خروجی
  - سوء استفاده از ابزار پرداخت مستقر در فروشگاهها
  - سوء استفاده تلفنی
- تکثیر غیر مجاز
  - تکثیر بازیهای رایانه ای
  - تکثیر نیمه هادی
  - تکثیر نرم افزارهای دیگر

- خرابکاری رایانه ای
  - خراب کردن سخت افزار
  - خراب کردن نرم افزار
- سایر جرمهای رایانه ای

- سرقت اسرار تجاری(فاش، انتقال و استفاده)
- ذخیره سازی هرزه نگاری کودک و سایر نرم افزارهای غیر قانونی
- سایر موضوعهای تعقیب شدنی

کنوانسیون جرم سایبر(بوداپست، ۲۰۰۱)(۲۲ مهم)

- جرمهای علیه محرمانگی، تمامیت و در دسترس بودن داده ها و سیستمهای رایانه ای
  - دسترسی عمدی و غیر مجاز به سیستم رایانه ای
  - شنود عمودی و غیر مجاز داده های رایانه ای
  - ایجاد اخلال عمدی و غیر مجاز در داده های رایانه ای
  - سوء استفاده از وسایل، رمز عبور، کد دستیابی یا داده ها یا برنامه های رایانه ای
- جرمهای مرتبط با رایانه
  - جعل مرتبط با رایانه
  - کلاهبرداری مرتبط با رایانه
- جرمهای مرتبط با محتوی
  - تولید هرزه نگاری کودک به قصد انتشار در سیستم رایانه
  - ارائه هرزه نگاری کودک از رهگذر سیستم رایانه
  - تهیه هرزه نگاری کودک از رهگذر سیستم رایانه
- جرمهای مرتبط با نقض حق مولف
  - جرمهای مرتبط با حق مولف
  - جرمهای مرتبط با حقوق مربوط به حق مولف

داد و ستد الکترونیکی

حصول اطمینان از :

۱. شناسائی هویت واقعی فرستنده پیام الکترونیکی
۲. تمامیت داده ها (manipulation)

۳. عدم قابلیت انکار(non-repudiation)
٤. حفظ محرمانگی(confidentiality): نقش امضای الکترونیکی
٥. حمایت از داده ها(data protection): حفظ حریم خصوصی

امضای الکترونیکی(اسلاید ۴۸ -صددرصد سوال)

- ماده ۲-۹ قانون تجارت الکترونیکی جمهوری اسلامی ایران:
  - امضای الکترونیکی عبارت از هر نوع علامت منضم شده یا به نحو منطقی متصل شده به داده پیام است که برای شناسائی امضا کننده داده پیام مورد استفاده قرار می گیرد. دراین قانون به رکن روانی امضا یعنی قصد التزام امضا کننده به مفاد سند اشاره ای نشده است.

امضای الکترونیکی ایمن

- در قانون فرانسه امضای الکترونیکی با شرایط ذیل امضای ایمن نامیده می شود:
  - بطور انحصاری متعلق به امضا کننده باشد.
  - با سازوکارهائی ایجاد شده باشد که امضا کننده بتواند آنها را تحت کنترل انحصاری خود بگیرد.
  - چنان رابطه ای بین امضا و متن باشد که تغییرات بعدی سند قابل کشف باشد.
- ماده ۱۰ قانون تجارت الکترونیکی جمهوری اسلامی ایران شرایط زیر را برای امضای الکترونیکی مطمئن ضروری میداند:
  - نسبت به امضا کننده منحصر بفرد باشد
  - هویت امضا کننده داده پیام را مشخص کند
  - به وسیله امضا کننده و یا تحت اراده انحصاری وی صادر شده باشد.
  - به نحوی به داده پیام متصل باشد که هر تغییری در آن داده پیام قابل کشف باشد.

انواع امضاهای الکترونیکی

۱. **<u>دسته بندی برمبنای بکارگیری یاعدم بکارگیری رمزنگاری:</u>**

۱/۱. امضاهای الکترونیکی بر مبنای رمزنگاری که دریافت کننده پیام آنرا برای اهداف زیر بکار می گیرد: تبدیل متن کدگذاری شده به شکل اصلی و رمز نگاری نشده آن، تشخیص هویت فرستنده پیام، تشخیص تمامیت داده ها یا عدم آن، ترکیبی از موارد فوق

۱/۲. امضاهای الکترونیکی غیر مبتنی بر رمز نگاری: مثل امضای اسکن شده، یا بکار گیری biometric identifiers

۲. تقسیم بندی بر مبنای سطح ایمنی فراهم شده:

امضاهای الکترونیکی از نظر سطح ایمنی که فراهم می کنند متفاوت اند. بر پایه ماده ۲-۲ دستورالعمل امضاهای الکترونیکی اتحادیه اروپا "امضاهای الکترونیکی پیشرفته" شرایط زیر را دارد:

- بطور انحصاری با امضا کننده مرتبط باشد
- شناسائی امضا کننده را ممکن سازد
- از بکارگیری ابزاری ایجاد شده باشد که امضا کننده بتواند آنها را بطور انحصاری تحت کنترل خود درآورد و
- با داده هائی که به آنها مربوط می شود، بگونه ای مرتبط باشد که هرگونه تغییر بعدی در این داده ها کشف شدنی باشد.

یکی از شرایط پذیرفتن امضای الکترونیکی در دادگاه، "پیشرفته بودن " آن به معنای فوق است.