## مقدمه

وجود بازارها، پاساژها و مغازه های مجازی که هیچ مکان فیزیکی را اشغال نکرده اند و در عین حال امکان بازدید و گردش در این بازارها به صورت لحظه ای و در هر نقطه از جهان بدون ترک منزل میسر است و نیز انتخاب و سفارش خرید کالاهایی که در نقاط نامعلومی از جهان در ویترین های مغازه های مجازی قرار دارند و بر روی شبکه مجازی نیز تبلیغ می شوند از طریق پرداخت های الکترونیکی فراهم شده است. همه این گزینه ها سبب شده اند که تجارت الکترونیکی (E-Commerce) معجزه قرن تلقی شود.

بدیهی است با ظهور تجارت الکترونیکی و به ویژه نقل و انتقالات مالی در این بستر امنیت در این حوزه اهمیت بالایی پیدا میکند. پیش از پرداختن به مقوله امنیت مروری بر مفاهیم اولیه تجارت الکترونیک خواهیم داشت:

# مروری بر مفاهیم اولیه تجارت الکترونیکی

## تجارت الکترونیکی

تجارت الکترونیک مجموعه ارتباطات، مدیریت اطلاعات و قابلیت های امنیتی است که به سازمان ها ، بنگاه ها ،شرکت ها ،عامه مردم ،دولت و .....اجازه می دهد که اطلاعات، خدمات و کالاهای خود را بهینه تر آسان تر و سریع تر با استفاده از شبکه های ارتباطی کامپیوتری، به ویژه اینترنت عرضه دارند .تجارت الکترونیک، تجارت بدون کاغذ است .به وسیله تجارت الکترونیک تبادل اطلاعات، خرید و فروش و حمل و نقل کالاها، با زحمت کمتری انجام می گیرد.

تجارت الکترونیک عبارت است از خرید (buy) و فروش (sell) و مبادله (Exchange) کالا(product) ، خدمات (services)و اطلاعات (Information) از طریق شبکه های رایانه ای از جمله اینترنت .

## تاریخچه تجارت الکترونیک

۱۹۷۹ Michael Aldrich : خرید آنلاین را اختراع کرد

۱۹۸۱ Thomson Holidays : اولین خرید انلاین B2B را در بریتانیا ایجاد کرد.

۱۹۸۲ Minitel : سیستم سراسر کشور در فرانسه بوسیله France Telecom و برای سفارش گیری انلاین استفاده شد.

۱۹۸۴ Gateshead : اولین خرید انلاینB2C را بنام SIS/Tesco و خانم Snowball در ۷۲ اولین روش خانگی انلاین را راه انداخت.

۱۹۸۵ Nissan : فروش ماشین و سرمایه گذاری با بررسی اعتبار مشتری به صورت انلاین از طریق نمایندگیهای فروش

۱۹۸۷ Swreg : شروع به فراهم اوردن ومولفه های اشتراک افزار و نرم افزار به منظور فروش انلاین محصولاتشان از طریق مکانیسم حسابهای الکترونیکی بازرگانی.

۱۹۹۰ Tim Berners-Lee : اولین مرورگر وب را نوشت، وب جهان گستر (www)

۱۹۹۴ : راهبر وب گرد Netscape : در اکتبر با نام تجاری Mozilla ارایه شد. Pizza Hut سفارش انلاین را در صفحه وب پیشنهاد داد .اولین بانک انلاین راه اندازی شد. تلاشها برای پیشنهاد تحویل گل و اشتراک مجله به صورت انلاین شروع شد. Netscape 1.0 در اواخر ۱۹۹۴ با رمز گذاری SSL که تعاملات مطمئن را ایجاد میکرد، معر فی شد.

۱۹۹۵ Amazon.com , Jeff Bezos : اولین تجارت ۲۴ ساعته رایگان را راه انداخت .ایستگاههای رادیوی اینترنتی رایگان، رادیو HK و رادیوهای شبکه ای شروع به پخش کردند. Dell و Cisco به شدت از اینترنت برای تعاملات تجاری استفاده کردند. eBay توسط Pierre Omidyar برنامه نویس کامپیوتر به عنوان وب سایت حراج بنیانگذاری شد.

۱۹۹۸ : توانایی خریداری و بارگذاری تمبر پستی الکترونیکی برای چاپ از اینترنت .گروه Alibaba در چین با خدمات B2B و C2C , B2C با سیستم خود تاییدی تاسیس شد.

۱۹۹۹ Business.com : به مبلغ ۷/۵ میلیون دلار به شرکتهای الکترونیکی فروخته شد. که در سال ۱۹۹۷ به مبلغ ۱۴۹،۰۰۰ دلار خریداری شده بود .نرم افزار اشتراک گذاری فایل Napster راه اندازی شد. فروشگاه های ATG برای فروش اقلام زینتی خانه به صورت انلاین راه اندازی شد.

۲۰۰۲ : ای بی برای پی پال ۱/۵ میلیون دلار بدست اورد .

۲۰۰۳ Amazon.com : اولین سود سالیانه خود را اعلان کرد.

۲۰۰۷ Business.com : بوسیله R.H. Donnelley به مبلغ ۳۴۵ میلیون دلار خریداری شد.

۲۰۰۹ Zappos.com : توسط Amazon.com با قیمت ۹۲۸ میلیون دلار خریداری شد.خرید اپراتورهای فروش وبسایتهای خصوصی RueLaLa.com بوسیله GSI Commerce به قیمت ۱۷۰ میلیون دلار بعلاوه سود فروش تا سال ۲۰۱۲

۲۰۱۰ Groupon : گزارش داد پیشنهاد ۶ میلیارد دلاری گوگل را رد کرده است .در عوض این گروه طرح خرید وب سایتگای IPO را تا اواسط ۲۰۱۱ دارد.

۲۰۱۱ : پروژه تجارت الکترونیک امریکا و خرده فروشی انلاین به ۱۹۷ میلیارد دلار رسیده است که نسبت به ۲۰۱۰ افزایش ۱۲ درصدی داشته است. Quidsi.com ، parent company of Diapers.com توسط Amazon.com به قیمت ۵۰۰ میلیون بعلاوه ۴۵ میلیون بدهکاری و تعهدات دیگر خریداری شد.

## زیرشاخه های تجارت الکترونیک

- مبادله و تحویل فوری مطالب دیجیتال
- انتقال الکترونیکی وجوه
- مبادله الکترونیکی سهام
- بارنامه الکترونیکی
- طرح های تجاری و مهندسی
- خدمات پس از فروش
- و غیره

تجارت الکترونیک دارای زیر شاخه‌های عمده‌ای به شرح زیر می‌باشد:

- تجارت الکترونیک
- کسب و کار الکترونیک
- بازاریابی الکترونیکی
- بانکداری الکترونیکی
- کارتهای هوشمند
- مدیریت روابط عمومی با مشتری

## مزایا و معایب تجارت الکترونیک

برخی از مهم ترین فواید تجارت های الکترونیکی را می توان به شرح زیر اعلام نمود:

۱. افزایش فروش و در پی آن افزایش درآمد و توان سرمایه گذاری افزایش سطح رفاه زندگی مردم از طریق ایجاد اشتغال، کاهش ترددها و افزایش سرعت عمل جهانی شدن کاهش هزینه‌های تبلیغات برای شرکتها وبه دلیل عدم حضور واسطه با افتتاح فروشگاه اینترنتی شما این قابلیت را دارید که با هزینه ای کم کالا و سرویس خود را در تمامی نقاط دنیا بازاریابی کنید و به فروش برسانید. در واقع شما مغازه ای دارید که در کل زمان روز و شب باز است و مراجعه کنندگان آن از تمام نقاط دنیا هستند! یعنی می توانید مطمین شوید که یک تجارت جهانی راه اندازی کرده اید.
۲. در تجارت الکترونیکی دیگر نیازی به واسطه و دلال برای فروش کالا،نیست وقتی که در خرید و فروش سنتی صرف رفت و آمد های اضافه میشد در تجارت الکترونیکی صرف شناسایی نیاز های مشتری شود.
۳. تجارت الکترونیکی وارد شدن به بازارهارا آسان کرده،خریدار اینترنتی میتواند تنها با یک اتصال اینترنت از سرتاسر دنیا به فروشگاه شما متصل می گردد.
۴. تجارت الکترونیکی موقعیت های تجاری جدید برای کارآفرینان را در اینترنت ایجاد می کند.

۵. با تجارت الکترونیک فروشنده قادر به تجزیه و تحلیل بهتر از نیاز های مشتری خواهد بود و خریدار اینترنتی قادر به ارزیابی بهتر قیمت ها و محصول مورد نیاز خود می باشد .

در مقابل تجارت های الکترونیکی معایبی نیز دارند، از جمله:

۱. تأثیر ناشناخته آن بر روابط اجتماعی انسان
۲. ورشکستگی به علت عدم توانایی شرکتهای کوچک و کاهش تولید
۳. بسترهای لازم برای تجارت الکترونیک
۴. یک سیستم بانکی روان و دقیق
۵. قوانین گمرکی،مالیاتی و بانکداری الکترونیکی
۶. کد تجاری محصول و ایجاد امنیت اطلاعات
۷. تهیه و تدوین نظام مالی اطلاعات و نظام حقوقی اطلاع رسانی (کپی رایت)
۸. محرمانه بودن اطلاعات شخصی
۹. تطبیق مقررات ملی با مقررات متحدالشکل بین المللی
۱۰. همکاری دانشگاهها،مراکز تحقیقاتی و سازمانهای مختلف
۱۱. پذیرش اسناد الکترونیکی توسط قوه قضاییه
۱۲. تأمین، صدور و بکارگیری کارت هوشمند
۱۳. تأمین خطوط ارتباطی پرسرعت و مطمئن و ایجاد بستر مخابراتی به شکل بی سیم.

## چارچوب های تجارت الکترونیک

چارچوب های تجارت الکترونیک از چند سطح تشکیل یافته است که برای داشتن تجارت الکترونیک موفق وجود این چارچوب ها لازم است:

۱. **زیر ساخت:** بخش اول از چارچوب های مورد نیاز تجارت الکترونیک شامل سخت افزار، نرم افزار، پایگاه های داده ای و ارتباطی است که برای انجام وظیفه در قالب خدمات worldwide web بر روی اینترنت و یا سایر روش های پیام گذاری و پیام گیری بر روی اینترنت و یا سایر شبکه ها به کار می رود.

۲. **خدمات:** بخش دوم از چارچوب ها شامل دامنه گسترده ای از خدمات که توانایی پیدا کردن و ارائه اطلاعات را فراهم می آورند و شامل جست وجو برای شرکای تجاری و همچنین مذاکره و توافق درمورد مبادلات تجاری هستند.

۳. **محصولات و ساختارهای تجارت الکترونیک:** این بخش از چارچوب های (E-Commerce) مشتمل بر پیش بینی و تدارک مستقیم کالاها و خدمات تجاری وابسته به اطلاعات برای مشتریان و شرکای تجاری،

همکاری و سهیم شدن در اطلاعات داخل و خارج سازمان و سازمان دهی محیط بازار الکترونیکی و زنجیره تهیه و پشتیبانی است.

## مراحل اعمال تجارت الکترونیک

مراحل رشد و گسترش تجارت الکترونیکی را می توان به بخش های زیر تقسیم کرد که هر چه به گام های پایانی تر نزدیک می شویم در حقیقت به تجارت الکترونیکی واقعی نزدیک تر شده ایم و شرکت ها و سازمان هایی که در جست وجوی بازار الکترونیکی برای کالاها و خدمات خود هستند، سعی در رسیدن به مراحل پایانی این چرخه دارند.

۱. **طراحی سایت:** در مرحله اول از مجموعه مراحل پنج گانه، شرکت یا سازمان متقاضی تجارت الکترونیک سعی در ایجاد یک سایت ساده شامل اطلاعات محصولات و خدمات تولیدی خود را دارد تا این اطلاعات از طریق اینترنت در اختیار مشتریان قرار بگیرد. در حقیقت، مرحله اول به معنای به وجود آمدن ویترینی بر روی شبکه جهانی وب برای بازدیدکنندگان است تا اطلاعات مورد نظر خود را از طریق این صفحات دریافت کنند.

۲. **توسعه و تکمیل بانک اطلاعاتی:** این مرحله شامل توسعه و گسترش مرحله اول است. در این مرحله سایت شرکت تبدیل به یک پایگاه داده ای (DataBase) قوی شده، برای نگهداری اطلاعات مورد استفاده قرار می گیرد، در این مرحله، اطلاعات همه محصولات و خدمات و شرح کامل آنها در بانک اطلاعات قرار می گیرد و کاربران امکان ارسال سفارش خرید از طریق این وب سایت را خواهند داشت، اما هنوز زیرساخت های لازم برای پرداخت اینترنتی فراهم نشده است و پرداخت پول به همان روش سنتی انجام خواهد گرفت.

۳. **ایجاد ساز و کارهای تعامل کاربران با سایت:** برقراری امکان تعامل از مهمترین نکات مرحله سوم است. در این مرحله، کاربران امکان تعامل با مدیر سایت را خواهند داشت که این تعامل از طریقe-mail ، chatو voice خواهد بود و کاربران در بازه زمانی بسیار کوتاه مدت پاسخ خود را از مدیر سایت دریافت خواهند کرد و امکان پرسش و پاسخ online میان فروشنده و خریدار و نیز رد و بدل شدن اطلاعات در مورد کالا و یا خدمات خواسته شده وجود دارد.

۴. **برقراری امکان پرداخت اینترنتی:** در این مرحله، امکان پرداخت اینترنتی برای کاربران فراهم خواهد شد و مشتریان پس از ارسال فرم های سفارش خرید و دریافت کالا، وجه موردنظر و توافق شده را از طریق پایانه های فروش بانک ها و مؤسسات مالی طرف قرارداد برای فروشنده ارسال خواهند کرد که این حمل و نقل پول به صورت بسیار امن از طریق اینترنت برای مشتریان فراهم خواهد شد.

۵. **یکپارچه سازی:** مرحله آخر که آخرین مرحله از مراحل پنج گانه است، به مرحله یکپارچگی معروف است. در این مرحله، سیستم های واسطه ای میان فروشنده و خریدار با سیستم های موجود در سازمان و یا شرکت به حالت یکپارچگی کامل درخواهند آمد. بدین معنا که اگر کالایی فروش رود، موجودی کالای فروش رفته به

میزان خریداری شده از موجودی انبار کسر شده و همزمان دستور خرید جدیدی برای جایگزین کردن کالای فروش رفته به انبار ارسال خواهد شد و در خریدهای بعدی موجودی انبار بلافاصله به نمایش درخواهد آمد. این مرحله از مجموعه مراحل تجارت الکترونیک کامل ترین مرحله در تجارت الکترونیکی است که در آن نتیجه همه عملیات مربوط به داد و ستد در همه سیستم های سازمان منعکس می شود.

## انواع مدل‌های تجارت الکترونیکی

استفاده از اینترنت به عنوان اصلی ترین بستر ارتباطی در تجارت الکترونیکی باعث به وجود آمدن مدل های گوناگونی در این سبک از تجارت شده است. این مدل ها که حاصل تعامل گروه های مختلف تجارت الکترونیکی یعنی دولت، مشتری و بنگاه های اقتصادی است، باعث توسعه و گسترش مدل های مختلف تجارت الکترونیک شده است. تجارت الکترونیکی بر مبنای نوع مبادلات شامل انواع زیر می باشد :

### تجارت بین بنگاهی ( B2B)

این نوع از تجارت الکترونیکی، انجام دادن تمام فعالیتهای تجاری بین دو یا چند بنگاه را در بر می گیرد، که به صورت الکترونیکی انجام می شود. فعالیتهایی از قبیل برگزاری مناقصات و مزایده ها ، عملیات بازاریابی، خرید و فروش که با اینترنت به سادگی قابل انجام است.

این مدل از تجارت الکترونیک مهمترین نوع تجارت الکترونیکی است که در حدود نصف درآمدهای تجارتی الکترونیکی را به خود اختصاص خواهد داد. این مدل سبب پیدایش ارتباطی گسترده میان تأمین کنندگان، تولیدکنندگان، توزیع کنندگان و فروشندگان خواهد بود. در این مدل، ارتباط میان دو یا چند سازمان ، توسعه اقتصادی، تولیدکنندگان مواد اولیه و ارائه کنندگان انواع گوناگون خدمات موردنظر است. در حقیقت، این مدل را به نوعی می توان توسعه یافته مدل قدیمی EDI (Electronic Data Interchange) دانست، اما در این مدل واسطه ها کاهش یافته، همین خود سبب کاهش قیمت ها خواهد شد.

### تجارت بین افراد و بنگاه (B2C , C2B)

این نوع تجارت الکترونیکی شامل فعالیتهای تجاری بین افراد و بنگاه است. اغلب این نوع فعالیتهای تجاری به صورت خرید محصولات اعم از کالا، خدمات، نرم افزار و بنگاه است. نمونه بارز این نوع از مبادلات خرید از خانه است، که افراد به واسطه آن می توانند از منزل یا محل کار خود به خرید مبادرت ورزند. همچنین سازمانها می توانند از خدمات افراد بهره گیرند. بدین صورت که افراد، عرضه کننده و سازمانها مصرف کننده هستند .

مدل های B2C و C2B بیان کننده ارتباط متقابل تولیدکننده و خریداران نهایی محصولات و خدمات است. مدل های دوگانه B2C و C2B دارای مزایایی مانند خرید ارزان تر کالا نسبت به دنیای واقعی، امکان ارسال خریداری شده به مکان درخواستی مشتری و غیره است. این مدل از تجارت الکترونیک به عنوان ساده ترین نوع تجارت الکترونیکی شناخته

می شود که منجر به ارتباط نزدیکی میان مشتری و فروشنده خواهد بود و در این میان به دلیل کاهش قیمت ها به دلیل از بین رفتن واسطه ها خریدار منفعت بیشتری خواهد داشت.

### فرد به فرد ( C2C)

مشتریان به طور مستقیم با مشتریان دیگر ارتباط پیدا کرده و از یکدیگر خرید می کنند.

این مدل از تجارت الکترونیک بیشتر به خرده فروشی های کالای دسته دوم خانگی اختصاص دارد. جایی که خریداران و فروشندگان هر دو از گروه نهایی هستند و در این میان ردپای تولیدکننده و یا واسطه ای دیده نمی شود. نمونه سنتی رایج این شیوه از تجارت را می توان در جمعه بازارها و یا حراج های محلی و منطقه ای دید که هر کس کالای تولیدی خود را به صورت تک فروشی در معرض فروش خریداران قرار می دهد. از مشهورترین نمونه های این مدل از تجارت الکترونیک می توان به سایت ebay اشاره کرد. از نمونه های ایرانی این مدل می توان به نرم افزار اندرویدی دیوار اشاره کرد که طرفداران زیادی را به خود جلب کرده است.

### نقطه به نقطه ( P2P)

مدل تجارت الکترونیکی P2P برای تسویه حساب کردن شرکت کنندگان در حراج با فروشنده است که مشهورترین آنها سرویسی است به نامPAYPAL . تجارت P2P در چهارچوبی کار می‌کند که افراد بتوانند مستقیما با هم پول رد و بدل کنند و در حالیکه سهم اصلی داد و ستد پولی را نقل و انتقالات رو در رو برعهده دارد، فن آوری تلفنهای همراه تعداد افراد بیشتری را در داد و ستد غیرحضوری سهیم می‌کند.

با استفاده از سخت افزارMONDEX که زیر مجموعهMASTERCARD می‌باشد، کاربران قادرند تا نقل و انتقالات الکترونیکی پولی خود را انجام دهند و پول خود را از یک کارت اعتباری، به کارت اعتباری دیگر منتقل نمایند.

نحوه استفاده از تلفن همراه بدین صورت است که به جای فن آوریGSM که استاندارد معمول ارتباطی تلفن همراه در بسیاری از کشورها، به ویژه در اروپاست،فن آوری دیگری تحت عنوان پروتکل بکارگیری نرم افزار کاربردی از طریق تجهیزات بی سیم که به اختصارWAP نامیده می‌شود، جایگزین می‌گردد. در این شیوه جدید، هر تلفن همراه از طریق مرکز تلفن با یک کامپیوتر سرویسگر مرتبط می‌شود و می‌تواند نرم افزار مورد نیاز کاربر خود را بر روی کامپیوتر مذکور فعال نماید. بدین ترتیب،استفاده کننده می‌تواند اطلاعات خود را از طریق کامپیوتر سرویسگر که خود از طریق اینترنت و یا شبکه‌های ارزش افزوده (VAN ) به مراکز تجاری و خدماتی متصل است، ارسال و یا دریافت نماید.

### تجارت الکترونیکی درون بنگاهی ( Intrabusiness E-commerce )

که شامل مبادلات اطلاعات، خدمات و کالا میان بخشهای مختلف بنگاه است.

### بنگاه به دولت (B2G , G2B)

رابطه ای تجاری میان دولت و بنگاه‌ها است که در آن بنگاه ها به دولت محصولات می فروشند، یا به آنها خدمات ارائه می دهند.

در این مدل ها، سازمان ها و مراکز دولتی و خصوصی در ارتباط با مراکز اقتصادی و بنگاه های تجاری دولتی هستند. در این ساختار، دو طرف با مراجعه به وب سایت های طرف قرارداد و تعامل با یکدیگر از طریق شبکه های رایانه ای امور بازرگانی مورد نیاز خود را انجام می دهند. این امور شامل مواردی چون ارسال درخواست های بانکی برای مؤسسات دولتی، گرفتن مجوزهای لازم برای انجام امور اداری، پرداخت وجه مورد درخواست سازمان ها و بانک ها و غیره است. مزیت اصلی این دو مدل صرفه جویی در انجام امور برای شرکت های دولتی و سازمان های خصوصی و نیز کاهش زمان انجام کارها است و نیز سبب تحصیل فرایندهای اداری توسط دولت شده است.

### دولت به افراد (G2C , C2G)

دولت از طریق ارتباطات الکترونیکی به شهروندان، خدمات مختلف ارائه می‌کند.

در این مدل ها، ارتباط میان مردم و دولت مطرح است و این رابطه بیش از آن که ماهیتی تجاری داشته باشد، ماهیتی خدماتی دارد و شامل خدماتی است که دولت می تواند به مردم ارائه دهد و یا زمینه ای برای تسهیل ارتباطات مالی مردم و دولت در امور مالیاتی است و یا درخواست خدماتی که از سوی شهروندان به دولت ارائه می شود که می تواند شامل درخواست های مختلف در زمینه اقتصادی و یا بازرگانی باشد.

### دولت به دولت (G2G)

شامل مبادلات میان دولتها یا درون دولتها است.

در این مدل، ارتباط متقابل میان دو یا چند سازمان دولتی و یا وزارتخانه مطرح است و مواردی چون ارتباط شهرداری با پلیس، ادارات برق و آب با شهرداری ها، نهادهای نظامی و انتظامی با وزارتخانه ها و غیره را شامل می شود. در این مدل، امکان تبادل اطلاعات میان مؤسسات دولتی و یا دادوستد بازرگانی میان شرکت های دولتی فراهم شده است. به علاوه، بخش نامه ها و دستورالعمل های دولتی را می توان از طریق این مدل کسب و کار الکترونیکی برای سازمان ها ارسال کرد.

### تجارت سیار (Mobile Commerce)

هنگامی که تجارت الکترونیکی از طریق شبکه بی سیم صورت می گیرد، تجارت سیار نامیده می شود.

## پول الکترونیکی

پول الکترونیکی یا پول دیجیتالی، ارزش پول واحدهای پول منتشره از سوی دولت یا بخش خصوصی است که به شکل الکترونیکی بر روی یک وسیله الکترونیکی ذخیره شده است.

نشر گسترده پول الکترونیکی آثار تجاری، اقتصادی، سیاسی و اجتماعی قابل توجهی دارد. مهم‌ترین اثر گسترش استفاده از پول الکترونیکی بر عرضه پول، سیاست‌های پولی و بانک مرکزی اختصاص دارد و در ادامه با توسعه بازارهای پول، سرمایه، کار و کالا ایجاد نسل‌های جدید اقتصادی را هدف‌گذاری کرده است.

با توجه به قابلیت پول الکترونیکی برای جایگزینی به جای اسکناس و مسکوک، این امکان وجود دارد که پول الکترونیکی به تدریج جایگزین پول بانک مرکزی شود و بدین ترتیب موقعیت انحصاری بانک مرکزی در زمینه‌های سیاست‌گذاری پولی، نظارت بانکی، نظارت بر نظام پرداخت‌ها، ثبات نظام مالی و به ویژه استقلال آن با خطر مواجه شود.

نتایج ارزیابی آثار گسترش کاربرد پول الکترونیکی بر اقتصاد ایران نشان می‌دهد نشر گسترده پول الکترونیکی اثر ناچیزی بر حجم پول، قدرت کنترلی بانک مرکزی و سیاست‌های پول به همراه خواهد داشت.

البته واکنش‌های بانک مرکزی در قبال نشر پول الکترونیکی، نقش بسیار مهمی در چگونگی تاثیرگذاری گسترش کاربرد پول الکترونیکی بر اقتصاد دارد. اگرچه تا کنون اقتصاددانان تعریف جامع و مانعی از پول، که بتواند همه ویژگی‌ها و وظایف پول را پوشش دهد، ارائه نکرده‌اند، اما می‌توان با کمی اغماض پول را به عنوان وسیله‌ای برای داد و ستد که مورد قبول عموم افراد جامعه باشد، تعریف کرد.

پول در زندگی اقتصادی بشر از چنان اهمیتی برخوردار است که برخی از آن به عنوان یکی از مهم‌ترین اختراعات بشر یاد کرده و تاریخ اقتصادی را با توجه به اهمیت نقش پول به سه دوره تقسیم می‌کنند:

۱. اقتصاد پایاپای
۲. دوره اقتصادی پولی
۳. اقتصاد اعتباری

با توجه به پیشرفت روزافزون فناوری اطلاعات و ارتباطات و گسترش استفاده از پول الکترونیکی از اواسط دهه ۱۹۹۰، شاید بتوان دوره کنونی را نیز دوره اقتصاد اینترنتی نامید.

گسترش فزاینده استفاده از پول الکترونیکی، پیامدهای تجاری، اقتصادی، سیاسی و اجتماعی قابل ملاحظه‌ای به همراه دارد. از نظر اقتصادی مهم‌ترین آثار گسترش استفاده از پول الکترونیکی بر روی عرضه پول، سیاست‌های پولی و بانک مرکزی ایجاد می‌شود.

آثار گسترش کاربرد پول الکترونیکی بر سیاست‌های پولی از آن جهت که می‌تواند کارآیی یکی از ابزارهای سیاست‌گذاری کلان اقتصادی دولت برای دستیابی به اهداف اقتصادی خود، به خصوص تثبیت سطح عمومی قیمت‌ها را کاهش دهد، بسیار حائز اهمیت است.

## ویژگی های پول الکترونیکی

پول الکترونیکی نوعی ابزار مالی الکترونیکی است که حداقل از عهده انجام همه وظایف پول برمی‌آید بنابراین پول الکترونیکی می‌تواند جانشین بسیار نزدیکی برای پول بانک مرکزی باشد.

ارزش پولی ذخیره شده بر روی وسیله الکترونیکی با اجازه مصرف کننده درگیر معاملات پرداختی، می‌تواند به وسیله الکترونیکی دیگری انتقال یابد.

این روش با سیستم‌های پرداخت الکترونیکی مرسوم، نظیر کارت‌های پرداخت و اعتباری و نقل و انتقالات کابلی که هر کدام معمولا نیازمند اخذ مجوز مستمر بوده و ممکن است در هر معامله متضمن بدهکار کردن و بستانکار کردن حساب‌های بانکی باشند، متفاوت است.

به نقل از بانک توسعه صادرات ایران ، بر خلاف پول بانک مرکزی که پول بیرونی است، پول الکترونیکی همانند یک سپرده دیداری یا چک مسافرتی پول درونی می‌باشد.

پول درونی طلب قانونی دارنده آن از ناشر آن می‌باشد در حالی که پول بیرونی متضمن چنین طلبی نیست، به عبارت دیگر موجودی پول الکترونیکی، یک طلب جاری بر عهده ناشر آن است که با هیچ حساب خاصی ارتباط ندارد.

اگر چه درفرایند توسعه پول الکترونیکی، انواع بسیار متفاوتی از فرآورده‌های پول الکترونیکی با ویژگی‌های مختلف عرضه شده است اما در طراحی همه آنها سعی شده حداقل همه ویژگی‌های پول بانک مرکزی لحاظ شود.

به طور کلی فرآورده‌های پول الکترونیکی را از نظر فنی می‌توان به دو دسته تقسیم کرد.

۱. پول الکترونیکی مبتنی بر کارت‌های هوشمند
۲. پول الکترونیکی مبتنی بر نرم‌افزار رایانه‌ای

فرآورده‌های پول الکترونیکی مبتنی بر کارت‌های هوشمند، برای تسهیل پرداخت‌های با ارزش کوچک در معاملات خرد رو در رو طراحی شده‌اند، بنابراین انتظار می‌رود که فرآورده‌های پول الکترونیکی مبتنی بر کارت‌های هوشمند، استفاده از پول بانک مرکزی و نیز در حد کمتر استفاده از کارت‌های اعتباری و پرداخت را برای پرداخت‌های مستقیم، کاهش دهد. همچنین به احتمال زیاد استفاده از چک، کارت‌های پرداخت و کارت‌های اعتباری در پرداخت‌های غیرمستقیم، یعنی پرداخت‌های به هنگام را نیز کاهش خواهد داد.

فرآورده‌های پول الکترونیکی مبتنی بر نرم‌افزار رایانه‌ای نیز از طریق کاهش هزینه‌های مبادلاتی با تسهیل نقل و انتقال پول میان انواع مختلف حساب‌ها، بانک‌ها و کشورها و نیز سرریزهای یادگیری، تقاضای سپرده‌های دیداری را تحت تاثیر قرار می‌دهد و آن را کاهش خواهد داد.

سرریزهای یادگیری به مهارتی که افراد در طی زمان ضمن استفاده از نرم‌افزارهای مالی شخصی و فناوری‌های ارتباطی برای مدیریت بهینه برنامه‌های مالی شخصی و فناوری‌های ارتباطی برای مدیریت بهینه برنامه‌های مالی خود کسب می‌کنند، مربوط می‌شود.

مهمترین ویژگی پول الکترونیکی یعنی فراملیتی یا بی‌مرز بودن آن نقش مهمی در اثرگذاری بر سایر متغیرهای اقتصادی ایفا می‌کند.

اگر چه این ویژگی ازنظر دولت‌ها منشا برخی تبعات منفی نشر گسترده پول الکترونیک تلقی می‌شود اما به ارتقای سطح کارایی مبادلات بین‌المللی نیز کمک قابل ملاحظه‌ای می‌کند.

طبیعتا با استفاده از پول الکترونیکی، هزینه نقل و انتقال بین‌المللی وجوه، به طور قابل توجهی کاهش خواهد یافت. البته با افزایش بی‌سابقه کارایی پرداخت‌های بین‌المللی، ممکن است بی‌ثباتی نظام پولی جهانی افزایش یابد و به بروز کشمکش بین ناشران و استفاده کنندگان پول الکترونیکی از یک سو و بانک‌های مرکزی کشورها از سوی دیگر منجر شود.
ویژگی دیگر پول الکترونیکی، پول قانونی یا پول رایج نبودن آن است که این امر درمراحل اولیه نشر، مقبولیت عمومی آن را کاهش می‌دهد.

علاوه براین پول الکترونیکی برخلاف اسکناس و مسکوک و دیگر وسایل مبادله امروزی ، مستلزم حضور فیزیکی پرداخت‌کننده و دریافت کننده وجه برای قطعیت **پرداخت** نیست، زیرا موجودی پول الکترونیکی می‌تواند از طریق شبکه‌های رایانه‌ای به صورت به هنگام انتقال یابد.

## زیرساخت های تجارت الکترونیک

برای راه اندازی یک تجارت الکترونیک موفق زیرساخت هایی لازم است که برخی از آن ها همچون دسترسی به اینترنت پرسرعت در حد اختیارات شرکت ها نیست، اما می توانیم با بررسی آن ها و شرایط جامعه سطحی از تجارت الکترونیک را فراهم سازیم که با امکانات کاربران همخوانی داشته باشد.

از زیرساخت های اساسی تجارت الکترونیک می توانیم موارد زیر را نام ببریم:

- امنیت ارتباط
- پهنای باند دسترسی کاربران
- شیوه های دسترسی کاربران (خط تلفن، اینترنت بی سیم، وایمکس، ای دی اس ال، ...)
- فروشگاه آنلاین
- مدل پرداخت الکترونیکی
- سیستم های رهگیری تراکنش ها
- سیستم های آمارگیری
- سیستم های نظرسنجی
- مدیریت سطوح دسترسی کاربران
- بالابردن رتبه در موتورهای جستجو

ابزارهای مختلفی می توانند برای کمک مستقیم و غیرمستقیم به تجارت الکترونیک به کار روند. در ادامه سعی خواهیم کرد با برخی از این ابزارها آشنا شویم. برخی از این ابزارها در روند الکترونیکی ساختن فعالیت ها نقش دارند و تجارت الکترونیک نیز می تواند در بخش هایی از آن ها به کار رود.

- Customer Relationship Management : CRM
- Supplier Relationship Management : SRM
- Management Information System : MIS
- Supply Chain Management : SCM
- Enterprise Resources Planning : ERP

# امنیت اطلاعات

## تعاریف

امنیت اطلاعات به حفاظت از اطلاعات و به حداقل رساندن خطر افشای اطلاعات اشاره دارد. امنیت اطلاعات مجموعه ای از ابزارها برای جلوگیری از سرقت، حمله، جنایت، جاسوسی و خرابکاری بوده و علم مطالعه روش های حفاظت از داده ها در رایانه ها و نظام های ارتباطی در برابر دسترسی و تغییرات غیرمجاز است.

تعریف: امنیت اطلاعات به مجموعه ای از تدابیر، روش ها و ابزارها برای جلوگیری از دسترسی و تغییرات غیرمجاز در نظام های رایانه ای و ارتباطی تلقی می شود.

## مدیریت امنیت اطلاعات

مدیریت امنیت اطلاعات بخشی از امنیت اطلاعات است که وظیفه تعیین اهداف امنیت و بررسی موانع سرراه رسیدن به این اهداف و ارائه راهکارهای لازم را برعهده دارد. هدف مدیریت امنیت اطلاعات، حفظ سرمایه های سازمان در مقابل هرگونه تهدید می باشد.

## تاریخچه

در سال ۱۹۱۸ میلادی مخترع آلمانی Arthur Scherblus به همراه Richard Ritter شرکتی را تاسیس کردند که منجر به ساخت نخستین ماشین رمزنگاری با نام انیگما شد.

در جنگ جهانی دوم ارتش آلمان ۳۰ هزار دستگاه انیگما خریداری نمود. پس از ۱۳ سال شکست ناپذیری انیگما یک افسر ریاضیدان لهستانی به نام Marian Reje Wski روشی برای شکست انیگما ارائه نمود.

شکست های امنیتی از ضعف های مدیریتی (از لحاظ امنیتی) و عوامل انسانی (به خاطر عدم آموزش) ناشی می شوند.

## مفاهیم اصلی در امنیت اطلاعات

۱. محرمانگی (Confidentially) : حفاظت از اطلاعات در مقابل دسترسی غیرمجاز
۲. تمامیت (Integrity) : یکپارچگی داده ها
۳. اعتبار و سندیت (Authenticity) : موثق بودن داده ها
۴. دسترسی پذیری (Availability) : دسترسی به اطلاعات در زمان نیاز

## مزایای سرمایه گذاری در امنیت اطلاعات

- کاهش احتمال از کار افتادن سیستم ها
- استفاده موثر از منابع

- کاهش هزینه از دست دادن داده
- افزایش حفاظت از مالکیت معنوی

## حفره امنیتی

حفره امنیتی به نقاط ضعف سیستم حفاظتی (از لحاظ سخت افزاری یا نرم افزاری) گفته می شود.

وجود حفره امنیتی دارای پیامدهای منفی زیر می باشد:

- کاهش درآمد و افزایش هزینه
- خدشه به اعتبار و شهرت سازمان
- پیامدهای قانونی ناشی از ازدست دادن اطلاعات مهم
- از دست دادن اعتماد مشتریان و سرمایه گذاران

برای جلوگیری از ایجاد حفره امنیتی می توان رویکردهای پیشگیرانه ای را جهت مدیریت خطرات امنیتی به شرح زیر اعمال نمود:

- شناسایی تهدیدات موجود
- اولویت بندی تهدیدات و خطرات
- مدیریت در سطحی قابل قبول
- کاهش خطر آسیب پذیری

با پیاده سازی فرآیند مدیریت خطرات امنیتی می توان دستآوردهای زیر را بدست آورد:

- افزایش زمان پاسخگویی به تهدیدات
- مدیریت قانونمند
- مدیریت هزینه های زیرساخت
- اولویت بندی خطرات

## سیستم امنیت اطلاعات

از وظایف مهم مدیریت امنیت یا مشاور امنیت ایجاد یک سیستم امنیت اطلاعات می باشد برای این منظور توجه به نکات زیر از اهمیت زیادی برخوردار است:

- آشنایی با منابع اطلاعاتی موجود در سازمان
- ارزیابی ارزش اطلاعات : ارزیابی ارزش اطلاعات می تواند بر مبنای هزینه تولید آن ها صورت پذیرد.
- تعیین هزینه فاش شدن اطلاعات

- شناسایی تهدیدات

تهدیدات موجود برای امنیت سیستم های اطلاعاتی معمولا از قرار زیر می باشند:

- افشای اطلاعات محرمانه (افشا)
- صدمه به یکپارچگی اطلاعات (دستکاری)
- موجود نبودن اطلاعات (تطبیق خدمات)
- خطای نیروی انسانی
- بلایای طبیعی
- ایرادات سیستمی
- فعالیت های خرابکارانه

### اتخاذ سیاست های امنیتی

بر اساس استاندارد BS7799 مواردی که یک سازمان برای پیاده سازی یک سیستم امنیتی اعمال می کند به شرح زیر می باشد:

۱. تعیین سیاست امنیتی اطلاعات
۲. اعمال سیاست های مناسب
۳. برسی فوری وضعیت امنیت اطلاعاتی بعد از اعمال سیاست امنیتی
۴. بازرسی و تست امنیت شبکه اطلاعاتی
۵. بهبود روش های امنیت اطلاعاتی سازمان

## تاریخچه استاندارد امنیت اطلاعات

### استاندارد امنیتی مدیریتی BS7799 [۱]

نسخه جدیدتر آن ISO/IEC 27001 می باشد.

این استاندارد اولین استاندارد مدیریت امنیت اطلاعات است. نسخه اول این استاندارد در سال ۱۹۹۵ و در یک بخش منتشر شد. نسخه دوم نیز در سال ۱۹۹۹ ارائه شد که نسخه دوم با نام ISMS [۲] به آن اضافه شد. این استاندارد متشکل از ۳۵ هدف امنیتی و ۱۲۷ اقدام بازدارنده برای تامین اهداف تعیین شده می باشد. در سال ۲۰۰۰ بخش اول این استاندارد با نام ISO/IEC 17799 توسط موسسه بین المللی استاندارد منتشر گردید.این استاندارد در سال های ۲۰۰۲ و ۲۰۰۵ بازنویسی شد که شامل ۳۹ هدف امنیتی و ۱۳۴ اقدام بازدارنده بود.

[۱] British Standard 7799
[۲] Information Security Management System

## سیستم مدیریت امنیت اطلاعات

هدف سیستم مدیریت امنیت اطلاعات اطمینان از تداوم کسب و کار از طریق جلوگیری و به حداقل رساندن اثرات حوادث امنیتی است. سه اصل مهم در یک سیستم جامع امنیتی به شرح زیر است:

۱. سیاست ها و دستورالعمل های امنیتی
۲. تکنولوژی و محصولات امنیتی
۳. عوامل اجرایی انسانی

## راهکارهای امنیتی

راهکارهای امنیت اطلاعات به دو دسته تقسیم می شوند:

### راهکارهای پیشگیرانه

- رمزنگاری داده
- استفاده از امضای دیجیتال
- استفاده از شبکه های مجازی خصوصی
- استفاده از نرم افزارهای جستجوگر نقاط آسیب پذیر سیستم
- استفاده از نرم افزارهای آنتی ویروس
- استفاده از پروتکل های امنیتی
- استفاده از سخت افزارهای امنیتی

### راهکارهای واکنشی

- فایروال
- کنترل دسترسی
- تعیین کلمات عبور
- بیومتریک (تعیین اعتبار با اثر انگشت، قرنیه، الگوی صدا، الگوی چهره، غیره)
- سیستم آشکارسازی نفوذ (IDS) سیستم دفاعی جهت تشخیص فعالیت های مخاطره آمیز
- Logging : ثبت رخدادها
- دسترسی از راه دور : استفاده از این سیستم ها خطر جعل هویت را افزایش می دهد.

# حریم خصوصی در تجارت الکترونیک

تعریف کمیته کالکات انگلستان از حریم خصوصی: حق افراد برای حمایت شدن در مقابل ورود بدون اجازه به امور زندگی و خانواده هایشان با ابزار مستقیم فیزیکی یا بوسیله نشر اطلاعات.

ماده ۱۲ اعلامیه جهانی حقوق بشر در مورد حریم خصوصی: نباید در زندگی خصوصی، امور خانوادگی، اقامتگاه یا مکاتبات هیچکس مداخله ی خودسرانه صورت گیرد یا به شرافت، آبرو و شهرت کسی حمله شود.

اصلاحیه چهارم مصوب ۱۷۹۱ قانون اساسی آمریکا: حق امنیت، جان، مسکن، اوراق، اسناد و مصونیت دارایی های مردم در برابر تفتیش و توقیف غیرموجه تضمین می شود و هیچگونه حکم بازداشت اشخاص یا اموال صادر نمی گردد، مگر بر پایه یک دلیل محتمل یا سوگند یا اعلام رسمی و محل مورد تفتیش و اشخاص یا اموالی که باید توقیف شود.

اصل ۲۲ قانون اساسی جمهوری اسلامی ایران: حیثیت، جان، حقوق، مسکن و شغل اشخاص از تعرض مصون است مگر در مواردی که قانون تجویز می کند.

اصل ۲۳ قانون اساسی جمهوری اسلامی ایران: تفتیش عقاید ممنوع است و هیچکس را نمی توان به صرف داشتن عقیده ای مورد تعرض قرار داد.

اصل ۲۵ قانون اساسی جمهوری اسلامی ایران: بازرسی و نرساندن نامه ها، ضبط و فاش کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس، سانسور، عدم مخابراه و نرساندن آن ها، استراق سمع و هرگونه تجسس ممنوع است، مگر به حکم قانون.

ماده ۵۲۸ قانون مجازات اسلامی مصوب خرداد ۷۵: بازرسی و گشودن مخابرات یا مراسلات بدون مجوز و افشای آنها و همچنین افشای اسرار مردم جرم تلقی و مجازاتی از ۱ تا ۳ سال حبس یا ۶ تا ۱۸ میلیون ریال جریمه برا مرتکبین تعیین شده است.

## حوزه های حریم خصوصی

- حریم اطلاعات: حریم اطلاعات مالی، پزشکی و دولتی افراد
- حریم جسمانی: حریم جسم در مقابل آزمایش های ژنتیک، دارویی و امثال آن
- حریم ارتباطات: حریم تلفن ها، نامه ها و ارتباطاتی از این قبیل
- حریم مکانی: نظارت ها در محیط کار زندگی

## نکات حریم خصوصی در تجارت الکترونیکی

به منظور عدم نگرانی مشتریان و استفاده درست از اطلاعات لازم است نکات زیر برای حریم خصوصی افراد در تجارت های الکترونیکی در نظر گرفته شوند:

- هدف از جمع آوری اطلاعات مشخص باشد و به اطلاع مشتری برسد.
- داده های جمع آوری شده محدود به مواردی باشند که جهت حصول هدف مشخص شده می باشد.
- استفاده از داده های جمع آوری شده باید محدود به هدف مشخص شده باشد.
- داده های جمع آوری شده نباید برای زمانی طولانی تر از حصول هدف نگاهداری شوند.
- داده های جمع آوری شده باید صحیح و کامل و به روز باشند.
- مشتری باید حق انتخاب جهت ارائه اطلاعات را داشته باشد.
- مشتری باید امکان بررسی، اصلاح، تکمیل و حذف اطلاعات خود را در هر زمان به راحتی داشته باشد.
- از داده های مشتریان باید محافظت شود و پایگاه داده ها امنیت بالایی در مقابل نفوذ داشته باشد.

دو عامل اصلی که سبب نقض حریم خصوصی افراد در فضای سایبری می شود به شرح زیر می باشند:

- منافع اقتصادی و تجاری
- منافع سیاسی

## قانون محافظت حریم شخصی برای کودکان

با افزایش تعداد کاربران موبایل برای کودکان زیر ۱۳ سال COPPA در اول آوریل ۲۰۰۰ قوانینی را برای گردانندگان وب سایت های با مخاطب کودکان ایجاد کرد:

۱. برای والدین کودکان پیامی درخصوص اطلاعاتی که جمع آوری می گردد و هدف از جمع آوری آن ها ارسال گردد.
۲. اجازه و موافقت قابل تغییر والدین برای جمع آوری و استفاده از اطلاعات دریافت گردد.
۳. امکان مشاهده اطلاعات جمع آوری شده توسط والدین و امکان جلوگیری از استفاده بیشتر از اطلاعات در هر زمان را داشته باشند.
۴. محدود کردن اطلاعات مورد نیاز از کودک برای بازی، مسابقه و غیره در حد اطلاعات ضروری صورت گیرد.
۵. پیاده سازی فعالیت های امنیتی جهت محافظت از اطلاعات جمع آوری شده

## اصول حفاظت از حریم خصوصی

در سال ۱۹۹۸ ، FTC پنج اصل را برای استفاده از اطلاعات با نام اصول مرکزی وضع نمود:

- اعلان/آگاهی : سیاست های جمع آوری اطلاعات باید به آگاهی مشتری برسد. این سیاست ها شامل هویت نهاد مع آوری کننده اطلاعات، نوع داده ها، نوع استفاده مورد نظر و دریافت کنندگان احتمالی داده ها می باشد.

- رضایت/انتخاب : مشتریان باید حق انتخاب تعیین داده های جمع آوری شده، انصراف از ارائه داده و انتخاب نحوه استفاده از داده ها را داشته باشند.
- دسترسی/مشارکت : امکان دسترسی و تصحیح اطلاعات جمع آوری شده توسط مشتری فراهم شود.
- یکپارچگی/امنیت : داده های شخصی باید به صورت منطقی، امن و به روز نگهدادی شوند.
- اجبار به اقدام/تزریق : همه نهاد ها موظف هستند چهار اصل فوق را به طور مناسبی اجرا کنند.

## قوانین حریم خصوصی در ایران

در ایران دو قانون مقررات و ضوابط شبکه های اطلاع رسانی رایانه ای مصوب ۱۳۸۰ و قانون تجارت الکترونیکی وجود دارند که به حریم خصوصی اشاره نموده اند.

### مقررات و ضوابط شبکه های اطلاع رسانی رایانه ای

این قانون مراکز ارائه دهنده سرویس اینترنت و کافی نت ها را ملزم به نگهداری تمامی اطلاعات کاربران و ارائه آن به مراجع دولتی می کند و در عین حال از اطلاعات کاربران در برابر تجاوز اشخاص حقیقی و حقوقی دیگر حمایت می کند.

در این قانون بخش آیین نامه شرکت های ارائه دهنده سرویس های اینترنت مواردی جهت حفاظت از حریم خصوصی افراد آمده است که بخش های مرتبط آن ها به شرح زیر می باشد:

- حریم اطلاعات خصوصی کاربران از مصونیت برخوردار بوده و هرگونه دسترسی غیرقانونی توسط شرکت و هر مرجع دیگر به فعالیت های کاربران ممنوع می باشد.
- ۶-۱۳: افشای روابط خصوصی افراد و تجاوز به حریم اطلاعات شخصی آنها ممنوع می باشد.
- ۶-۱۴: انتشار اطلاعات حاوی کلیدهای رمز بانک اطلاعاتی، نرم افزارهای خاص، صندوق های پست الکترونیکی و یا روش های شکستن آن ها ممنوع می باشد.
- ۶-۱۷: هرگونه نفوذ غیرمجاز به مراکز دارنده اطلاعات خصوصی و محرمانه و تلاش در جهت شکستن قفل رمز آن ها ممنوع می باشد.
- ۶-۱۹: هرگونه تلاش برای انجام شنود و بررسی بسته های در حال گذر در شبکه که به دیگران تعلق دارد ممنوع می باشد.

مسوولیت نظارت بر حسن اجرای این موارد بر عهده وزارت ارتباطات و فناوری اطلاعات می باشد.

### قانون تجارت الکترونیکی

یک فصل کامل از این قانون (فصل سوم) به حمایت از داده های شخصی اختصاص دارد. برخی از موارد در زیر آمده است:

ماده ۵۸- ذخیره، پردازش و یا توزیع داده پیام های شخصی مبین ریشه های قومی یا نژادی، دیدگاههای عقیدتی، مذهبی، خصوصیات اخلاقی و داده پیام های راجع به وضعیت جسمانی، روانی و یا جنسی اشخاص بدون رضایت صریح آنها به هر عنوان غیر قانونی است.

ماده ۵۹- در صورت رضایت شخص موضوع داده پیام نیز به شرط آنکه محتوای داده پیام وفق قوانین مصوب مجلس شورای اسلامی باشد ذخیره، پردازش و توزیع داده پیام های شخصی در بستر مبادلات الکترونیکی باید با لحاظ شرایط زیر صورت پذیرد:

الف – اهداف آن مشخص بوده و به طور واضح شرح داده شده باشند.

ب – داده پیام باید تنها به اندازه ضرورت و متناسب با اهدافی که در هنگام جمع آوری برای شخص موضوع داده پیام شرح داده شده جمع آوری گردد و تنها برای اهداف تعیین شده مورد استفاده قرار گیرد.

ج- داده پیام باید صحیح و روز آمد باشد.

د- شخص موضوع داده پیام باید به پرونده های رایانه ای حاوی داده پیام های شخصی مربوط به خود دسترسی داشته و بتواند داده پیام های ناقص و یا نادرست را محو یا اصلاح کند.

ه- شخص موضوع داده پیام باید بتواند درهر زمان با رعایت ضوابط مربوطه درخواست محو کامل پرونده رایانه ای داده پیام های شخصی مربوط به خود را بنماید.

ماده ۶۰- ذخیره، پردازش و یا توزیع داده پیام های مربوط به سوابق پزشکی و بهداشتی تابع آیین نامه ای است که در ماده (۷۹) این قانون خواهد آمد.

ماده ۶۱- سایر موارد راجع به دسترسی موضوع داده پیام، از قبیل استثنائات، افشای آن برای اشخاص ثالث، اعتراض، فراکردهای ایمنی، نهادهای مسوول دیدبانی و کنترل جریان داده پیام های شخصی به موجب مواد مندرج در باب چهارم این قانون و آیین نامه مربوطه خواهد بود.

ماده ۷۱- هر کس در بستر مبادلات الکترونیکی شرایط مقرر در مواد (۵۸) و (۵۹) این قانون را نقض نماید مجرم محسوب و به یک تا سه سال حبس محکوم می شود.

ماده ۷۲- هر گاه جرایم راجع به داده پیام های شخصی توسط دفاتر خدمات صدور گواهی الکترونیکی و سایر نهادهای مسوول ارتکاب باید، مرتکب به حداکثر مجازات مقرر در ماده (۷۱) این قانون محکوم خواهد شد.

ماده ۷۳- اگر به واسطه بی مبالاتی و بی احتیاطی دفاتر خدمات صدور گواهی الکترونیکی جرایم راجع به داده پیام های شخصی روی دهد، مرتکب به سه ماه تا یک سال حبس و پرداخت جزای نقدی معادل پنجاه میلیون (۵۰/۰۰۰/۰۰۰) ریال محکوم می شود.

## طرح حمایت از حریم خصوصی

این طرح شامل ۸۰ ماده و در ۷ فصل آمده است.

# برخی ملاحظات حریم خصوصی

## هرزنامه

در دستورالعمل ADMA ملاحظاتی جهت جلوگیری از ارسال هرزنامه اعمال شده است که باید توسط ارسال کنندگان پیام رعایت شوند.

- اعضا نباید پیام های ناخواسته بی هدف ارسال کنند.
- پیام های بازاریابی باید حاوی یک شناسه شناخته شده باشند تا گیرنده قادر باشد مستقیما با سازمان ارسال کننده تماس بگیرد.
- همچنین باید فرآیندی وجود داشته باشد که گیرنده بتواند از دریافت پیام های آتی انصراف دهد.

## جمع آوری اطلاعات موقعیت

طبق قانون بازاریابی ADMA پیام های مبتنی بر مکان تنها باید به کاربرانی ارسال شود که با دریافت پیام های مبتنی بر مکان موافقت نموده اند.

## نگهداری رکوردهای داده های شخصی

سرویس دهندگان موظف هستند اطلاعات مشتریان را تا ۶ الی ۱۲ ماه نگهداری نمایند تا درصورت بروز فعالیت های تبهکاری امکان ردیابی توسط نهادهای مربوطه وجود داشته باشد.

## ارکان امنیت فناوری اطلاعات

۱. چارچوب قانونی و اجرایی
۲. امنیت الکترونیکی در سیستم های پرداخت
۳. چالش های نظارت و پیش گیری
۴. بیمه خصوصی به عنوان یک سیستم نظارت تکمیلی
۵. گواهی، استانداردها، و نقش بخش های عمومی و خصوصی
۶. دقت در اطلاعات رخدادهای امنیتی
۷. آموزش و پیش گیری از وقوع رخدادهای امنیت الکترونیکی
۸. امنیت چند لایه

## لایه های امنیت الکترونیکی

۱. مسوول امنیت اطلاعات
۲. مدیریت مخاطرات
۳. کنترلهای دسترسی و تصدیق هویت
۴. دیواره های آتش (فایروال)
۵. غربال کردن اطلاعات به صورت فعال
۶. سیستم مهاجم یاب (IDS)
۷. ویروس یاب ها
۸. رمزگذاری
۹. آزمون آسیب پذیری
۱۰. راهبری صحیح سیستم ها
۱۱. نرم افزار مدیریت سیاست
۱۲. طرح واکنش به رخداد (IRP) [۳] و تداوم کسب و کار

[۳] Incident Response Plan

## رمزگذاری

کدگذاری و رمزنگاری فنونی هستند که رشته های حروف را به قالب و شکل دیگری تبدیل می کنند. این فرآیند برگشت پذیر است و بعدا می توان قالب کدگذاری شده را کدگشایی نمود تا به شکل اصلی خود تبدیل شود.

روش های رمزگذاری به قرار زیر می باشند:

- رمزگذاری متقارن
- رمزگذاری کلید عمومی
- رمزگذاری یک طرفه با استفاده از Hash

## رمزگذاری متقارن

رمزگذاری متقارن شبیه کدگذاری است که حروف اصلی متن تغییر ظاهری می یابند.

به طور نمونه یکی از ساده ترین الگوریتم های رمزگذاری این است که هر حرف را با حرف بعدی آن جایگزین کنیم. در روش تعداد تغییر مکان حروف را کلید رمزگذاری می گویند. جولیوس سزار از این روش با کلید رمزگذاری ۳ برای ارسال پیام های خود استفاده می نمود.

در رمزگذاری متقارن فرستنده و گیرنده از یک کلید مشابه استفاده می کنند. در واقع /ان ها باید در مورد یک کلید مشخصبه توافق برسند. اگر کلید مفقود شود اطلاعات نیز قطعا قابل بازیابی نخواهند بود.

## رمزگذاری کلید عمومی

این رمزگذاری مشابه رمزگذاری متقارن می باشد با این تفاوت که در آن از دو کلید به جای یک کلید استفاده می شود. در این شیوه کلیدی که برای رمزگذاری پیام استفاده می شود با کلید رمزگشایی متفاوت است. معمولا کلید اول (رمزگذاری) عمومی می باشد و همه از آن اطلاع دارند و کلید دوم (رمزگشایی) خصوصی می باشد که فقط خود شخص آن را در اختیار دارد.

لذا به طور مثال چنانچه بخواهیم پیامی را برای کسی ارسال کنیم با استفاده از پیام عمومی آن شخص (که آن را در اختیار همه قرار داده است) پیام را برای او ارسال می کیم و او با استفاده از کلید خصوصی خود می تواند پیام را رمزگشایی کند.

پس می توان گفت که کلید خصوصی را به هیچ وجه نباید در اختیار سایرین قرار داد.

در این روش شخص مطمئن نیست که چه کسی پیام را برای او ارسال نموده است اما فرستنده می تواند مطمئن باشد که فقط صاحب پیام (گیرنده مورد نظر) می تواند پیام را رمزگشای کند و بخواند.

کلیدهای عمومی و خصوصی می توانند عکس این حالت نیز به کار روند. در این حالت پیام را با کلید خصوصی خود رمزگذاری کرده و ارسال می کنیم در این حالت هر کس که کلید عمومی را داشته باشد می تواند پیام را رمزگشایی کند. در اینصورت آنچه که قابل اطمینان است هویت فرستنده پیام است.

## رمزگذاری یک طرفه با استفاده از درهم سازی

این روش را می توان مشابه روش رمزگذاری کلید عمومی فرض کرد به گونه ای که هیچ کس کلید خصوصی را ندارد. مطالب می توانند رمزگذاری شوند اما نمی توانند رمزگشایی شوند. در این روش معمولا پیام رمز شده طول مشخصی دارد.

از الگوریتم های رایج این روش می توان MD5 را نام برد که طول پیام رمز شده آن همیشه ۱۲۸ بیت معادل ۱۶ بایت می باشد.

این روش دو کاربرد دارد:

- **تضمین جامعیت:** با اعمال این الگوریتم روی یک سند، برنامه یا متن و ذخیره خروجی کد شده در مراجعات بعدی نیز می توان مجددا الگوریتم را روی آن اعمال و خروجی را با نتیجه قبلی مقایسه نمود و در صورت یکسان بودن به معنای عدم تغییر اطلاعات اولیه می باشد.
- **ذخیره رمز عبور:** برای ذخیره رمز عبور می توان از این الگوریتم ها استفاده نمود بدین ترتیب درصورت دسترسی نفوذگران به اطلاعات رمز عبور امکان خواندن آن ها وجود ندارد.

# امضای دیجیتالی

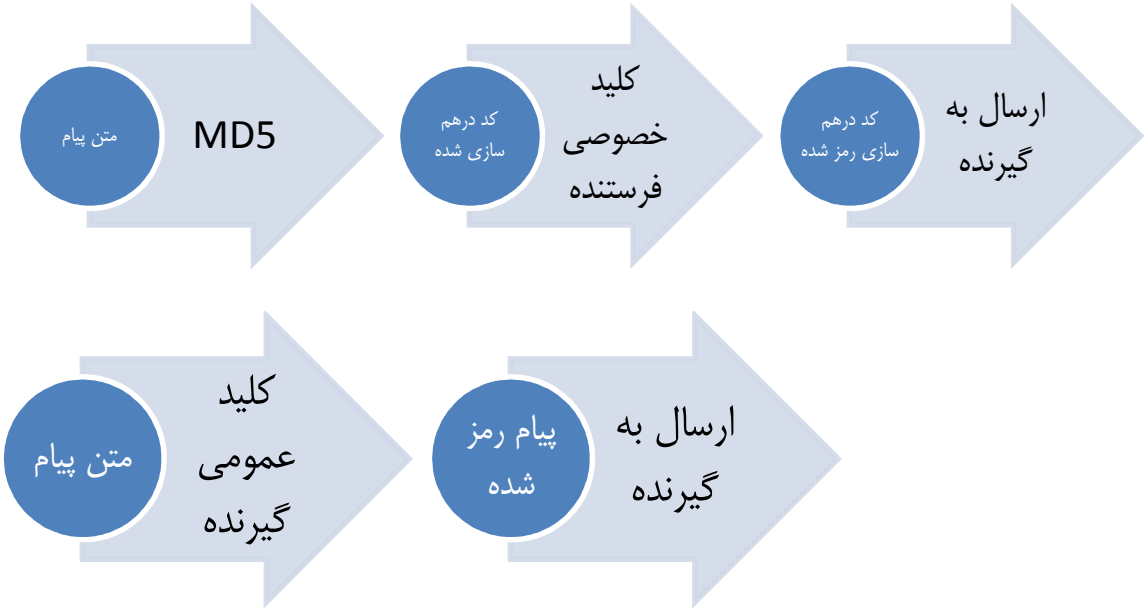
برای ارسال پیام به صورت رمز گذاری شده و اهراز هویت فرستنده می توان از ترکیب روش های فوق استفاده کرد.

۱. فرستنده از کد MD5 برای ایجاد کد درهم سازی شده استفاده می کند.
۲. فرستنده با استفاده از کلید خصوصی خود کد درهم سازی شده را رمزگذاری می کند.
۳. فرستنده با استفاده از کلید عمومی گیرنده پیام را رمز گذاری می کند.
۴. خروجی پیام و کد در هم سازی رمزگذاری شده را برای گیرنده ارسال می کند.
۵. گیرنده پیام را دریافت میکند.
۶. گیرنده با استفاده از کلید عمومی فرستنده، کد در هم سازی را رمزگشایی می کند تا کد در هم سازی شده اصلی بدست آید.
۷. گیرنده متن پیام رمز شده دریافتی را با استفاده از کلید خصوصی خود رمزگشایی می کند.

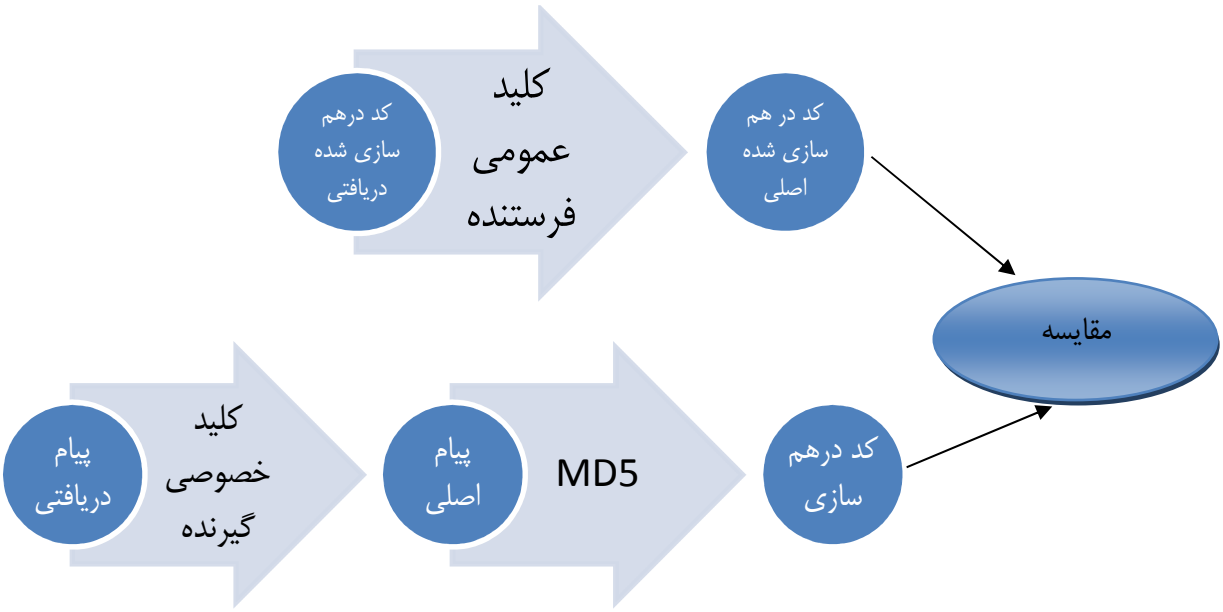
۸. متن پیام رمزگشایی شده را با ستفاده از MD5 کد کرده و کد در هم سازی را بدست می آورد.

۹. کد در هم سازی بدست آمده (خروجی بند ۸) را با کد درهم سازی رمزگشایی شده (خروجی بند ۶) مقایسه می کند، اگر یکسان باشند، متن ارسالی تغییر نکرده و فرستنده نیز همان شخصی است که گیرنده انتشار داشته است.

**فرستنده:**




**گیرنده:**



# مخاطرات امنیتی

## مخاطرات امنیتی شبکه های بی سیم

۱. حملات درج[۴]: نفوذگر سعی می کند از طریق یک نقطه دسترسی سیار[۵] به شبکه داده وارد شود.
۲. سرقت جلسه[۶]: از آنجا که تلفن هویت خود را برای ایستگاه ثابت ارسال می کند اما ایستگاه این کار را نمی کند می توان با شبیه سازی یک ایستگاه ثابت جلسه بین تلفن و ایستگاه را به سرقت برد.
۳. پارازیت: نوعی حمله تخریب سرویس است که با داده پراکنی در فرکانس کاری شبکه انجام می شود.
۴. حملات رمزنگاری: رمزنگاری شبکه های بی سیم مبتنی بر WEP می باشد که بسیار ضعیف بوده و بارها شکسته شده است.
۵. تصاحب ترافیک و دیده بانی: دریافت داده های بی سیم در محدوده شبکه و شنود اطلاعات را می گویند.
۶. ارتباط نقطه سیار با نقطه سیار دیگر: ارتباط نقطه به نقطه اجازه انتقال فایل یا برنامه مخرب را توسط نقاط سیار بدست می دهد.
۷. تنظیمات نادقیق: پیکره بندی نادرست تجهیزات می توانند امنیت شبکه را دچار مخاطره کنند.
۸. حملات Brute Force : (مثلا حمله بر اساس فرهنگ لغت) استفاده از یک کلی یا رمز عبور، احتمال این نوع حمله را افزایش می دهد.

[۴] Insertion Attack
[۵] Mobile Access Point
[۶] Session Hijacking

## انواع حملات

حملات به طور کلی به سه دسته تقسیم می شوند:

- حملات تخریب سرویس و بهره برداری از راه دور: از کار انداختن سرویس
- تهدیدات برنامه ای: تسخیر سیستم با استفاده از برنامه مخرب
- مهندسی اجتماعی: استفاده از خصوصیات طبیعی و اجتماعی کاربران

## راهکارهای کاهش صدمات حاصله از حمله

- نصب سیستم های ناظر
- تفکیک شبکه به چند زیرشبکه
- تهیه چند اتصال اینترنت
- استفاده از دریچه ورودی: رد درخواست ها درصورت افزایش بیش از حد در بازه زمانی کوتاه
- اطمینان از سازگار بودن محدودیت های موجود در فایل پیکربندی

انواع حملات روی سیستم ها وجود دارند در ادامه برخی از آن ها اشاره می شوند:

- DDOS [۷] : مهاجم سیلی از درخواست سرویس ها را از نقاط مختلف به سمت سرور می فرستد تا سرور با درخواست های بیش از حد مواجه شده و از کار بیافتد.
- سیل پیام ها[۸] : با ارسال تعداد زیادی پیام به آدرس یک سیستم سرعت پردازش آن کند می شود و نهایتا ممکن است سیستم به علت مواجهه با خطای ناشی از کمبود حافظه برای ذخیره بسته های ورودی از کار بیافتد.
- حملات انسداد[۹] (سیل Sync) : اتصال های TCP از مکانیزمی به نام دست دادن چند مرحله ای برای باز کردن یک اتصال و تنظیمات آن استفاده می کنند. اگر یک مهاجم چندین پیام ایجاد اتصال ارسال کند و مراحل بدی ایجاد اتصال را انجام ندهد، چندین اتصال نیمه باز در سمت گیرنده باقی می ماند و منابع آن را اشغال م یکند و زمانی که منابع بیش از حد اشغال شوند سیستم از کار می افتد.
- Malformed Traffic Attack (ترافیک بدشکل) این حملات مربوط به اشکالات سطوح پایین شبکه می باشد که سیستم ها در برخورد با یک بسته یا درخواست بدفرم از کار بیافتند. معروف ترین نوع این حملات Ping of Death بوده است که با ارسال بسته ICMP طولانی تر از اندازه مجاز سرویس های ویندوز و لینوکس را از کار می انداخت. تنها راه مقابله با این نوع حمله، استفاده از Proxy و به روز نگاه داشتن سیستم ها می باشد.
- اسب تروا

---

[۷] Distributed Denial Of Service
[۸] Message Flooding
[۹] Stateless

- Buffer overflow
- cross-site scripting
- SQL injection
- canonicalization
- Network eavesdropping
- Brute force attack
- dictionary attacks
- cookie replay
- credential theft
- Elevation of privilege
- disclosure of confidential data
- data tampering
- luring attacks
- Session hijacking
- session replay
- man in the middle
- DLL Reflection (در صورت استفاده از DLL)

برخی مواردی که می توانند در معماری امنیتی نرم افزارها رعایت شوند:

- رعایت قواعد Protection in depth در معماری
- تبعیت از قواعدMicrosoft Security Development Lifecycle
- موفقیت در آزمون های Penetration tests گروه امنیت مبتنی بر استاندارد OWASP
- هماهنگی با قواعد FxCop
- استفاده از استانداردهای ISO12207, 15288, 15289 جهت تولید نرم افزار

## سازمان های امنیتی

برخی از این سازمان ها با انتشار خبرنامه، برگزاری کنفرانس و مراکز آموزشی می توانند کمک زیادی در افزایش دانش امنیتی سازمان ها نمایند.

### ACM[۱۰]

از قدیمی ترین سازمان های حرفه ای در حوزه رایانه می باشد که گروه های تخصصی زیادی دارد و در زمینه امنیت و کاربرد امنیت نیز فعالیت دارد.

### ASIS[۱۱]

یک سازمان حرفه ای در حوزه امنیت با بیش از ۲۵ کمیته دائمی در زمینه امنیت می باشد. هر ماه مجلیه ای نیز در حوزه امنیت به چاپ می رساند.

### CSI[۱۲]

در سال ۱۹۷۴ راه اندازی شد و از برگزاری کارگاه ها و کنفرانس های امنیتی حمایت مالی می کند. یک مجله تحقیقاتی و یک نشریه تخصصی در زمینه امنیت دارد.

### EFF[۱۳]

از مسائل مرتبط با آزادیهای مدنی و اینترنتی حمایت قانونی می کند.

### EPIC[۱۴]

یک مرکز تحقیقات عمومی که موضوعات مرتبط با محرمانگی اطلاعات الکترونیکی را مورد بررسی قرار می دهد. همچنین از مسائل حریم خصوصی و آزادی مدنی حمایت قانونی می کند.

### HTCIA[۱۵]

و بسیاری موسسات دیگر که در حوزه امنیت از نظر تامین اطلاعات، قوانین و حتی پی گیری های قانونی فعال می باشند:

ISSA

ISACA

---

[۱۰] Association for Computing Machinery
[۱۱] American Society for Industrial Security
[۱۲] Computer Security Institute
[۱۳] Electronic Frontier foundation
[۱۴] Electronic Privacy Information Center
[۱۵] High Technology Crimes Investigation Association

ISC

The Internet Society

IEEE-CS

FIRST[1]

CERT/CC[2]

## گواهینامه امنیتی

از گواهینامه های معتبر بین المللی در حوزه امنیت می توان به CISSP [3] اشاره نمود. این مدرک مستقل از هرنوع نرم افزار و سخت افزار شرکتی می باشد. این مدرک توسط کنسرسیوم ISC طراحی و ارائه شده است و به شرکت کنندگان داشتن دانش در حوزه های زیر را پیشنهاد می کند:

۱. سیستم‌های کنترل دسترسی
۲. توسعه سیستم‌ها وبرنامه‌های کاربردی
۳. برنامه ریزی برای مقابله با بلاهای طبیعی و خطرات کاری
۴. رمزنگاری
۵. مسائل حقوقی
۶. امنیت عملیاتی
۷. امنیت فیزیکی
۸. مدلها و معماری امنیتی
۹. تمرین‌های مدیریت امنیت
۱۰. امنیت شبکه داده‌ای و مخابراتی

[1] Forum of Incident and Response Security Teams
[2] Computer Emergency Response Team / Coordination Center
[3] Certified Information Systems Security Professional