

به نام خدا

دوره آموزشی

کلیات و مفاهیم دولت الکترونیک

اداره فناوری اطلاعات ارتباطات و تحول اداری

اداره کل دامپزشکی خراسان جنوبی

زمستان ۱۴۰۲

ظهور فناوری اطلاعات تمامی حیطه های بشری را مورد دستخوش قرار داده است. در این میان دولت‌ها برای ارائه خدمات به ذی نفعان اجتماعی باید به تعریف نقشها و کارکردهایشان پردازد که برای نیل به این هدف دولت الکترونیک شکل گرفته است. دولت الکترونیکی، دولتی هوشمند است که به فناوری های ارائه اطلاعات و خدمات پیوسته از طریق اینترنت یا سایر روش های دیجیتالی توسط دولت ها اطلاق گردد. انقلاب الکترونیکی این ظرفیت را دارد تا بخش دولتی را تغییر شکل دهد و رابطه میان دولت و شهروندان را از نو پایه ریزی نماید.

داده چیست؟ نوعی اطلاعات خام پردازش نشده است.

اطلاعات چیست؟ مجموعه ای از داده ها که معنی دار شده اند.

معنای دانش: اطلاعات قابل درک و ارزشمندی است که در پرتو تجارب و بستر آگاهی های فردی شکل گرفته و نهادینه می شود و به حل مسئله می انجامد.

انواع دانش: ۱- دانش فردی ۲- دانش عمومی ۳- دانش صریح ۴- دانش نهان

مفهوم علم؟ یکی از انواع دانش می باشد که نیازمند تحلیل و اثبات به روش های خاص می باشد.

مفهوم فناوری :

فناوری متشکل از مجموعه دانش، محصولات، فرایندها، ابزار، روش‌ها و سیستم‌هایی است که در جهت خلق و ساخت کالاها و ارائه خدمات به کار می‌رود، به بیان ساده‌تر اجرای عملی دانش است.

انواع فناوری : اطلاعات-ارتباطات-سرگرمی-فضایی-پزشکی- عملیاتی و ...

تعریف فناوری اطلاعات : فناوری اطلاعات به معنی و مفهوم بسیار ساده یعنی علم استفاده از یک سری ابزار که این ابزار همان پردازش، نگهداری، جمع‌آوری، ذخیره، توزیع، انتقال، امنیت است که بر روی اطلاعات اعمال میشود. سه محور اصلی در فناوری اطلاعات سخت افزار ، نرم افزار و فکر افزار (مدیریت دانش) می باشد.

مزایا :

راحت‌تر کردن زندگی-ارتباط با راه دور-درمان بیماری‌ها - ساخت دارو و واکسن‌ها و ...

معایب :

کاهش مطالعه-زیست محیطی-کاهش فعالیت‌های جسمانی-پدید آوردن برخی بیماری‌ها-انزوای اجتماعی-هدر رفت وقت و پول-نقض حریم شخصی-وابستگی و اعتیاد-محتوای نامناسب-خرابکاری و جنایت

ساختار سازمانی :

به طور یقین تمامی کسب و کارها دارای ساختار سازمانی هستند.

خصوصیات ساختار سازمانی

۱- توضیحی از روند کاری و مسئولیت‌هاست

۲- راهنمای روزانه برای مدیریت وظایف، تعامل و گزارشگری کارمندان است

۳- روشی سریع برای برای کمک به کارکنان است تا بدانند باید از کجا برای حل مسائل خاص کمک بگیرند.

انواع ساختارهای سازمانی:

ساختار سازمانی سلسله‌مراتبی

ساختار عملکردی

ساختار سازمانی تقسیم‌شده

ساختار سازمانی ماتریسی

ساختار تیم‌محور

ساختار سازمانی افقی یا مسطح (Horizontal/ Flat)

ساختار سازمانی شبکه‌ای (Network)

مفهوم تحول اداری :

تحول سازمانی یا Organizational Transformation فرآیندی است که توسط رهبران سازمان برای ایجاد تغییر در نحوه عملکرد یک سازمان دنبال می‌شود و هدف از آن می‌تواند دستیابی به مزیت رقابتی، مقابله با یک چالش مهم و یا تضمین آینده سازمان باشد.



انواع تحول سازمانی :

- ۱- تحول در فرهنگ سازمانی
- ۲- تحول در فرآیندهای سازمانی
- ۳- تحول در تکنولوژی سازمانی

مزایای تحول سازمانی :

- ۱- بهبود کارایی سازمان
- ۲- ارتقاء فرهنگ سازمانی
- ۳- اثرگذاری بیشتر بر بازار
- ۴- افزایش مزیت رقابتی

دولت الکترونیک : (SMART)

دولت الکترونیک به وضعیتی اطلاق می شود که سازمان های قانون گذاری، مجری و قضائی عملیات داخلی و خارجی خود را الکترونیکی کنند و از سیستم های شبکه ای به منظور ارائه خدمات عمومی به شهروندان با کیفیت بهتر، به طور موثری استفاده کنند.

دولت الکترونیک را در یک کلمه خلاصه کرده اند که به آن SMART می گویند.

۱- SMALL (کم اهمیت)

۲- Moral (اخلاقی)

۳- AUDITABLE (اطلاع رسانی)

۴- RESPONSIBLE (پاسخگو بودن)

۵- TRANSPAREN (شفافیت)

دولت الکترونیک عبارتست از استفاده از ابزارها و سیستم هایی ایجاد شده توسط فناوری اطلاعات و ارتباطات، به منظور ارائه خدمات عمومی بهتر به شهروندان و کسب و کارها.

اهداف دولت الکترونیک :

هدف دولت الکترونیکی، توسعه و رشد فعالیت های آنلاین است که از طریق چهار حوزه زیر میسر می شود:

- ۱- تمرکز این مؤلفه بر شهروند محوری و ارتقا زندگی شهروندی است
- ۲- استفاده از خدمات و اطلاعات ارایه شده توسط دولت به بازرگانان در سطح محلی و بین المللی
- ۳- بهینه سازی نحوه ارتباطات دولت با کارمندان سازمان های مختلف دولتی
- ۴- تعاملات و ارتباطات میان دولت ها نظیر تبادل اسناد و اطلاعات به صورت الکترونیکی

دولت الکترونیک و شفافیت حاکمیت :

اساسی ترین برنامه های دولت الکترونیک ، تأثیر آن بر شفاف سازی و کاهش فساد است.

مزایای ناشی از شفاف سازی اطلاعات :

- ۱- مشارکت مدنی ۲- مانع از فساد ۳- زمینه جلوگیری از دستکاری ، رشوه و فساد
- ۴- مجازات معنوی فساد از طریق قرار گرفتن در معرض دید عموم ۵- قابلیت کشف فساد و بهبود پاسخگویی
- ۵- استانداردسازی روش های ارایه خدمات ۶- کاهش زمان خدمات رسانی و کاهش هزینه ها

مزایا و دستاوردهای دولت الکترونیک

- ۱- کاهش تشریفات دست و پا گیر اداری
- ۲- ارائه خدمات الکترونیکی و اطلاع رسانی الکترونیکی
- ۳- تأمین رضایت شهروندان
- ۴- افزایش اقتدار ملی
- ۵- افزایش بهره‌وری
- ۶- توسعه مشارکت مردمی شفافیت امور و کاهش رشوه خواری
- ۷- اثرات مثبت زیست‌محیطی
- ۸- کار آفرینی
- ۹- ارتقا سطح کیفیت سیاست گذاری و تدوین قوانین
- ۱۰- تنظیم بهتر مقررات

ساختار دولت الکترونیک

دولت الکترونیک می بایست بستری ایجاد کند که مردم بتوانند با مسئولین دولتی ارتباط برقرار کرده و به انجام کارهایی همچون کسب مجوزها و ... پردازند. همچنین دولت از این راه می تواند با شرکت ها و دولت های دیگر به تعامل پردازد.

ابعاد این دولت بر چهار قسم ۱. دولت - شهروند، ۲. دولت - بازار، ۳. دولت - دولت و ۴. درون دولت است تا منجر به افزایش سطوح خدمات مشتری و کاهش هزینه‌ها، توزیع اطلاعات، ایجاد رضایت‌مداری در مشتریان، کمک بر تمرکز گرایی در برخی فعالیت‌ها، مدیریت دولتی کاراتر، کاهش فساد اداری و شفافیت بیشتر امور، انجام فعالیت‌های مالی و اعتباری، شرکت در انتخابات و برخی از این امور شود.

نمادهای مورد استفاده در دولت الکترونیک :

۱- G2C دولت و شهروندان ۲- G2C دولت و مصرف کننده ۳- G2B دولت و سازمان های تجاری و خصوصی
۴- G2G دولت ها و ارگان های درون دولت ۵- G2E دولت با کارمندان دولتی ۶- C2G مردم و دولت

معماری مفهومی خدمات دولت الکترونیکی



موانع گسترش دولت الکترونیک :

۱- عوامل فرهنگی

۲- عوامل سازمانی و اداری

۳- کمبود منابع

موانع استقرار دولت الکترونیکی در سازمان ها:

۱- عدم احساس نیاز به وجود دولت الکترونیکی

۲- عدم حمایت مدیریت ارشد سازمان ها

۳- ناتوانی در مرزبندی بین اطلاعات محرمانه و اطلاعاتی که باید در دسترس شهروندان و بنگاه های اقتصادی قرار گیرد.

۴- هزینه سنگین ایجاد، نگهداری و توسعه شبکه های اطلاع رسانی و پایگاه های اطلاعاتی

۵- کمبود تخصص فناوری اطلاعات در برخی کشورها

دولت الکترونیک و روند آن در ایران :

*سایتهای دولتی

*دفاتر خدمات الکترونیک

*اعطای وام های از طریق طرح های توسعه ای

*تاکید دولت و تصویب بکارگیری خدمات الکترونیکی در سازمان های دولتی

*ارزیابی مستمر خدمات دولت الکترونیک از طریق تجزیه و تحلیل و ارایه راهکارها

نقشه راه توسعه دولت الکترونیکی :

شورای عالی فناوری اطلاعات در ششمین جلسه مورخ ۱۳۹۲/۱۲/۲۰ در راستای سیاست های کلی نظام اداری و

اقتصاد مقاومتی ابلاغی مقام معظم رهبری و برنامه پنجم توسعه جمهوری اسلامی ایران و با هدف چابک سازی،

کاهش زمان و هزینه خدمات اداری، شفاف سازی و مبارزه با فساد اداری، «ضوابط فنی و اجرایی توسعه دولت

الکترونیکی» را تصویب نمود. که مشتمل بر دو بخش به شرح ذیل می باشد :

بخش اول : آیین نامه توسعه خدمات الکترونیکی دستگاههای اجرایی (مصوب شورای عالی اداری) مشتمل بر ۷ فصل

بخش دوم : ضوابط فنی اجرایی توسعه دولت الکترونیکی (مصوب شورای عالی فناوری اطلاعات) مشتمل بر ۸ فصل

کارکردها و نوآوری ها در دولت الکترونیک :

۱- اقتصاد الکترونیکی : شبکه‌ای جهانی از اقتصاد و فعالیت‌های اجتماعی است که از طریق فناوری اطلاعات مانند اینترنت، موبایل و شبکه‌ها محقق شده است دارای دو رکن اساسی تولید کالای دیجیتال و تولید کالای غیر دیجیتال می باشد

۲- آموزش الکترونیکی : امکان آموزش های از راه دور ، در دسترس بودن محتواهای آموزشی و ...

۳- تجارت الکترونیک : به خرید و فروش کالا یا خدمات به صورت الکترونیکی در سطح اینترنت اشاره دارد. تجارت الکترونیکی بخش اساسی بسیاری از مشاغل است که به فروش آنلاین محصولات یا خدمات فیزیکی متکی هستند.

انواع تجارت الکترونیک :

۱- بنگاه - مصرف کننده (B2C)

۲- بنگاه - بنگاه (B2B)

۳- مصرف کننده - مصرف کننده (C2C)

۴- مصرف کننده - بنگاه (C2B)

۵- بنگاه - سازمان دولتی (B2A)

۶- مصرف کننده - سازمان دولتی (C2A)



۴- گردشگری الکترونیک : گردشگری الکترونیک به کاربرد فناوری های نوین در صنعت گردشگری اشاره می کند و کارهایی از قبیل رزرو کردن بسته های سفر، پروازها، هتل ها و عرضه ی اطلاعات گردشگری را سهولت می بخشد.

۵- رای گیری الکترونیک : یکی از مهمترین اهداف دولت الکترونیکی صرفه جویی در وقت مردم و همچنین کاهش هزینه های اجرایی سازمانهای دولتی است که سیستم رای گیری الکترونیکی به عنوان زیر سیستم دولت الکترونیکی هم ، چنین اهدافی را دنبال میکند.

سیستم های رای گیری الکترونیکی

* رای گیری کامپیوتری :

* رای گیری اینترنتی :

- 
- 
- نقش شبکه های اجتماعی در توسعه دولت الکترونیک :
- * ابزارهای بهینه و کم هزینه ای را برای تبلیغ تجارت های آنلاین
 - * اهمیت بالای آن برای کسب و کارها از دید مشتریان
 - * تمایل به خرید و فروش و مبادلات الکترونیکی و مجازی
 - * خصیصه های ساختاری و رابطه ای شبکه های اجتماعی بر تعاملات مابین مشتریان تاثیر دارد
 - * ایجاد شبکه های اجتماعی و نفوذ هر چه بیشتر آنها در میان کاربران مختلف به ابزاری مناسب برای تبلیغات و تجارت الکترونیک برای شرکت ها و سازمان ها بدل شده

مزایای شبکه های اجتماعی مجازی

- ۱- انتشار سریع و و آزادانه اخبار و اطلاعات، افزایش قدرت تحلیل و تقویت روحیه انتقادی
- ۲- افزایش سرعت در فرایند آموزش و ایجاد ارتباط شبانه روزی بین استاد و شاگرد
- ۳- افزایش اعتماد، صمیمیت و صداقت در فضای مجازی
- ۴- امکان بیان ایده ها به صورت آزادانه و آشنایی با ایده‌ها، افکار و سلیقه های دیگران
- ۵- کارکرد تبلیغی و محتوایی

پیامدهای منفی شبکه‌های اجتماعی

- ۱- شکل گیری و ترویج سریع شایعات و اخبار کذب
- ۲- تبلیغات ضد دینی و القای شبهات
- ۳- نقض حریم خصوصی افراد

امنیت دولت الکترونیک :

امنیت سایبری از یک مجموعه پروتکل تشکیل شده است که وظیفه دارد از اطلاعات شما در مقابل حملات هکرها محافظت کند. در صورتی که این محافظت از اطلاعات در فضای سایبری به خوبی انجام شود، می‌توانید در مواقع بحرانی مانند رخ دادن خطاها یا خراب شدن هارد و یا قطعی برق، اطلاعات خود را بازیابی کنید.

انواع سایبر :

فضای سایبری (Cyberspace) ، شهروند سایبر (Cybercitizen) ، پول سایبر (Cybercash) ، فرهنگ سایبر (Cyberculture) ، راهنمایی فضای سایبر (CyberCoach) ، تجارت سایبر (Cyberbussiness) ، کانال سایبر (Cyberchannel)

فضای سایبری Cyberspace:

در معنا به مجموعه‌هایی از ارتباطات درونی انسانها از طریق کامپیوتر و مسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود.

تعریف فضای مجازی :

فضای مجازی به هر محیطی اطلاق می‌شود که به صورت آنلاین در دسترس قرار دارد و کاربران می‌توانند با استفاده از اینترنت و دستگاه‌های مختلف به آن دسترسی داشته باشند. این فضا شامل وبسایت‌ها، اپلیکیشن‌ها، رسانه‌های اجتماعی، پیام‌رسان‌ها، بازی‌های آنلاین، شبکه‌های عصبی و... است.

امنیت سایبری چیست؟

امنیت سایبری به معنای محافظت از شبکه‌ها و سیستم‌هایی است که حاوی اطلاعات هستند تا در صورتی که حمله‌ای به این اطلاعات رخ داد بتوان آن‌ها را تغییر داد و یا جابجا و یا حتی در موقعیت‌های بحرانی‌تر بتوان آن‌ها را نابود کرد.

اهمیت رعایت اصول امنیت سایبری

همان‌طور که گفتیم تامین امنیت سایبری به مثابه‌ی یک جنگ همیشگی است، تنها در سال ۲۰۱۹ میلادی ۷,۹ میلیارد حمله‌ی سایبری رخ داده است که نسبت به سال قبل از آن افزایش چشمگیر دو برابری داشته است. هدف بیشتر این حملات اطلاعات پزشکی و مالی افراد بوده است. بدون وجود امنیت سایبری، اطلاعات شخصی افراد و سازمان‌ها به دست افراد سودجو می‌افتد و تبعات جبران‌ناپذیری مانند جعل هویت افراد و... به دنبال خواهد داشت.

انواع تهدیدات سایبری :

به صورت کلی تهدیدات سایبری براساس هدفی که دنبال می کنند به سه دسته ی زیر تقسیم می شوند:

۱- جرایم سایبری یا Cyber Crime

۲- حمله ی سایبری یا Cyber Attack

۳- تروریسم سایبری یا Cyber Terrorisom

انواع تهدیدات سایبری به صورت جزئی، دسته های زیر را شامل می شوند:

۱- تهدیدات شبکه ای:

هکرها توسط ویروس ها و بدافزارها و با اهداف تغییر و سرقت اطلاعات به شبکه نفوذ می کنند. این حملات به دو نوع فعال و غیرفعال می توانند انجام بگیرند.

۲- تهدیدات برنامه های کاربردی :

خلل در برنامه های کاربردی مانند برنامه های مدیریت حساب بانکی، برنامه های تلفن همراه و لپ تاپ می تواند بستر مناسبی برای هکرها باشد تا از آن طریق بتوانند کدهای برنامه را تغییر دهند و باعث اختلال در کار برنامه ها شوند.

۳- تهدیدات نقاط پایانی :

امروزه که به دلیل قرنطینه و کرونا بسیاری از مشاغل به صوت دورکاری انجام می-شود تعداد کارمندانی که از راه دور و از خانه‌ی خود به شبکه‌ی سازمانی وصل می‌شوند افزایش یافته است و به تبع آن ریسک سرقت اطلاعات از طریق سیستم شخص و نفوذ به شبکه‌ی سازمانی بالاتر می‌رود.

۴- تهدیدات دستکاری داده‌ها:

در صورتی که هکر با هدف دستکاری اطلاعات پایگاه‌های داده به یک سیستم یا شبکه نفوذ کند می‌تواند با ارتقای سطح مجوزهای خود مانند مدیر شبکه به ویرایش اطلاعات و حذف آن‌ها پردازد. (یکی از اقدامات امنیتی برای جلوگیری از این پیشامد استفاده از لایه‌های امنیتی چندگانه برای سیستم‌ها و شبکه‌ها است

۵- تهدیدات هویتی:

در حملاتی که توسط سرقت هویتی کاربران رخ می‌دهد هکر با جعل هویت مدیران و مسئولان ارشد یک سازمان، به اطلاعات محرمانه‌ی کارمندان و پسوردها دسترسی پیدا کنند. فیشینگ یکی از این نوع حملات است.

۶- تهدیدات پایگاه‌های داده و زیرساخت‌ها:

در صورتی که روتری به درستی تنظیم نشده باشد یا دارای خلل باشد به سادگی می‌تواند هدف هکرها قرار بگیرد و دسترسی به منابع و شبکه‌ها و سیستم‌های بزرگ را برای آن‌ها فراهم کند. در مورد حمله به زیرساخت‌ها نیز هکرها می‌توانند با نفوذ به سرورها اهداف خود را عملی کنند.

۸- تهدیدات تجهیزات همراه:

ساده‌ترین روش برای نفوذ به یک شبکه‌ی سازمانی از طریق تلفن همراه تنها یک کارمند است که روی گوشی خود بدافزار نصب کرده باشد. این بی‌احتیاطی، رهی برای نفوذ هکرها به شبکه‌ی سازمانی که در آن کار می‌کند فراهم می‌کند و امنیت اطلاعات همه‌ی کارمندان آن شبکه را به خطر می‌اندازد.

توصیه‌هایی برای حفظ امنیت اطلاعات خود در فضای سایبری :

- از آنتی ویروس‌ها یا برنامه‌های امنیتی برای دستگاه‌های خود استفاده کنید.

- رمزهای عبور خود را در دوره‌های زمانی کوتاه تغییر دهید.

- فایروال سیستم خود را فعال کنید.

- اطلاعات خود را به درستی رمزگذاری کنید.

- نکات مربوط به جعل آدرس اینترنتی درگاه‌های بانکی را جدی بگیرید.

- رمزگذاری دو مرحله‌ای را روی برنامه‌های کاربردی خود فعال کنید تا بدون احراز هویت دسترسی به اطلاعاتتان غیرممکن باشد.

- برای اتصال به شبکه‌های سازمانی یا اطلاعات مهم و حساس از وای فای عمومی و شبکه‌های اینترنت نامعتبر استفاده نکنید چرا که احتمال شنود اطلاعات وجود دارد.
- آپدیت نرم افزارها و آنتی ویروس خود را جدی بگیرید.
- ایمیل‌های ناشناس را بدون باز کردن حذف کنید ولی در صورتی که ایمیل را باز کردید بر روی لینک‌های پیوستی آن کلیک نکنید.
- USB‌های ناشناس را به لپ تاپ و سیستم‌های خود متصل نکنید.

امنیت سایبری برای شرکت‌ها و سازمان‌ها :

۱- امنیت زیرساخت‌های حیاتی

۲- امنیت شبکه:

۳- امنیت سایبری با استفاده از فضای ابری:

۴- امنیت با برنامه‌های امنیتی

۵- امنیت اپلیکیشن‌ها

۶- امنیت اطلاعاتی

۷- امنیت عملیاتی