علوم اسلامی انسانی، شماره ۱۶، زمستان ۱۳۹۷، ص ۱۳۴- ۱۲۲

ISSN: 2538-3671
http://www.johi.ir

مجله علمی علوم اسلامی انسانی (سال چهارم)
شماره ۱۶/ زمستان ۱۳۹۷ / ص ۱۳۴-۱۲۲

# فرهنگ حمایت از نوآوری و رفتار شهروندی سازمانی در امنیت سیستم اطلاعات الکترونیکی در سازمان های دولتی

**مرتضی امیری[۱]، شمس الدین نیک منش[۲]، شهرام هاشم نیا[۳]**

[۱] کارشناس ارشد، مدیریت دولتی، گرایش مدیریت سیستم های اطلاعاتی پیشرفته، دانشگاه پیام نور، تهران، ایران
[۲] استادیار، گروه علوم تربیتی، دانشگاه پیام نور، تهران، ایران
[۳] استادیار، گروه مدیریت، دانشگاه پیام نور، تهران، ایران

**نویسنده مسئول:**
شمس الدین نیک منش

**چکیده**

ظهور اینترنت، دستیابی آسان و ارتباط نسبتاً مقرون بصرفه ای را بین سازمان ها، شرکت و مشتریانش ایجاد کرده است. دولت الکترونیک بعنوان یک ابزار کارآمد توسط دولت برای ارتباط با کاربر می باشد. مباحث امنیت اطلاعات موانعی جدی بر سر راه دولت الکترونیک هستند. اکثر دولتها باید همواره به نوآوری در خصوص امنیت سیستمهای اطلاعاتی (ISS) بپردازند. ISS هم بعنوان عامل موفقیت، هم بعنوان مانعی برای دولت الکترونیک شناسایی شده است. هدف از این تحقیق و پژوهش تاثیر فرهنگ حمایت از نوآوری و رفتار شهروندی سازمانی در امنیت سیستم اطلاعات الکترونیکی در سازمان های دولتی بوده است. جامعه آماری این تحقیق ۵۰۰ نفر از کارکنان و مدیران سازمان فناوری اطلاعات و ارتباطات شهرداری تهران بوده است. بر اساس جدول مورگان ۲۱۷ نفر بعنوان نمونه تصادفی ساده انتخاب شده اند. برای آزمون فرضیه ای از نرم افزار SMART.PLS استفاده شده است. نتایج تحقیق نشان داد تناظر تقلیدی در ارتباط با امنیت سیستم اطلاعات تاثیر مثبت فرهنگ حمایتی و نوآوری بر رفتار شهروندی فردی، رفتار شهروندی سازمانی و مشروعیت سازمانی را برای ISS نشان می دهد. همچنین فرهنگ حمایتی ـ نوآوری، تاثیری مثبت بر کارآیی و اثربخشی و مشروعیت سازمانی ISS دارد. مشروعیت سازمانی، رفتار شهروندی فردی وسازمانی، تاثیری مثبت بر کارآیی و اثربخشی ISS دارد. با توجه به بررسی تایید نتایج فرضیات مبنی بر تاثیر فرهنگ حمایت از نوآوری و رفتار شهروندی سازمانی، رفتار شهروندی فردی بر کارایی و اثربخشی امنیت سیستم اطلاعات الکترونیکی در سازمان های دولتی در مجموع می توان نتیجه گرفت فرضیه اصلی در بازه معنا داری است و مورد تایید است.

**کلمات کلیدی:** فرهنگ حمایت نوآوری، امنیت سیستم های اطلاعات الکترونیک، رفتار شهروندی سازمانی، سازمان های دولتی، فناوری اطلاعات و ارتباطات شهرداری تهران.

ISSN: 2538-3671
http://www.johi.ir

**مقدمه**

دولت الکترونیک به عنوان یک ابزار کارآمد توسط دولت برای ارتباط با کاربر می باشد. در سطح بالاتری به منظور افزایش مشارکت کارکنان، مکانیزمهایی به منظور افزایش اعتماد به خدمات دولت الکترونیک بایستی در نظر گرفته شود. پروژه های دولت الکترونیک در بسیاری از کشورها موفق نبوده است. موفقیت طرحهای مختلف دولت الکترونیک نه تنها به ارائه دهندگان خدمات، بلکه به کاربران نهایی نیز بستگی دارد . بنابراین برای ارائه دهندگان خدمات الکترونیک، شناسایی عوامل کلیدی در استفاده از خدمات دولت الکترونیک ضروری می باشد (شارما[1]،۲۰۱۵). بسیاری از دولتها، سیستمهای دولت الکترونیک را توسعه داده اند. نشان داده شده است که طرحهای ابتکاری دولت الکترونیک، می توانند مزایایی را از نظر کارآیی، بهره وری، صرفه جویی در هزینه، و کیفیت خدمات فراهم کنند. از اواسط دهۀ ۱۹۹۰ به بعد، فشارهای هم ریختی و تناظر، باعث گسترش سریع نفوذ دولت الکترونیک شده و سیستمهای موفق دولت الکترونیک مورد ارزیابیهای مقایسه ای قرار گرفته و محک زده شده اند (اوم[2]، ۲۰۱۲). بخاطر تناظر تقلیدی، اغلب فشاری بر روی دولتها وجود دارد تا برنامه ها و استراتژیهای نوآورانه ای را در پیش بگیرند. با این حال چنین برنامه ها و استراتژیهایی، گاهی به شیوه ای غیر رضایت بخش اجرا می شوند. دولت الکترونیک شامل طیف وسیعی از فاکتورها و عوامل است از قبیل فناوری و بکارگیری اطلاعات، عناصر سازمانی، چیدمانهای نهادی، و زمینه های اجتماعی ـاقتصادی. با این حال درکی ناکافی از روابط موجود در میان این فاکتورها، مکررا باعث ناکامی دولت الکترونیک شده است. از آنجا که دولت الکترونیک در اواسط دهۀ ۱۹۹۰ پدیدار گشته، تحقیق در مورد این موضوع نسبتا تازه متولد بوده و در حال رشد است. با وجود مزایای دولت الکترونیک و این واقعیت که دولت الکترونیک به شکلی فزاینده در سراسر جهان پذیرفته می شود، اما خدمات دولت الکترونیک به واسطۀ حملات سایبری تهدید می شوند. اکثر دولتها اقدام به توسعۀطرحهای امنیتی کرده اند؛ برای مثال دولت فدرال آمریکا طرحی را برای دفاع سایبری توسعه داده است (ژائو وژائو[3]، ۲۰۱۰).

براساس تحقیقات نوریس و کروسی[4] (۲۰۰۸)، مباحث امنیت اطلاعات، موانعی جدی بر سر راه دولت الکترونیک هستند و اکثر دولتها باید همواره به نوآوری در خصوص امنیت سیستمهای اطلاعاتی (ISS) بپردازند. ISS از اواخر دهۀ ۱۹۹۰ بشدت مورد توجه قرار گرفته و مباحث زیادی پیرامون آن پدیدار گشته است. سازمانهایی که به دنبال حفاظت از اطلاعات خود هستند باید کنترلهایی بر سهامداران داخلی را هم در نظر داشته باشند؛ تعداد قابل توجهی رخنه به امنیت اطلاعات به دلیل متابعت ضعیف از قواعد ISS در میان کاربران رخ داده است. به بیان دیگر، سهامداران داخلی هم می توانند امنیت اطلاعات را به خطر بیندازند. اهمیت ISS در حفاظت از اطلاعات سازمانی به شکلی فزاینده، تشخیص داده شده است. بعنوان یک فرآیند مستمر، ISS را می توان دربر گیرندۀ سیستمها و پروسه هایی دانست که به منظور حفاظت از دارایی های اطلاعاتی یک سازمان در برابر هر شخص یا نهاد غیر مجاز برای دسترسی به آن اطلاعات، طراحی شده اند. نقض ISS باعث آسیب دیدن سازمانهای خصوصی می شود زیرا باعث تلفات مالی شده و به شهرت این سازمانها آسیب می زند. در بخش دولتی، نقض ISS می تواند منجر به آسیب جدی تری به شهرت سازمان شود؛ خسارتهای اقتصادی، سیاسی و مالی پیچیده ای را به دنبال داشته باشد و از همه مهمتر اینکه اعتماد عمومی را به دولت الکترونیک از بین می برد (هوانگ و چوی، ۲۰۱۷)

در مقالات مربوط به دولت الکترونیک، ISS را بعنوان یکی از شایع ترین مشکلات شناسایی کرده اند. ISS هم بعنوان عامل موفقیت و هم بعنوان مانعی برای دولت الکترونیک شناسایی شده است. مباحث ISS دولت الکترونیک مورد مطالعه عبارتند از حفاظت از داد های شخصی شهروندان، امنیت اطلاعات برای دموکراسی الکترونیک (شامل رأی گیری الکترونیک و مشارکت شهروندان)، اجرا، ترورها و حملات سایبری، امنیت سیستم برای محاسبات ابری، و امنیت مبادلات. با این حال تحقیقات انجام شده در مورد ISS در دولت الکترونیک، کمتر به رخنه های امنیتی ناشی از افراد داخل سازمان توجه کرده اند در حالیکه مطالعات ISS، افراد داخل سازمان را بعنوان فاکتوری شناسایی کرده اند که ضعیف ترین ارتباط را در ISS دارد. از آنجا که حریم خصوصی و امنیت اطلاعات در دولت الکترونیک تا حد زیادی بر اعتماد و اطمینان کاربران تاثیر می گذارد آنهم در زمانی که اطلاعات، داده های شخصی و خدمات بصورت آنلاین تحویل و ارائه می شوند، لذا حریم خصوصی و امنیت را باید به شکلی جدی بررسی کرد تا به اعتماد عمومی دست یافت. در مقایسه با سازمانهای خصوصی، که زیانهای آنها مالی است، موارد نقض ISS در ارتباط با دولت الکترونیک می تواند تبعات جدی تری را برای سازمانهای دولتی به همراه داشته باشد؛ ممکن است آسیبی

[1] sharma
[2] Eom
[3] Zhao and Zhao
[4] Coursey and Norris

ISSN: 2538-3671
http://www.johi.ir

ماندگارتر بر شهرت آنها وارد شود و ممکن است زیانهای اقتصادی، سیاسی، مالی پیچیده ای ببینند و اعتماد مردم را از دست بدهند(هوانگ و چوی، ۲۰۱۷)

استقرار دولت الکترونیک و خدمات مرتبط با آن رامیتوان ضروریترین اقدام دولت ها برای کاربرد فناوری اطلاعات IT درجامعه عنوان نمود دستاوردهای استقرار دولت الکترونی که درزمینه های سیاسی اقتصادی اجتماعی محیط زیست و ... برای کشورها برکمترکسی پوشیده است ولی آنچه ازاهمیت ویژه ای برخوردار است لزوم توجه به چالشها و پیش نیازهای استقرار این سیستم می باشد شاید بتوان امنیت اطلاعات را یکی ازحیاتی ترین نیازها و یکی ازچالش برانگیز ترین عوامل دردستیابی به این هدف عنوان نمود چرا که درصورت مغفول واقع شدن این مهم ممکن است با استقرار دولت الکترونیک راهی برای سوء استفاده سودجویان و دشمنان هموار شده و با نتیجه معکوس و تبعات بعضا جبران ناپذیر سیاسی اقتصادی و اجتماعی برای کشور به دنبال داشته باشد. پیشرفت سریع جوامع و رشد فن آوری های اطلاعاتی، مباحث جدیدی در حوزه شهرداری ها مطرح شده است که استقرار آن ها در مقیاس جهانی و حتی ملی و منطقه ای، می تواند موجب تسریع در پیشرفت مادی و معنوی شهروندان و نیز صرفه جویی در وقت و هزینه ها شود. اصولاً ارائه خدمات فراگیر به شهروندان به صورت متمرکز در یک شهر با تحقق شهرداری الکترونیک میسر می گردد. با توجه به چالش های مطرح شده، تحقیق حاضر در صدد پاسخ به پرسش زیر است:

تاثیر فرهنگ حمایت از نوآوری و رفتار شهروندی سازمانی در امنیت سیستم اطلاعات الکترونیکی در سازمان های دولتی، چگونه است؟

در ادامه مقاله به ارایه یک نمای کلی از ادبیات پژوهش و فرضیه ها پرداخته می شود.در بخش بعدی، به طرح پژوهش و جمع آوری اطلاعات پرداخته  پس از تفسیر یافته های پژوهش، به نتیجه گیری پرداخته می شود.

## ادبیات پژوهش

دولت الکترونیک به عنوان استفاده از فناوری اطلاعات و ارتباطات، فن آوری تلفن همراه و اینترنت به منظور ارائه خدمات مورد نیاز به مشتریان تعریف شده است که بهبود عملکرد سازمان های دولتی، تسهیل مشارکت عمومی موفق و توسعه فرآیند اجتماعی شهروندان را در بر می گیرد (ابوشناب[5]، ۲۰۱۶). دولت الکترونیک به عنوان یک ابزار برای تغییر مفهوم دولت و در نتیجه مشارکت شهروندان، شفافیت در عملکرد عمومی و بهره وری در ارائه خدمات عمومی بوده است. دولت در سراسر جهان، فناوری اطلاعات و ارتباطات، فرصت بالقوه ای برای افزایش بهره وری داخلی و ارائه بهتر خدمات را به مشتریان فراهم می نماید (آونیش و همکاران[6]، ۲۰۱۶).

با وجود مزایای دولت الکترونیک و این واقعیت که دولت الکترونیک به طور فزاینده‌ای در سراسر جهان مورد پذیرش قرار می‌گیرد، خدمات دولت الکترونیک تهدید شده‌است.بیشتر دولت‌ها ابتکارهای امنیتی را توسعه داده‌اند با وجود مزایای دولت الکترونیک و این واقعیت که دولت الکترونیک به طور فزاینده‌ای در سراسر جهان مورد پذیرش قرار می‌گیرد، خدمات دولت الکترونیک تهدید شده‌است.بیشتر دولت‌ها ابتکارهای امنیتی را توسعه داده‌اند؛ ژائوو ژائو[7] (۲۰۱۰) بیان کردند مسایل امنیتی اطلاعاتی موانع جدی برای دولت الکترونیک هستند و اغلب دولت‌ها باید به طور مداوم در رابطه با امنیت سیستم اطلاعات (امنیت اطلاعات)نوآوری کنند.از اواخر دهه ۱۹۹۰ توجه زیادی به امنیت سیستم‌های اطلاعات شده‌است و تعداد مسائل پیرامون امنیت سیستم‌های اطلاعات در حال افزایش است سازمان‌هایی که به دنبال حفاظت از اطلاعات هستند نیز باید کنترل‌ها را در مورد سهامداران داخلی در نظر بگیرند، تعداد قابل‌توجهی از موارد نقض امنیت اطلاعات توسط پذیرش ضعیف امنیت سیستم‌های اطلاعات در میان کاربران، ایجاد شده است. سیستم امنیتی، به عنوان یک فرآیند مستمر، است سیستم امنیت اطلاعات را می توان، به صورت سیستم‌ها و روش‌هایی تعریف کرد که برای حفاظت از دارایی‌های اطلاعاتی سازمان، افشا به هر شخص یا نهادی که اجازه دسترسی به آن اطلاعات را نداشته باشد، فراهم می کند (هونگ و همکاران، ۲۰۱۷).

نقض امنیت سیستم‌های اطلاعات با ایجاد خسارات مالی (فنگ، وانگ، و لی، ۲۰۱۴)و آسیب اعتباری به سازمان‌های خصوصی، می گردد (ویلسون و وارکتین[8]، ۲۰۱۳).  در بخش عمومی، نقض امنیت سیستم‌های اطلاعات می‌تواند منجر به آسیب بیشتری به شهرت شود.مشکلات پیچیده مالی، سیاسی و اقتصادی را به همراه داشته باشدو از همه مهم‌تر از دست دادن اعتماد عمومی به دولت الکترونیک و سازمان‌های دولتی را به همراه داشته باشد که از دولت الکترونیک استفاده می‌کنند. از سوی دیگر، نبود یک

[5] abu-shanab
[6] avinash
[7] Zhao & Zhao
[8] Willison & Warkentin

ISSN: 2538-3671
http://www.johi.ir

سازمان مشخص در مورد مدیریت مسائل دولت الکترونیک و همچنین این واقعیت، که دولت‌های آتی ممکن است با توجه به سیاست‌های دولت الکترونیک، تصمیم‌گیری متفاوتی داشته باشند، عدم اطمینانی را در مورد پایداری دولت الکترونیکی را ایجاد کرده‌است (لارسون و گراندد[9]، ۲۰۱۶). با این شرایط، خطر درک شده از مشکلات امنیت سیستم‌های اطلاعات، سبب می شود که دولت ها، سیستم‌های خدمات دولت الکترونیک را کاهش دهند. .بر این اساس، امنیت سیستمهای اطلاعاتی پیشرفته و نوآوری در زمینه ی امنیت سیستمهای اطلاعاتی می تواند، اعتماد عمومی را در دولت الکترونیک افزایش داده و بنابراین مشروعیت و پایداری دولت الکترونیک را بهبود بخشند. با توجه به تغییرات مداوم در محیط داخلی و خارجی فعالیت های دولتی، برای دولت‌ها طبیعی است که به دنبال فرایندهای مدیریت پیشرفته امنیتی و نوآوری پیوسته امنیت اطلاعات باشند برای اطمینان از موفقیت دولت الکترونیک، نوآوری امنیت سیستمهای اطلاعاتی باید شامل بیش از تغییرات فنی باشد. (هونگ و همکاران، ۲۰۱۷). اثربخشی سیستم‌های امنیت اطلاعات را می توان تا حدی درک کرد که در آن اهداف و اهداف سازمان امنیت اطلاعات به خوبی محافظت می‌شوند، و معیارهای امنیتی (به عنوان مثال، روش‌ها، سیاست‌های امنیتی اطلاعات / رویه‌ها، معیارهای کنترل / ابزارها)به طور مداوم اعمال می‌شوند. در بررسی کارآیی این سیستم ها، باید عملکرد کلی سازمان رادر رابطه با امنیت اطلاعات مورد بررسی قرار داد. این شامل تلاش‌های مبتنی بر سازمان؛ و افزایش آگاهی بوده است. اثربخشی سیستم‌های امنیت اطلاعات به شیوه محتوای امنیتی در سیاست و چگونگی ارتباط آن با کاربران، بستگی دارد. علاوه بر این، اثربخشی را می توان با ماهیت سازمان، معیارهای امنیتی و پذیرش آن توسط کارمندان در عمل واقعی، تقویت کرد. اثربخشی سیستم‌های امنیتی تحت‌تاثیر عوامل سازمانی (کناپ و همکاران[10]، ۲۰۰۷)، معیارهای امنیتی (هاگن و همکاران[11]، ۲۰۰۸)و عوامل ترکیبی در نظر گرفت. ( چوی[12]، ۲۰۱۶). اگر چه عوامل سازمانی به عنوان مهم برای اثربخشی سیستم‌های امنیت سیستم‌های اطلاعات شناخته شده‌اند (هسو و همکاران[13]، ۲۰۱۲). تئوری سازمانی، رویکرد کل نگرانه تری را ارایه می‌دهد که عناصری چون تاثیرات سازمانی، عوامل سازمانی، فرآیندهای تصمیم‌گیری، و منطقه‌ای فنی را در نظر می‌گیرد.این رویکرد می‌تواند به طور دقیق‌تر محرک های امنیت اطلاعات در دولت الکترونیکی را توضیح دهد(هونگ و همکاران، ۲۰۱۷).

دولت الکترونیک به عنوان استفاده از اینترنت و شبکه جهانی برای ارائه اطلاعات و خدمات دولتی به شهروندان تعریف شده‌است.آن به دنبال بهبود شفافیت، رضایت شهروندان، کیفیت اطلاعات، تصمیم‌گیری و بهره‌وری است.همچنین قصد دارد بین دولت‌ها، شهروندان و سایر ذینفعان خدمات یکپارچه ارائه کند. ویر[14] (۲۰۱۰) نشان دادند که ویژگی‌های پیچیده دولت الکترونیک،(به عنوان مثال، موقعیت آن در میان عدم قطعیت‌های تکنولوژیکی و چالش مدیریت، منابع، و ساختارهای اجتماعی)می‌تواند انتشار نوآوری را تسهیل کند(هونگ و همکاران، ۲۰۱۷).

نمونه‌های مختلفی از سیستم‌های دولت الکترونیک وجود دارد.این موارد عبارتند از خدمات تدارکات عمومی برای تدارکات مرکزی (خدمات تدارکات عمومی، ۲۰۱۴)؛سیستم خدمات یک توقف برای صادرات و واردات کالا، که یک سرویس را برای تدارکات بندر فراهم می‌کند؛ خدمات مالیات خانگی، خدمات مالیاتی ملی (خدمات مالیات ملی، ۲۰۱۴)؛کیپوانت[15]، یک سیستم مدیریت ثبت اختراع آنلاین برای سیستم تدارک الکترونیک آنلاین و دولت برای شهروند، وب سایت رسمی پورتال دولتی برای خدمات مدنی است(دولت برای شهروندان، ۲۰۱۴). بسیاری از محققان پیشنهاد کرده‌اند که رفتار شهروندی سازمانی، رابطه مثبتی با اثربخشی سازمانی، بهره‌وری و موفقیت دارد. ین و همکاران[16] (۲۰۰۸) دریافتند که رفتار شهروندی سازمانی می‌تواند منجر به موفقیت در سیستم‌های اطلاعاتی شود (ین و همکاران، ۲۰۰۸). چوی و چویی[17] (۲۰۱۵) دریافتند که رفتار شهروندی سازمانی می‌تواند فرد را بهبود بخشد تا خود را با سیاست‌های امنیتی اطلاعات منطبق کند(چوئی و چوی، ۲۰۱۵).

رفتار شهروندی سازمانی، را به عنوان رفتاری فردی تعریف کرد که اختیاری است، نه وابسته به استفاده از پاداش‌ها و یا تنبیه برای تشویق عملکرد و اینکه در مجموع عملکرد موثر سازمان را ارتقا می‌دهد. کارمندانی که رفتار شهروندی سازمانی را نشان می‌دهند، تمایل بیشتری به پذیرش تغییرات دارند و راه‌حل‌هایی برای مشکلات به شیوه‌ای سازنده پیدا می‌کنند که به کل سازمان کمک می‌کند.مشارکت داوطلبانه کارمندان در تصمیم‌گیری شرکت، به کارمندان کمک می‌کند تا با یکدیگر همکاری

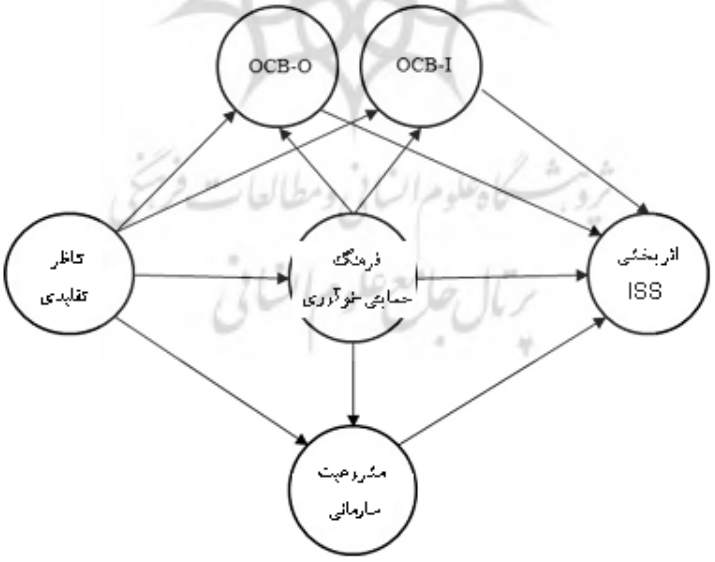
[9] Larsson, H., & Grönlund
[10] Knapp
[11] Hagen
[12] Choi
[13] Hsu
[14] Weare
[15] KIPOnet
[16] Yen
[17] Choi, M., & Choi

ISSN: 2538-3671
http://www.johi.ir

کنند، قدرت را در سازمان، به اشتراک بگذارند، در بین کارمندان تعامل وجود داشته باشند، و تعارض و خطرات سازمانی که اتفاق می افتد را تحمل کند. رفتار شهروندی سازمانی، می‌تواند تمایل سازمان‌ها و افراد را برای حل تعارض افزایش داده و خود را به کل سازمان متعلق بدانند، تا اینکه به صورت جداگانه یا برای گروه‌هایی، به دنبال منافع خود باشند (هونگ و همکاران، ۲۰۱۷).

کورکتو و گریفین ( ۲۰۱۸)، در بررسی رفتار ایمنی شهروندی سازمانی با توجه به نقش واسطه ای تعهد عاطفی و مالکیت روانی، نشان دادند رفتار شهروندی ایمنی سازمانی به طور عمده ای بر وابستگی عاطفی سازمان، تاثیر دارد و با ارتباطات درون سازمانی برای ارتقای ایمنی (مالکیت روانشناختی) نیز مرتبط است. هوانگ و چوی (۲۰۱۷)در بررسی تاثیرات فرهنگ حمایتی ـ نوآوری و رفتار شهروندی سازمانی بر امنیت سیستم اطلاعات دولت الکترونیک، نشان دادند، مناسب بودن فرهنگ حمایتی ـنوآوری ISS برای کارآیی و اثربخشی ISS در دولت لازم است. دولت هم باید تجلی های فرهنگی مصنوعات فرهنگی را تشخیص دهد تا به دست اندرکاران ISS کمک کند به فرمول بندی، اجرا و مدیریت استراتژیهای ISS بپردازند. لارسون و گرولند[18]( ۲۰۱۶) ماندگاری دولت الکترونیک را بررسی کردند. آنها واژه دولت الکترونیک و در سوئدرا مورد بررسی قرار دادند؛ آنها متوجه شده اند که فناوری بعنوان مشکلی برای دولت الکترونیک ادراک نشده است در حالیکه مباحث اقتصادی و اجتماعی را بعنوان مسئلهٔ اصلی ماندگاری دولت الکترونیک، استنباط می کنند.

مرور ادبیات بر روی دولت الکترونیک نشان می‌دهد که اثر متقابل بین عملکرد فنی، و جنبه‌های انسانی و اجتماعی (از جمله عوامل سازمانی، اجتماعی - اقتصادی و سازمانی)بر نوآوری، نفوذ دولت الکترونیک و موفقیت و شکست دولت الکترونیک تاثیر می‌گذارد. هر چند که موضوعات متنوعی با دیدگاه‌های مختلف مورد بررسی قرار گرفته‌اند برای اطمینان از موفقیت دولت الکترونیک، نوآوری ISS باید بیشتر از تغییرات فنی را دربر بگیرد. تحقیق حاضر، نوآوری ISS و مدیریت آن را صرفا یک نوآوری تکنولوژیک و مدیریت آن نمی داند بلکه آن را یک نوآوری اداری و سازمانی کلی نگر می داند. نوآوری ISS نه تنها نوآوری تکنولوژیک متمرکز بر توسعه و پیشرفتهایی در زمینهٔ فناوریهای امنیت اطلاعات را شامل می شود بلکه فلسفهٔ نوآوری اداری و اجرایی را هم شامل می شود که خود این دربر گیرندهٔ توسعهٔ برنامه های مدیریت امنیت، تغییرات فرهنگی، و تغییرات رفتاری در میان سهامداران است. نوآوری ISS همچنین دربر گیرندهٔ تثبیت انواع گوناگون فعالیتهای ISS روتین جدید است چرا که نوآوری به شکلی بالقوه می تواند روالهای متعددی را دربر بگیرد که به طرق مختلف قابل ترکیب شدن با یکدیگر هستند. در این تحقیق، با الگوپذیری از تحقیق هوآنگ و چوی (۲۰۱۷) به آزمون فرضیه ها پرداخته می شود.




**شکل۱**- مدل مفهومی تحقیق (هوانگ و چوی، ۲۰۱۷).

[18] Larsson & Gronlund

ISSN: 2538-3671
http://www.johi.ir

## فرضیه پژوهش

با توجه به مطالعات انجام شده، فرضیه های زیر مورد آزمون قرار گرفت:

فرضیه اصلی:

فرهنگ حمایت از نوآوری و رفتار شهروندی سازمانی در امنیت سیستم اطلاعات الکترونیکی در سازمان های دولتی تاثیر دارد.

فرضیه های فرعی:

H1 : تناظر تقلیدی در ارتباط با ISS، یک فرهنگ حمایتی ـ نوآور را برای ISS پیش بینی می کند.

H2 : تناظر تقلیدی در ارتباط با ISS، مشروعیت سازمانی ISS را پیش بینی می کند.

H3-a : تناظر تقلیدی در ارتباط با ISS، OCB-O را پیش بینی می کند.

H3-b : تناظر تقلیدی در ارتباط با ISS، OCB-I را پیش بینی می کند.

H4a : فرهنگ حمایتی ـ نوآوری، تاثیری مثبت بر OCB-O دارد.

H4b : فرهنگ حمایتی ـ نوآوری، تاثیری مثبت بر OCB-I دارد.

H5 : فرهنگ حمایتی ـ نوآوری، تاثیری مثبت بر مشروعیت سازمانی ISS دارد.

H6 : فرهنگ حمایتی ـ نوآوری، تاثیری مثبت بر کارآیی و اثربخشی ISS دارد.

H7 : مشروعیت سازمانی، تاثیری مثبت بر اثربخشی و کارآیی ISS دارد.

H8a : OCB-O تاثیری مثبت بر اثربخشی ISS دارد.

H8b : OCB-I تاثیری مثبت بر اثربخشی ISS دارد.

جامعه آماری تحقیق حاضر شامل کارکنان، مدیران میانی، مدیران سازمان فناوری اطلاعات و ارتباطات شهرداری تهران که در سال ۱۳۹۷-۱۳۹۶ مشغول به کار می‌باشد را شامل می‌شود. طبق آمار به دست آمده تعداد کل آنها حدود ۵۰۰ نفر بوده است. کل جامعه آماری در سازمان فناوری اطلاعات و ارتباطات شهرداری تهران، ۵۰۰ نفر هستند. بر اساس جدول مورگان، ۲۱۷ نفر، به صورت تصادفی انتخاب شده اند. ابزار گرآوری این تحقیق، پرسشنامه بوده است. پرسشنامه، بر اساس تحقیق هونگ و همکاران(۲۰۱۷) استخراج شده است. برای بخش میدانی نیز، تناظر تقلیدی را با استفاده از سه آیتم اقتباس شده از ابزار طراحی شده توسط هوگان و لندر[19] (۲۰۰۹)، اندازه گیری کرده ایم. فرهنگ نوآوری ـ حمایتی را با استفاده از پنج آیتم اقتباس شده از کار کویین و رورباق[20](۱۹۸۳) اندازه گیری کرده ایم. مشروعیت سازمانی را هم با استفاده از چهار آیتم برگرفته از کارهای لی و یون[21] (۲۰۱۱) و نیز یون و دی[22](۲۰۰۰) اندازه گیری کرده ایم. برای سنجش رفتار شهروندی فردی و رفتار شهروندی سازمانی، ما از ۱۲ آیتم بدست آمده از کارهای ویلیام و اندرسون[23] (۱۹۹۱) و نیز کویل- شاپیرو[24] (۲۰۰۲) استفاده کرد ایم. اثربخشی ISS را هم براساس مطالعات قبلی اندازه گیری شده است. برای سنجش کارآیی و اثربخشی ISS، ما از شش آیتم متعلق به تکمیل و اجرای سیاست امنیت اطلاعات و فاکتورهای دخیل در حفاظت از دارایی های اطلاعاتی، حفاظت از داده ها، خدمات اطلاعاتی، آگاهی، و سیستمهای سازمانی برای تشخیص نفوذ، استفاده کرده ایم . تمامی آیتمها در یک مقیاس لیکرت پنج امتیازی اندازه گیری شده اند که در آن ۱ به معنای قویا مخالف و ۵ به معنای قویا موافق است. برای آزمون فرضیه ها نیز از نرم افزار SMART.PLS استفاده شده است.

[19] Huegens & Lander
[20] Quinn & Rohrbaugh
[21] Lee & Yoon
[22] Yoon & Thye
[23] William & Anderson
[24] Coyle- Shapiro

ISSN: 2538-3671
http://www.johi.ir

## متغیرها و مدل پژوهش

### روایی و پایایی متغیرهای مدلهای تحقیق

از آنجایی که از پرسشنامه استاندارد برای سنجش متغیرها استفاده شده، ابتدا، شاخصهای مورد نظر ترجمه و سپس، با مراجعه به نخبگان اصلاحات لازم صورت گرفت. قدرت رابطه بین عامل (متغیر پنهان) و متغیر قابل‌مشاهده به‌وسیله بار عاملی نشان داده می‌شود. بار عاملی مقداری بین صفر و یک است. اگر بار عاملی کمتر از ۰/۳ باشد رابطه ضعیف در نظر گرفته شده و از آن صرف‌نظر می‌شود. بار عاملی بین ۰/۳ تا ۰/۶ قابل‌قبول است و اگر بزرگ‌تر از ۰/۶ باشد خیلی مطلوب است.( کلاین ۱۹۹۴ )در جدول (۱) می توان مشاهده کرد تمامی بارهای عاملی متغیرها مقداری بیشتر از ۰.۵ را دارا می باشند و مؤید این مطلب است که پایایی در مورد مدل اندازه‌گیری قابل‌قبول است.

**جدول ۱**- بارهای عاملی و متغیرهای تحقیق

| آماره تی | بار عاملی | جهت | آماره تی | بار عاملی | جهت |
|---|---|---|---|---|---|
| 13.649 | 0.688 | رفتار فردی ← q16 | 32.916 | 0.827 | تناظر تقلیدی ← q01 |
| 32.247 | 0.848 | رفتار فردی ← q17 | 24.917 | 0.809 | تناظر تقلیدی ← q02 |
| 16.559 | 0.778 | رفتار فردی ← q18 | 26.877 | 0.799 | تناظر تقلیدی ← q03 |
| 21.536 | 0.752 | رفتار سازمانی ← q19 | 12.023 | 0.692 | فرهنگ نوآوری ← q04 |
| 19.105 | 0.782 | رفتار سازمانی ← q20 | 24.112 | 0.813 | فرهنگ نوآوری ← q05 |
| 24.762 | 0.801 | رفتار سازمانی ← q21 | 28.283 | 0.798 | فرهنگ نوآوری ← q06 |
| 17.027 | 0.71 | رفتار سازمانی ← q22 | 10.224 | 0.672 | فرهنگ نوآوری ← q07 |
| 16.972 | 0.728 | رفتار سازمانی ← q23 | 9.42 | 0.607 | فرهنگ نوآوری ← q08 |
| 18.565 | 0.759 | رفتار سازمانی ← q24 | 19.513 | 0.757 | مشروعیت سازمانی ← q09 |
| 16.632 | 0.698 | اثربخشی و کارایی ← q25 | 32.592 | 0.852 | مشروعیت سازمانی ← q10 |
| 49.049 | 0.855 | اثربخشی و کارایی ← q26 | 32.411 | 0.844 | مشروعیت سازمانی ← q11 |
| 33.397 | 0.793 | اثربخشی و کارایی ← q27 | 31.534 | 0.801 | مشروعیت سازمانی ← q12 |
| 30.051 | 0.798 | اثربخشی و کارایی ← q28 | 31.959 | 0.852 | رفتار فردی ← q13 |
| 18.353 | 0.756 | اثربخشی و کارایی ← q29 | 19.056 | 0.721 | رفتار فردی ← q14 |
| 28.447 | 0.772 | اثربخشی و کارایی ← q30 | 19.06 | 0.723 | رفتار فردی ← q15 |

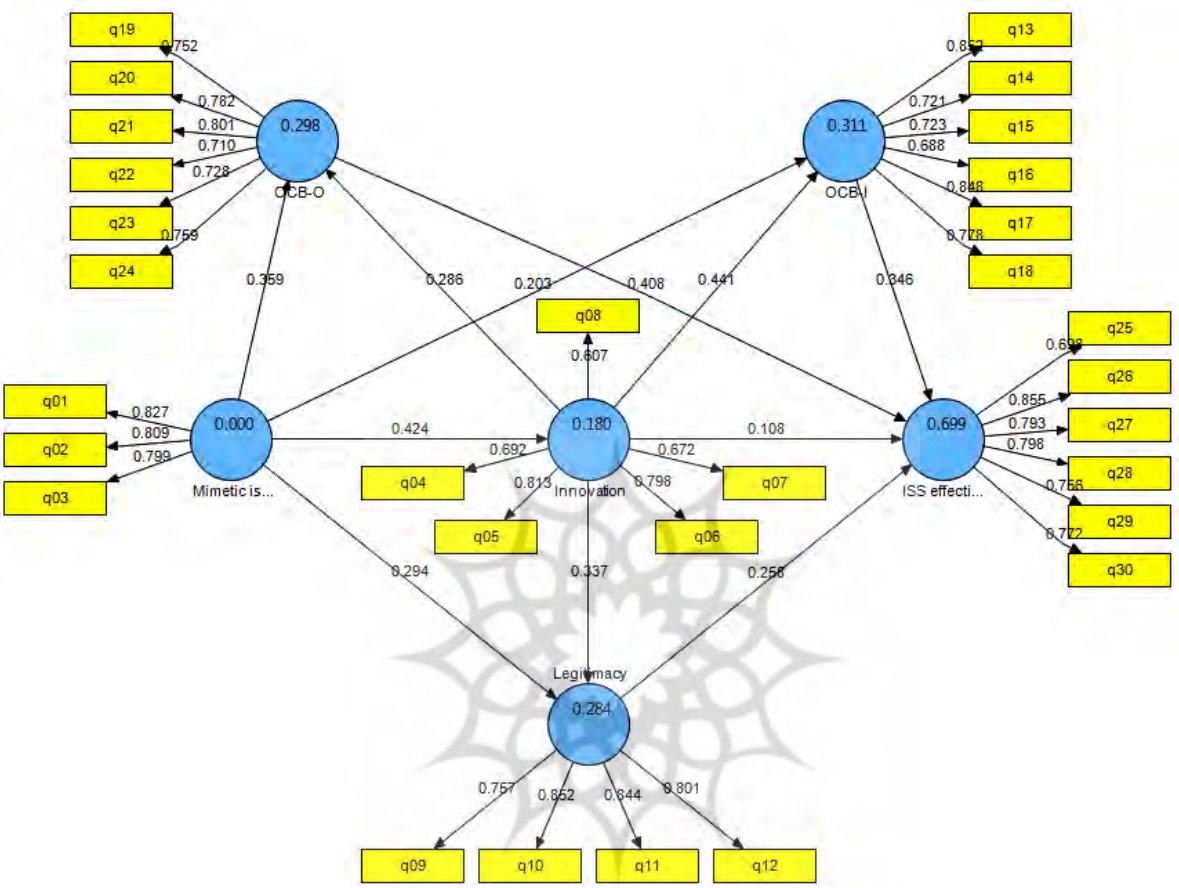
سپس، پایایی متغیرهای تحقیق توسط شاخصهای آلفای کرونباخ با میزان استاندارد بالای ۰.۷ (کرونباخ،۱۹۵۱) و پایایی ترکیبی (CR) با میزان استاندارد بالای ۰.۷ و میانگین واریانس توسعه یافته (AVE) با میزان استاندار بالای ۰.۵ (فورنل و لاکر، ۱۹۸۱) با استفاده از نرم افزار Smart-PLS بررسی شد. نتایج نشان داد آلفای کرونباخ تمامی متغیرها بزرگ‌تر از ۰/۷ بوده بنابراین ازنظر پایایی تمامی متغیرها مورد تائید است. مقدار میانگین واریانس استخراج‌شده (AVE) همواره بزرگ‌تر از ۰/۵ است بنابراین روایی همگرا نیز تائید می‌شود.

در قسمت روایی واگرا، میزان تفاوت بین شاخص‌های یک سازه با شاخص‌های سازه‌های دیگر در مدل مقایسه می‌شود. این کار از طریق مقایسه جذر AVE هر سازه با مقادیر ضرایب همبستگی بین سازه‌ها محاسبه می‌گردد. برای این کار یک ماتریس باید تشکیل داد که مقادیر قطر اصلی ماتریس جذر ضرایب AVE هر سازه هست و مقادیر پایین و بالای قطر اصلی، ضرایب همبستگی بین هر سازه با سازه‌های دیگر است. نتایج نشان داد، جذر AVE هر سازه از ضرایب همبستگی آن سازه با سازه‌های دیگر بیشتر شده است که این مطلب حاکی از قابل‌قبول بودن روایی واگرای سازه‌ها است.

ISSN: 2538-3671
http://www.johi.ir

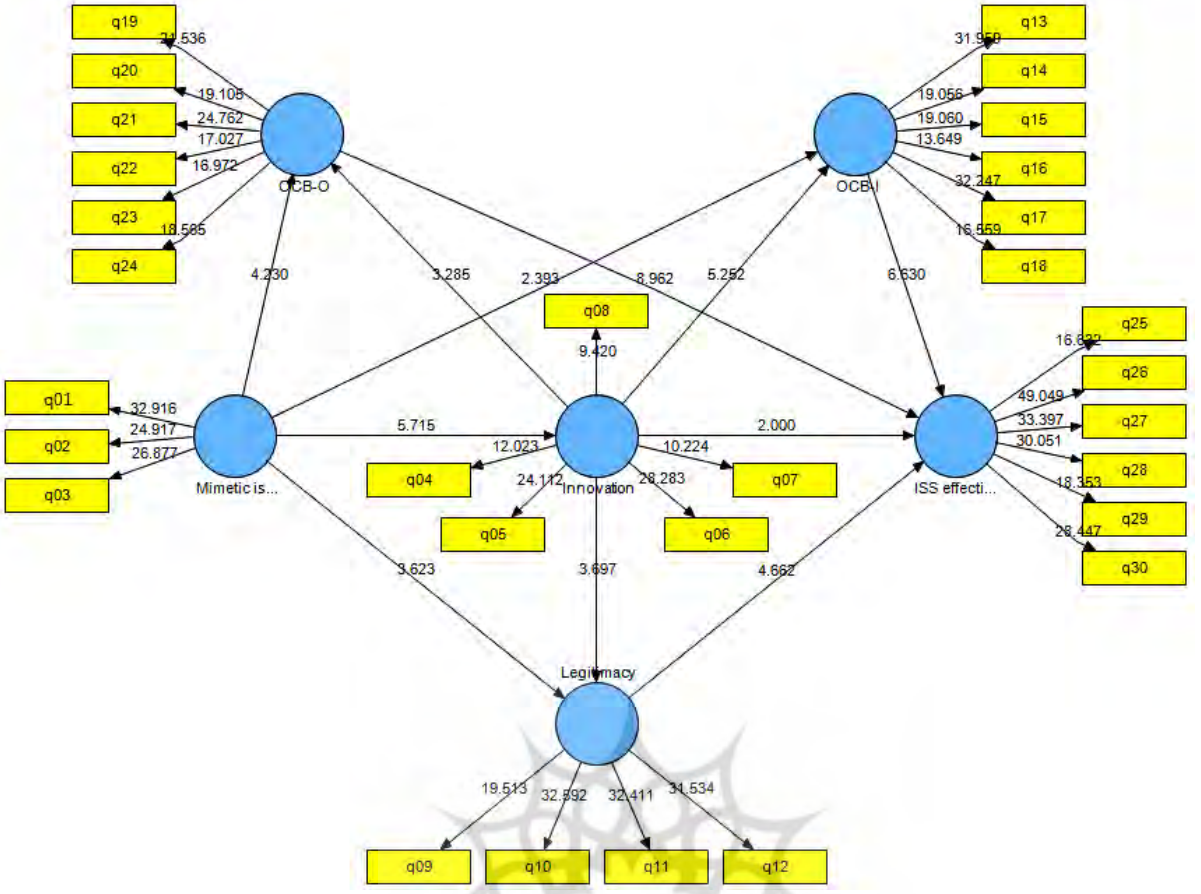
## یافته های پژوهش

رابطه متغیرهای موردبررسی در هر یک از فرضیه های تحقیق بر اساس یک ساختار علی با تکنیک حداقل مربعات جزئی PLS آزمون شده است. در مدل کلی تحقیق که در شکل (۲) ترسیم‌شده است مدل اندازه‌گیری (رابطه هریک از متغیرهای قابل‌مشاهده به متغیر پنهان) و مدل مسیر (روابط متغیرهای پنهان با یکدیگر) محاسبه شده است. برای سنجش معناداری روابط نیز آماره t با تکنیک بوت استراپینگ محاسبه شده است که در شکل (۳) ارائه‌شده است.




**شکل ۲**- تکنیک حداقل مربعات جزئی مدل کلی پژوهش

ISSN: 2538-3671
http://www.johi.ir




**شکل ۳**- آماره تی مدل کلی پژوهش با تکنیک بوت استراپینگ

فرضیه فرعی اول: تناظر تقلیدی در ارتباط با ISS، یک فرهنگ حمایتی ـ نوآور را برای ISS پیش بینی می کند.

مشاهده می گردد شدت اثر تناظر تقلیدی بر فرهنگ حمایتی ـ نوآور برابر ۰/۴۲۴ محاسبه شده است و آماره احتمال آزمون نیز ۵/۷۱۵ به‌دست‌آمده است که بزرگ‌تر از مقدار بحرانی t در سطح خطای ۵٪ یعنی ۱/۹۶ بوده و نشان می‌دهد تأثیر مشاهده‌شده معنادار است.

فرضیه فرعی دوم: تناظر تقلیدی در ارتباط با ISS، مشروعیت سازمانی ISS را پیش بینی می کند

مشاهده می‌گردد شدت اثر کل تناظر تقلیدی بر مشروعیت سازمانی برابر ۰/۴۳۷ به دست آمده است و مقدار معناداری برابر ۶/۱۸۶ محاسبه شده است که بزرگ‌تر از مقدار بحرانی t در سطح خطای ۵٪ یعنی ۱/۹۶ بوده و نشان می‌دهد تاثیر مشاهده‌شده معنادار است.

فرضیه فرعی سوم: تناظر تقلیدی در ارتباط با ISS، رفتار شهروندی سازمانی را پیش بینی می کند.

شدت اثر کل تناظر تقلیدی بر رفتار شهروندی سازمانی برابر ۰/۴۸۱ محاسبه شده است و آماره احتمال آزمون نیز ۶/۸۰۸ به‌دست‌آمده است که بزرگ‌تر از مقدار بحرانی t در سطح خطای ۵٪ یعنی ۱/۹۶ بوده و نشان می‌دهد تأثیر مشاهده‌شده معنادار است،

فرضیه فرعی چهارم: تناظر تقلیدی در ارتباط با ISS، رفتار شهروندی فردی را پیش بینی می کند.

شدت اثر کل تناظر تقلیدی بر رفتار شهروندی فردی برابر ۰/۳۹۰ محاسبه شده است و آماره احتمال آزمون نیز ۵/۰۴۶ به‌دست‌آمده است که بزرگ‌تر از مقدار بحرانی t در سطح خطای ۵٪ یعنی ۱/۹۶ بوده و نشان می‌دهد تأثیر مشاهده‌شده معنادار است.

فرضیه فرعی پنجم: فرهنگ حمایتی ـ نوآوری، تاثیری مثبت بر رفتار شهروندی سازمانی دارد.

شدت اثر کل فرهنگ حمایتی ـ نوآوری بر رفتار شهروندی سازمانی برابر ۰/۲۸۶ محاسبه شده است و آماره احتمال آزمون نیز ۳/۲۸۵ به‌دست‌آمده است که بزرگ‌تر از مقدار بحرانی t در سطح خطای ۵٪ یعنی ۱/۹۶ بوده و نشان می‌دهد تأثیر مشاهده‌شده معنادار است، فرضیه فرعی پنجم تایید می گردد.

ISSN: 2538-3671
http://www.johi.ir

فرضیه فرعی ششم: فرهنگ حمایتی ـ نوآوری، تاثیری مثبت بر رفتار شهروندی فردی دارد.
شدت اثر کل فرهنگ حمایتی ـ نوآوری بر رفتار شهروندی فردی برابر ۰/۴۴۱ محاسبه شده است و آماره احتمال آزمون نیز ۵/۲۵۲ به‌دست‌آمده است که بزرگ‌تر از مقدار بحرانی t در سطح خطای ۵٪ یعنی ۱/۹۶ بوده و نشان می‌دهد تأثیر مشاهده‌شده معنادار است.
فرضیه فرعی هفتم: فرهنگ حمایتی ـ نوآوری، تاثیری مثبت بر مشروعیت سازمانی ISS دارد.
شدت اثر کل فرهنگ حمایتی ـ نوآوری بر مشروعیت سازمانی برابر ۰/۳۳۷ محاسبه شده است و آماره احتمال آزمون نیز ۶/۶۹۷ به‌دست‌آمده است که بزرگ‌تر از مقدار بحرانی t در سطح خطای ۵٪ یعنی ۱/۹۶ بوده و نشان می‌دهد تأثیر مشاهده‌شده معنادار است.
فرضیه فرعی هشتم: فرهنگ حمایتی ـ نوآوری، تاثیری مثبت بر کارآیی و اثربخشی ISS دارد.
شدت اثر کل فرهنگ حمایتی ـ نوآوری بر کارآیی و اثربخشی برابر ۰/۴۶۴ محاسبه شده است و آماره احتمال آزمون نیز ۶/۷۷۰ به‌دست‌آمده است که بزرگ‌تر از مقدار بحرانی t در سطح خطای ۵٪ یعنی ۱/۹۶ بوده و نشان می‌دهد تأثیر مشاهده‌شده معنادار است.
فرضیه فرعی نهم: مشروعیت سازمانی، تاثیری مثبت بر کارآیی و اثربخشی ISS دارد.
شدت اثر کل مشروعیت سازمانی بر کارآیی و اثربخشی برابر ۰/۲۵۸ محاسبه شده است و آماره احتمال آزمون نیز ۴/۶۶۲ به‌دست‌آمده است که بزرگ‌تر از مقدار بحرانی t در سطح خطای ۵٪ یعنی ۱/۹۶ بوده و نشان می‌دهد تأثیر مشاهده‌شده معنادار است، بنابراین با اطمینان ۹۵٪ مشروعیت سازمانی بر کارآیی و اثربخشی تاثیر مثبت و معناداری دارد و فرضیه فرعی نهم تایید می گردد.
فرضیه فرعی دهم: رفتار شهروندی سازمانی، تاثیری مثبت بر کارآیی و اثربخشی ISS دارد.
شدت اثر کل رفتار شهروندی سازمانی بر کارآیی و اثربخشی برابر ۰/۴۰۸ محاسبه شده است و آماره احتمال آزمون نیز ۸/۹۶۲ به‌دست‌آمده است که بزرگ‌تر از مقدار بحرانی t در سطح خطای ۵٪ یعنی ۱/۹۶ بوده و نشان می‌دهد تأثیر مشاهده‌شده معنادار است، بنابراین با اطمینان ۹۵٪ رفتار شهروندی سازمانی بر کارآیی و اثربخشی تاثیر مثبت و معناداری دارد و فرضیه فرعی دهم تایید می گردد.
فرضیه فرعی یازدهم: رفتار شهروندی فردی، تاثیری مثبت بر کارآیی و اثربخشی ISS دارد.
شدت اثر کل رفتار شهروندی فردی بر کارآیی و اثربخشی برابر ۰/۳۴۶ محاسبه شده است و آماره احتمال آزمون نیز ۶/۶۳۰ به‌دست‌آمده است که بزرگ‌تر از مقدار بحرانی t در سطح خطای ۵٪ یعنی ۱/۹۶ بوده و نشان می‌دهد تأثیر مشاهده‌شده معنادار است، بنابراین با اطمینان ۹۵٪ رفتار شهروندی فردی بر کارآیی و اثربخشی تاثیر مثبت و معناداری دارد و فرضیه فرعی یازدهم تایید می گردد.
فرضیه اصلی: فرهنگ حمایت از نوآوری و رفتار شهروندی سازمانی در امنیت سیستم اطلاعات الکترونیکی در سازمان های دولتی (مطالعه موردی سازمان فناوری اطلاعات و ارتباطات شهرداری تهران)، تاثیر دارد.
با توجه به تایید نتایج فرضیات فرعی نهم و یازدهم و دوازدهم مبنی بر تاثیر فرهنگ حمایت از نوآوری و رفتار شهروندی سازمانی و رفتار شهروندی فردی بر کارایی و اثربخشی امنیت سیستم اطلاعات الکترونیکی، در مجموع می توان نتیجه گرفت فرضیه اصلی تحقیق در بازه احتمالی معنادار است وهمچنین نیز مورد تایید است .

ISSN: 2538-3671
http://www.johi.ir

## نتیجه‌گیری

برای اطمینان از اثربخشی سیستم‌های امنیتی، اقدامات امنیتی و رفتارهای سازمانی ضروری و وابسته به یکدیگر هستند.از دیدگاه رفتار سازمانی، عواملی مانند آموزش کاربر، فرهنگ امنیتی، ارتباط سیاسی، اجرای سیاست. اگر چه عوامل سازمانی به عنوان مهم برای اثربخشی امنیت سیستم‌های اطلاعات شناخته شده‌اند تئوری سازمانی، رویکرد کل نگرانه تری را ارایه می‌دهد که عناصری چون تاثیرات سازمانی، عوامل سازمانی، فرآیندهای تصمیم‌گیری، و منطقه‌ای فنی را در نظر می‌گیرد.این رویکرد می‌تواند به طور دقیق‌تر محرک های امنیت اطلاعات در دولت الکترونیکی را توضیح دهد. مرور ادبیات بر روی دولت الکترونیک نشان می‌دهد که اثر متقابل بین عملکرد فنی، و جنبه‌های انسانی و اجتماعی (از جمله عوامل سازمانی، اجتماعی - اقتصادی و سازمانی)بر نوآوری، نفوذ دولت الکترونیک و موفقیت و شکست دولت الکترونیک تاثیر می‌گذارد.هر چند که موضوعات متنوعی با دیدگاه‌های مختلف مورد بررسی قرار گرفته‌اند.با این حال، یلدز (۲۰۰۷)نشان داد که ادبیات دولت الکترونیک هنوز هم محدود است، به عنوان مثال، تمرکز بیش از حد بر روی تحقیقات نتیجه محور، نبود تحقیق مبتنی بر فرآیند دولت، و عدم درک محیط‌های پیچیده سیاسی و سازمانی که در آن فرایندهای تصمیم‌گیری و توسعه دولت الکترونیک رخ می‌دهد، انجام شده است.ادریس و همکاران (۲۰۰۹) نیز نشان دادند که چگونه ارزش‌های فرهنگی ملی بر آمادگی دولت الکترونیک تاثیر می‌گذارند و اینکه چگونه پویایی سیستم را می توان برای درک پدیده‌های پیچیده دولت الکترونیک مورد بررسی قرار داد. شکوه (۱۳۹۳) نشان داد دولت الکترونیک ضمن مهیا نمودن شرایط لازم برای ارتقا سطح فضای کاری، زمینه دسترسی آسان به خدمات دولتی را فراهم می نماید. ملارضامحرم خیاط مقدم (۱۳۹۶) نشان دادند که رفتار شهروندی به همراه کلیه مولفه هایش، رابطه سیستم های اطلاعاتی مبتنی بر وب و ایجاد جو نوآوری در آموزشگاهای آزاد فن آوری اطلاعات مشهد را تعدیل گری نمی کند ایفوندو (۲۰۱۴) بیان کردند که تغییری در چارچوب تحقیقات به سمت رویکردهای اجتماعی ـ سازمانی و به سمت تئوری نهادی بعنوان چارچوبی برای تشریح دولت الکترونیک و انتشار ISS، پدید آمده است هوگان و کوته (۲۰۱۳) نشان دادند که لایه های فرهنگی مورد آزمون نقش تعیین کننده ایی در ترویج نوآوری سازمانی دارند. یانگ و وو (۲۰۱۶) نشان دادند تسهیل شرایط و قابلیت سازمانی، دو عامل است که قوی ترین اثر مثبت را دارد. طبق سودمندی درک شده، نفوذ خارجی و فرهنگ سازمانی تأثیرات مثبت دارند، در حالی که خطرات درک شده در واقع تاثیر منفی بر روی هدف دارند. برعکس، تلاش درک شده و منافع درک شده تاثیر ناچیزی دارند هوانگ و چوی (۲۰۱۷) نشان دادند فرهنگ حمایتی ـنوآوری ISS برای کارآیی و اثربخشی ISS در دولت می باشند، دولت هم باید تجلی های فرهنگی مصنوعات فرهنگی را تشخیص دهد تا به دست اندرکاران ISS کمک کند به فرمول بندی، اجرا و مدیریت استراتژیهای ISS بپردازند کورکتو و گریفین ( ۲۰۱۸)، نشان دادند رفتار شهروندی ایمنی سازمانی به طور عمده ای بر وابستگی عاطفی سازمان، تاثیر دارد و با ارتباطات درون سازمانی برای ارتقای ایمنی (مالکیت روانشناختی) نیز مرتبط است. ویر[۲۵] (۲۰۱۰) نشان دادند که ویژگی‌های پیچیده دولت الکترونیک (به عنوان مثال، موقعیت آن در میان عدم قطعیت‌های تکنولوژیکی و چالش مدیریت، منابع، و ساختارهای اجتماعی)می‌تواند انتشار نوآوری را تسهیل کند نوریس و کروسی (۲۰۰۸)، نشان داد مباحث امنیت اطلاعات، موانعی جدی بر سر راه دولت الکترونیک هستند و اکثر دولتها باید همواره به نوآوری در خصوص امنیت سیستم های اطلاعاتی (ISS) بپردازند.امنیت سیستم‌های اطلاعات به عنوان یک عامل موفقیت و مانعی برای دولت الکترونیک شناخته شده‌است.امنیت اطلاعات برای دموکراسی الکترونیک، امنیت سیستم برای رایانش ابری و امنیت تبادل را شامل می شود. با این حال، تحقیقات در مورد امنیت سیستم‌های اطلاعات در دولت الکترونیک توجه کمتری به امنیت افراد داخلی سازمان مبذول داشته اند. بانوز۲۶ (۲۰۱۴) نشان داد که با اتکا به تکنولوژی اطلاعات امنیت سیستم‌های اطلاعاتی، نمی‌توان عملکرد کامل امنیت سیستم‌های اطلاعات را تضمین کند.این پرونده شامل نقض امنیتی در بخشی از افراد داخلی و هک کردن گروه‌های مخالف بوده است.این مساله پیچیدگی مورد نظر را در رابطه با اعضای سازمان، خارج از حملات سایبری و مسایل سیاسی آشکار می‌سازد. لارسون و همکارن (۲۰۱۶) نیز بیان کردندامنیت سیستمهای اطلاعاتی پیشرفته و نوآوری امنیت سیستمهای اطلاعاتی مداوم، اعتماد عمومی را در دولت الکترونیک افزایش داده و بنابراین مشروعیت و پایداری دولت الکترونیک را بهبود بخشند.

دولت الکترونیک حاصل بکارگیری فناوری اطلاعات و ارتباطات جهت ارایه خدمات به بخش عمومی است. بنابراین تاثیر دولت الکترونیک برای رفع فاصله میان صدای مردم و پاسخگویی دولت آشکار است. سان و همکاران[۲۷] (۲۰۱۵) نیز بیان کردند که دولت الکترونیک نیازمند اعتماد عمومی است، و امنیت سیستم‌های اطلاعات یک نگرانی اصلی در این زمینه است. بنابراین، برای

[25] Weare
[26] Boannews
[27] Sun

ISSN: 2538-3671
http://www.johi.ir

سیاست‌ها و پیاده‌سازی مناسب امنیت اطلاعات، نیاز به افزایش اعتماد عمومی به دولت الکترونیک وجود دارد.از این رو، تناظر تقلیدی در رابطه با نوآوری ISS ، می تواند مشروعیت دولت الکترونیکی و سازمان‌هایی که از دولت الکترونیک استفاده می‌کنند، فراهم کند. هونگ و همکاران (۲۰۱۷) نیز در مطالعه ی تجربی خود، استدلال کردند که چشم انداز اجتماعی ـ سازمانی مبتنی بر الگوی تفسیری باید برای دستیابی به کارآیی و اثربخشی ISS مهم باشد. با این حال اخیرا تئوری نهادی بعنوان چارچوب نظری و برای بررسی سیستمهای اطلاعاتی و IT بکار گرفته شده است. یک ریسک استنباط شده و ادراک شدهٔ مسائل ISS می تواند دولتها را وادار به کاهش خدمات و سیستمهای دولت الکترونیک نماید. دولت الکترونیک به عنوان یکی از زیرمجموعه های فناوری اطلاعات، دولت ها را قادر می سازد تا اطلاعات و خدمات را به طور موثر در حداقل زمان و هزینه ارایه دهند. دولت الکترونیک به کار گیری فناوری اطلاعات برای طراحی مجدد فرایند های کاری به منظور ارایه خدمات دولتی به صورت بهینه و همچنین تسهیل تعامل با دولت است. پیاده سازی و گسترش دولت الکترونیک اغلب به منظور ایجاد برخی تغییرات در فرآیندهای دولتی مانند عدم تمرکز و بهبود کارایی است.

**پیشنهادات تحقیق و پژوهش**

با توجه به نتایج حاصل از تحقیق، پیشنهادات زیر ارائه می‌گردد:

مدیران سازمان باید برای اجرایی کردن و استقرار دولت الکترونیک، بودجه به موقع را برای این امر تخصیص دهند و بر روند اجرای بودجه نظارت کافی بعمل آید .

با توجه به اینکه نیروی انسانی نقش تعیین کننده ایی در اجرایی کردن دولت الکترونیک در سازمان دارد، پیشنهاد می گردد آموزش های مناسب و لازم برای افراد در نظر گرفته شود.

برای این منظور بهتر است، حمایت های کافی از سوی سازمان مجری اعمال شود و رویه ها و سیاست های لازم برای اجرایی کردن دولت الکترونیک، ارائه گردد.

پیشنهاد می گردد تا مباحث فنی مربوط به حوزه امنیت اطلاعات ، امنیت سیستم های کامپیوتری ، شبکه ، نرم افزار ها ، سخت افزار ها مطابق با پیشرفت تکنولوژی بروزرسانی و حمایت گردد .

پیشنهاد می گردد منابع مالی کافی باید برای اجرایی کردن دولت الکترونیک در سازمان، تخصیص داده شود، تا بتوان شرایط اجرایی کردن دولت الکترونیک، تسهیل گردد.

به مدیران پیشنهاد می شود که در سازمان سیستم پاداش پرورش دهندهٔ رفتارخلاق، اجرایی شود تا با توسعه و حمایت از نوآوری، منجر به پذیرش بیشتر دولت الکترونیک شوند.

ISSN: 2538-3671
http://www.johi.ir

## منابع و مراجع

- Avinash Ramtohul , K.M.S. Soyjaudah , (2016) "Information security governance for e-services in southern African developing countries e-Government projects", Journal of Science & Technology Policy Management, Vol. 7 Iss: 1, pp.26 – 42.
- Choi, M., & Choi, H. (2015). A study on neutralization and organizational citizenship behavior for information security policy compliance. Information Systems Review, 17(3), 65–76.
- Choi,M. (2016). Leadership of information securitymanager on the effectiveness of information systems security for secure sustainable computing. Sustainability, 8(7), 1–21.
- Coursey, D., & Norris, D. F. (2008). Models of e-government: Are they correct? An empirical assessment. Public Administration Review, 68(3), 523–536.
- Eom, S. (2012). Institutional dimensions of e-government development: Implementing the business reference model in the United States and Korea. Administration and Society, 45(7), 875–907.
- Feng, N.,Wang, H. J., & Li, M. Q. (2014). A security risk analysismodel for information systems: Causal relationships of risk factors and vulnerability propagation analysis. Information Sciences, 256, 57–73.
- G4C: Government for Citizen, 2014, December 4. (Retrieved from: bhttp://www.egov.go. krN).
- Hagen, J.M., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. Information Management & Security, 16(4), 377–397.
- Hsu, C., Lee, J. N., & Straub, D. W. (2012). Institutional influences on information systems security innovations. Information Systems Research, 23(3), 918–939.
- Hwang Kumju, Choi Myeonggil.(2017).Effects of innovation-supportive culture and organizational citizenship behavior on e-government information system security stemming from mimetic isomorphism, Government Information Quarterly xxx (2017) xxx–xxx.
- Jun, K., & Weare, C. (2010). Institutional motivations in the adoption of innovations: The case of e-government. Journal of Public Administration Research and Theory, 21(3), 495–519.
- Knapp, K. J., Marshall, T. E., Rainer, R. K., Jr., & Ford, F. N. (2007). Information security effectiveness: Conceptualization and validation of a theory. International Journal of Information Security and Privacy, 1(2), 37–6.
- Larsson, H., & Grönlund, Å. (2016). Sustainable eGovernance? Practices, problems and beliefs about the future in Swedish eGov practice. Government Information Quarterly, 33(1), 105–114.
- Lee, S., & Yoon, J. (2011). The effects of corporate social responsibility. Korean Management Review, 40(4), 919–954.
- Sharma.Sujeet Kumar, (2015),"Adoption of e-government services", Transforming Government: People, Process and Policy, Vol. 9 Iss 2 pp. 207 – 222.
- William, L. J., & Anderson, S. E. (1991). Job satisfaction and organizational commitment as predictors of organizational citizenship and in-role behaviors. Journal ofManagement, 17(3), 601–617.
- Yen, H. R., Li, E., & Niehoff, B. P. (2008). Do organizational citizenship behaviors lead to information system success? Testing the mediation effects of integration climate and project management. Information Management, 45, 394–402.
- Yoon, C. (2009). The effects of organizational citizenship behaviors on ERP system - success. Computers in Human Behavior, 25, 421–428.
- Zhao, J. J., & Zhao, S. Y. (2010). Opportunities and threats: A security assessment of state egovernment website. Government Information Quarterly, 27(1), 49–56.