نشریه علمی مطالعات مدیریت کسب و کار هوشمند- سال هشتم ـ شماره ۳۲ـ تابستان ۱۳۹۹
مقاله پژوهشی/ صفحات ۱۸۰- ۱۴۷
Doi: 10.22054/IMS.2020.44465.1581

اثربخشی امنیت سیستم‌های اطلاعاتی، ناشی از تأثیر ابعاد تئوری نهادی بر رفتار سازمانی کارکنان

سید امین حسینی سنو*
نگار کدخدا**

چکیده

این پژوهش به امنیت سیستم‌های اطلاعاتی (ISS) به‌عنوان یکی از مهم‌ترین مسائل در سازمان‌ها و بخصوص شهرداری‌ها پرداخته است. امروزه نقض‌های امنیت اطلاعات به‌جای استثنا، تبدیل به هنجار شده است و امنیت سیستم اطلاعات تنها زمانی می‌تواند محقق شود که کارکنان به‌طور کامل این مفهوم را از طریق تغییر رفتار خود در مطابقت با فن‌آوری‌های پیشرفته امنیت سیستم اطلاعات بپذیرند. مدل این تحقیق در همین راستا بر مبنای تئوری نهادی ایجاد شده است. این مدل دو مسیر شامل رفتارهای شهروندی سازمانی (OCB) و رفتار ضد شهروند سازمانی (CWB) را در فرآیند بدعت‌گذاری امنیت سیستم اطلاعاتی معرفی کرده است. این پژوهش همچنین تأثیر فرهنگ نوآورانه را بر فرآیند امنیت سیستم اطلاعات مورد سنجش قرار داده است. جامعه آماری پژوهش شامل کارشناسان فناوری اطلاعات شهرداری مشهد است و ابزار جمع‌آوری داده پرسشنامه بوده است. داده‌ها عمدتاً از مدل تحقیق پیشنهادی پشتیبانی می‌کنند و نتایج حاکی از کاربرد تئوری نهادی در توضیح اثرگذاری فرآیند نهادینه‌سازی تغییرات امنیت سیستم اطلاعات بر فرهنگ نوآورانه سازمان، مشروعیت و پذیرش آن تغییرات و افزایش رفتار شهروندی سازمانی (کاهش رفتار ضد شهروندی) در کارکنان می‌شود؛ که این فرآیند در نهایت منجر به افزایش اثربخشی امنیت سیستم اطلاعات می‌شود.

کلیدواژگان: امنیت سیستم‌های اطلاعات، شهرداری، مشروعیت، بدبینی سازمانی، فرهنگ نوآورانه، رفتار شهروندی سازمانی، رفتار ضد شهروندی، اثربخشی امنیت سیستم‌های اطلاعاتی.

---

* عضو هیئت‌علمی، گروه مهندسی کامپیوتر، دانشگاه فردوسی مشهد، مشهد، ایران. (نویسنده مسئول)؛hosseini@um.ac.ir
** دانشجوی دکتری مدیریت فناوری اطلاعات، دانشگاه فردوسی مشهد، مشهد، ایران

تاریخ دریافت:۱۳۹۸/۰۶/۱۵ **تاریخ پذیرش:۱۳۹۸/۱۰/۳۰**

مقدمه

در جامعه جهانی، عصر حاضر را عصر اطلاعات و دانش می‌نامند و انبوه اطلاعات موجود در شبکه‌هایی نظیر اینترنت منجر به ایجاد جامعه نوینی به نام جامعه اطلاعاتی گشته است. مطابق سند چشم‌انداز ۲۰ ساله، جمهوری اسلامی ایران می‌بایستی تا سال ۱۴۰۴ به جایگاه اول علمی، اقتصادی و فناوری در سطح منطقه دست یابد و به کشوری توسعه‌یافته مبدل شود (مجمع تشخیص مصلحت نظام، ۱۳۸۲). در عصر حاضر، کشوری می‌تواند به توسعه پایدار و همه‌جانبه دست یابد که مردم آن کشور در مسیر رشد بلوغ فکری گام بردارند و این امر تنها از طریق آسان‌سازی در دسترسی و تسهیم دانش و اطلاعات میسر خواهد شد و از همین رو ضرورت توجه به فناوری اطلاعات بشدت احساس می‌گردد تا با استفاده از توانمندی‌های آن، زندگی شهروندان تسهیل گردد و اهداف عالیه کشور نیز محقق گردد. با پدیدار شدن شبکه‌ها و دسترسی آسان به اینترنت، قسمت عظیمی از اطلاعات از طریق این بستر در حال پردازش و انتقال است و همچنین بیشتر اطلاعات به‌صورت دیجیتالی بازیابی و ذخیره شده و با سرعت بیشتری در حال تکثیر است. به‌موازات این پیشرفت‌ها تهدیدات و تخریب و سرقت اطلاعات نیز افزایش یافته به‌طوری‌که حفاظت و امنیت اطلاعات به یکی از مهم‌ترین مسائل در عصر حاضر تبدیل شده است (وظیفه و همکاران، ۱۳۹۷).

بسیاری از مراکز و مؤسسات دولتی و خصوصی، بانک‌ها، شرکت‌ها و ادارات، مراکز آموزشی، پژوهشی، تبلیغی و اطلاع‌رسانی، در انجام وظایف و مأموریت‌های خود، از سیستم‌های جامع اطلاعاتی و فناوری اطلاعات در سازمان‌های خود بهره‌برداری می‌کنند که علت این امر، امتیازات و امکانات فراوان آن؛ از قبیل سهولت انتقال اطلاعات، سرعت انتقال اطلاعات، ذخیره‌سازی حجم گسترده‌ی اطلاعات، کاهش هزینه‌ها، صرفه‌جویی در وقت، قابلیت اعتماد و دقت در انجام کار است (توربان و همکاران[1]، ۲۰۱۸). اگر اخبار و اطلاعات در حوزه فناوری اطلاعات و ارتباطات را بررسی کنیم، خبرهای فراوانی در زمینه عملیات خرابکارانه در شبکه‌ها، سرورها و سایت‌های اینترنتی مشاهده خواهیم کرد. دست برد زدن به حساب‌های بانکی و نفوذ

1. Turban et al.

در سیستم‌های بانکی، سرقت اطلاعات مهم، حذف و مخدوش کردن اطلاعات، از کار انداختن و از سرویس خارج کردن سرورها، از جمله فعالیت‌هایی است که در نقاط مختلف جهان رخ می‌دهد. نکته جالب‌توجه اینکه حتی کشورهای مدعی در حوزه فناوری اطلاعات هم از عواقب سوء این حملات، مصون نبوده‌اند و هر یک به‌تناسب توانایی، دانش و درک موقعیت، برای جلوگیری از حملات و رفع آثار در صورت موفقیت حملات، ترمیم خرابی‌ها و تثبیت نقاط آسیب‌پذیر و توسعه فناوری، هزینه کرده‌اند و موفقیت‌های خوبی هم به دست آورده‌اند.

با توجه به اهمیت موضوع چالش‌برانگیز امنیت اطلاعات در سازمان‌های مختلف از جمله شهرداری‌ها، نیاز شدیدی به سرمایه‌گذاری، آموزش و حمایت مدیریت ارشد شهری در مقوله امنیت اطلاعات احساس می‌گردد تا گردش اطلاعات در شهرداری الکترونیک با حداقل مشکلات انجام پذیرد و حتی‌الامکان جلوی هرگونه حرکت عمدی و غیرعمدی به‌منظور دزدی و سوء استفاده احتمالی از اطلاعات با ارزش شهروندان در شهرداری الکترونیک گرفته شود و ریسک در خطر افتادن و نابودی و خرابی اطلاعات و وقفه در خدمت‌رسانی نیز کاهش یابد. با هدف کاهش احتمال بروز مشکل برای اطلاعات و بالا بردن کیفیت و میزان خدمت‌رسانی در شهرداری الکترونیک، سیستم مدیریت امنیت اطلاعات مورد نیاز است تا در تمامی مراحل طراحی، پیاده‌سازی و نگهداری از فناوری اطلاعات که شالوده شهرداری الکترونیک است، بکار گرفته شود (نعمتیان، ۱۳۹۳).

با توجه به اینکه مسائل امنیتی در سیستم‌های اطلاعاتی به سومین مانع عمده برای سازمان‌ها پس از فقدان منابع مالی و فنّاوری مناسب تبدیل شده‌اند، اکثر سازمان‌ها به نوآوری مستمر و مداوم در امنیت سیستم‌های اطلاعاتی خود می‌پردازند (کورسی و نوریس[1]، ۲۰۰۸). امنیت به‌عنوان "سیستم‌های جامع و روش‌های طراحی‌شده برای محافظت از دارایی‌های اطلاعاتی سازمان از افشا مقابل فرد یا سازمانی که مجاز به دسترسی به آن اطلاعات نیست"(هیل و پمبرتون[2]، ۱۹۹۵) تعریف می‌شود. امروزه نقض‌های امنیت اطلاعات به‌جای استثنا، تبدیل به

1. Coursey & Norris
2. Hill & Pemberton

هنجار شده است. این نقض قوانین و مقررات نه‌تنها موجب صدمه به شهرت می‌شود بلکه خطرات استراتژیک، مالی و قانونی را برای بنگاه‌ها ایجاد می‌کند (شرکت PWC، ۲۰۱۳). در مقایسه با سازمان‌های کوچک، نقض قوانین امنیت اطلاعات در شهرداری‌های الکترونیکی ممکن است عواقب جدی مانند لطمه به شهرت و اعتماد برای این‌گونه سازمان‌ها داشته باشد که درنهایت به زیان‌های پیچیده مالی، سیاسی و اقتصادی منجر می‌شود (فنگ و همکاران[1]، ۲۰۱۴).

بیشتر نقض‌های امنیت سیستم اطلاعات[2] به‌نوعی به کارکنان مربوط می‌شوند و نقض‌های داخلی بیشتر از ویروس‌ها یا هک شدن رخ می‌دهد (مؤسسه امنیت ملی، ۲۰۰۳). در مبحث تهدیدات انسانی، شرکت باید به شناسایی عوامل خرابکار داخلی و خارجی بپردازد. در برخی موارد عدم آموزش کافی کارمندان، بی‌توجهی و یا یک سهل‌انگاری ساده می‌تواند موجب نقض امنیت داخلی باشد. موفقیت در ایجاد امنیت اطلاعات تا حد زیادی به رفتار اثربخش کاربران وابسته است. رفتارهای مناسب و سازنده توسط مدیران سیستم، کاربران و افراد دیگر می‌تواند اثربخشی امنیت اطلاعات را تا حد زیادی افزایش دهد؛ درحالی‌که رفتارهای نادرست و مخرب، در حقیقت مانعی برای اثربخشی است (دلال[3]، ۲۰۰۵). آگاهی یافتن افراد از امنیت اطلاعات منجر به تقویت فعالیت‌های امنیتی مناسب و تغییر رفتار می‌شود و به افراد اجازه می‌دهد نسبت به امنیت سیستم‌های اطلاعات نگران و پاسخگو باشند و این موضوع به‌تدریج تبدیل به فرهنگ در سازمان‌ها خواهد شد (نیکرک و وان[4]، ۲۰۱۷). اثربخشی امنیت سیستم‌های اطلاعاتی تنها از طریق یکپارچه‌سازی مناسب فن‌آوری‌های امنیتی و سیاست‌ها و نهادینه‌سازی این سیاست‌ها در عمل به اجرا در می‌آیند. در این صورت است که کارکنان این سیاست‌ها را به‌طور کامل در آغوش می‌گیرند و مطابق آن رفتار می‌کنند (چوی و همکاران[5]، ۲۰۱۸). به نظر می‌رسد که فرایند نهادینه‌سازی نقش مهمی در اجرای واقعی سیاست‌ها و روش‌های امنیت سیستم‌های اطلاعات بازی می‌کند. سه نیروی اجتماعی مبتنی بر تئوری نهادی به‌عنوان پیشینه‌های مهم شناخته

1. Feng et al
2. Information Systems Security
3. Dalal
4. Nikrerk and Solms
5. Choi et al.

می‌شوند: فشارهای تقلیدی، هنجاری و اجباری. این فشارها یکدیگر را در بروز و ظهور سیاست‌ها و دستورالعمل‌های امنیتی در عملکرد حقیقی کارکنان تکمیل می‌کنند (دیمجیو و پاول[1]، ۱۹۸۳).

این مطالعه طراحی شده است تا نشان دهد که سازمان‌دهی امنیت سیستم اطلاعات در یک سازمان، نه‌تنها سیاست و شیوه‌های امنیت اطلاعات را شکل می‌دهند، بلکه چگونگی واکنش‌های سازمانی را که بر رفتار کارکنان تأثیر می‌گذارند، بیان می‌کند؛ و درنتیجه می‌تواند به پیاده‌سازی اثربخش سیاست‌های امنیتی سیستم اطلاعات منجر شود. مدل پژوهش با در نظر گرفتن دو مسیر در مورد اثرات فشارهای نهادی بر فرایند پذیرش فردی شکل گرفته است که یک مسیر افزایش مشروعیت الزامات امنیتی و دیگری بدبینی نسبت به این الزامات را نشان می‌دهد. مشروعیت و بدبینی سازمانی دو مسیر متفاوت اما به هم مرتبط در جهت اجرای موفق سیاست‌های امنیت سیستم‌های اطلاعات هستند. به‌عبارت‌دیگر، یک بعد از فشارهای نهادی از دو مسیر بر ادراک کارکنان تأثیر می‌گذارد: یکی از طریق بدبینی سازمانی که منجر به رفتار غیر شهروندی سازمانی و دیگری از طریق مشروعیت که منجر به رفتار شهروندی سازمانی می‌گردد و در نهایت به اثربخشی امنیت سیستم‌های اطلاعاتی منجر می‌شود. همچنین برای حصول موفقیت سازمان، نوآوری امنیت سیستم‌های اطلاعاتی باید بیش از تغییرات فنی صورت پذیرد. لذا وجود فرهنگ نوآورانه در امنیت سیستم‌های اطلاعاتی نقشی حیاتی در اثربخشی امنیت سیستم‌های اطلاعاتی ایفا می‌کند.

بنابراین پژوهش حاضر در جهت پاسخ‌دهی به این پرسش‌ها ایجاد شده است: چگونه فشارهای نهادی خارجی باعث می‌شوند تا سیاست‌ها و الزامات امنیتی سیستم اطلاعاتی در عملکرد واقعی کارکنان از طریق رفتار شهروندی سازمانی و رفتار ضد شهروندی سازمانی[2] بروز و ظهور یابد؟ دراین‌ارتباط نقش واسط مشروعیت سازمانی و بدبینی سازمانی نسبت به آن

1. DiMaggio & Powell
2. Counterproductive Work Behavior

الزامات چیست؟ و فرهنگ نوآورانه چگونه بر اثربخشی سیاست‌ها و الزامات امنیتی سیستم اطلاعاتی تأثیرگذار است؟

چارچوب نظری پژوهش

تئوری نهادی و هم‌شکلی سازمانی

تئوری نهادی بیان می‌کند که سازمان‌ها ساختارهای اجتماعی هستند که ساختارهای سازمانی آن‌ها از طریق واکنش نشان دادن به نقاط ضعف، قوت و تعهدات سازمان و همچنین فرصت‌ها و محدودیت‌های محیط خارج آن، ابزار انطباق‌پذیری‌شان است (مشبکی و همکاران، ۱۳۸۹)؛ بنابراین نهادها ازنظر سازوکارها و نتایج تعامل میان سازمان و محیط خارجی آن دارای تنوع هستند. تئوری نهادی با یک مبدأ جامعه‌شناختی قوی، این‌گونه متصور است که سازمان‌ها بر اساس پذیرش فشارهای نهادی اجباری، هنجاری و تقلیدی مشروعیت و بقا کسب می‌کنند. این مسئله دلالت بر انتقال ارزش‌های نهادی به استراتژی‌ها، ساختار و عملیات سازمان دارد که بدین‌وسیله هم‌شکلی سازمان با محیط اجتماعی ایجاد می‌شود (اسکات[1]، ۲۰۰۱). سازمان‌ها فرض می‌کنند هنگامی‌که با بی‌تفاوتی تسلیم فشارهای هنجاری و اجباری شوند، حمایت اجتماعی ذی‌نفعان را کسب می‌کنند. به‌عبارت‌دیگر، نظریهٔ نهادی معتقد است که سازمان‌ها به خاطر افزایش مشروعیت محیطی ساختارهای معینی را انتخاب می‌کنند که در حوزه سازمانی خود (در بازار یا جایگاه محیطی) به سمت الگوی مشترکی حرکت کنند (دیماجیو و پاول، ۱۹۸۳). نهادها به سه صورت شامل هم‌شکلی اجباری، تقلیدی و هنجاری به سازمان‌های مرتبط با خود فشار وارد می‌سازند تا ایشان را به متابعت از انتظاراتشان و هم‌شکلی با شیوه مورد انتظارشان مجبور کنند.

هم‌شکلی اجباری: ناشی از فشار اجباری از طرف نهادهای رسمی و دولتی. به‌عبارت‌دیگر، این هم‌شکلی ناشی از اختلافات قدرت است که از سوی سازمان‌های تأثیرگذار و نهادهای قانونی از طریق کنترل منابع، قانون‌گذاری و موقعیت اجتماعی بر سازمان تحمیل

1. Scott

می‌شود. دستور حفاظت از داده کمیسیون اروپا مثالی برای این نوع هم‌شکلی است (لیتر[1]، ۲۰۰۵).

هم‌شکلی تقلیدی: به‌ویژه در زمان‌های بحرانی پیش می‌آید و سازمان‌ها خود را با سازمان‌های موفق در حوزه سازمانی خود هم‌شکل می‌کنند. هم‌شکلی تقلیدی غالباً زمانی شکل می‌گیرد که مواجهه با عدم اطمینان حاکم بر سازمان نیازمند تحقیقاتی با هزینه‌های فراوان است (اشورس و همکاران[2]، ۲۰۰۹). حال‌آنکه نوآوری امنیت سیستم‌های اطلاعات به‌عنوان یک نوآوری فناوری در سازمان شامل عدم اطمینان فراوان است که سازمان را به سمت تقلید سوق می‌دهد. عدم اطمینان نشان می‌دهد که وقتی اعضای سازمان به‌روشنی فناوری‌های سازمانی مانند امنیت سیستم اطلاعاتی، با اهداف مبهم و عدم اطمینان زیاد را درک نمی‌کنند، به دنباله‌روی از روش‌ها و سیاست‌های نوآوری فنّاوری سازمان‌های دیگر روی می‌آورند (کوری[3]، ۲۰۱۲)

هم‌شکلی هنجاری: در این نوع هم‌شکلی، سازمان‌ها تلاش می‌کنند خود را با هنجارها و مدهای حرفه‌ای حوزه سازمانی خود هم‌شکل کنند. فشار هنجاری از تخصص و دانش بازیگران سازمانی، در زمینه‌های آموزشی و عضویت در جوامع حرفه‌ای، حاصل می‌شود (هو و همکاران[4]، ۲۰۰۷). حرفه‌ای سازی بازیگران سازمانی، بینش‌ها، فعالیت‌ها، مدل‌های حرفه‌ای و قوانین هنجاری را به دنبال دارد؛ و همان‌گونه که سازمان‌ها از مشاوران حرفه‌ای و کارشناسان از میان دانشگاهیان و محققان در مورد امنیت سیستم‌های اطلاعاتی خود از استفاده می‌کنند، هم‌شکلی هنجاری ممکن است بر الزامات امنیتی سیستم‌های اطلاعات این سازمان‌ها تأثیر بگذارد (دیماجیو و پاول، ۱۹۸۳)

نیروهای نهادی نه‌تنها تغییرات سازمانی مربوط به ساختارهای رسمی و سیستم‌های کنترل را موجب می‌شوند، بلکه تغییرات سازمانی مربوط به فرهنگ، هنجارها، قوانین، پاداش‌ها و مجازات و مهم‌تر از همه، رفتارهای شناختی و عاطفی اعضای سازمان را نیز ایجاد می‌کنند (چوی و همکاران، ۲۰۱۸). محققان استدلال کرده‌اند که تئوری نهادی می‌تواند در درک

1. Leiter
2. Ashworth et al.
3. Currie
4. Hu et al.

نوآوری‌های امنیت سیستم‌های اطلاعاتی هم در چارچوب این تغییرات مفید باشد (بیجورک[1]، ۲۰۰۴). هوو همکارانش پیشنهاد کردند که تئوری نهادی به‌عنوان یک چارچوب جامع اجتماعی سازمانی باید مورد استفاده قرار گیرد تا نه‌تنها رفتارهای اعضای سازمان، بلکه اعتقادات و نگرش‌های آنان در مورد توسعه و تغییر امنیت سیستم‌های اطلاعات را توضیح دهد؛ و مسئله بنیادین این است که چگونه این نگرش‌ها می‌تواند به اثربخشی امنیت سیستم‌های اطلاعاتی منجر شود (هو و همکاران، ۲۰۰۶).

اثربخشی امنیت سیستم‌های اطلاعات

امنیت اطلاعات مسئله‌ای مهم و حیاتی است که امروزه سازمان‌های سراسر دنیا با آن مواجه هستند. امنیت اطلاعات به عمل محافظت از اطلاعات در مقابل دسترسی نابجا، استفاده، افشا، اختلال یا تخریب غیرمجاز اطلاق می‌شود (سن و سامانتا[2]، ۲۰۱۴). به‌طورمعمول در تعاریف امنیت سیستم‌های اطلاعات، سه عامل به‌عنوان مبانی اصلی اثربخش در این مقوله معرفی می‌شوند:

- قابلیت اعتماد: اطمینان از اینکه اطلاعات تنها برای کسانی در دسترس است که مجاز به دستیابی به آن هستند.
- تمامیت (انسجام): از میزان درستی، انسجام و کامل بودن اطلاعات و روش‌های پردازش محافظت شود.
- در دسترس بودن: اطمینان از این‌که کاربرانِ مجاز، به‌موقع و به هنگام نیاز، به اطلاعات و دارایی‌ها دست پیدا می‌کنند (کوکلاکیس و همکاران[3]، ۲۰۰۰).

دستیابی به این عوامل را اثربخشی امنیت سیستم‌های اطلاعاتی گویند. ازنقطه‌نظر سازمانی می‌توان اثربخشی در سازمان‌ها را تحقق اهداف یا دستیابی به نتایج تعریف کرد. در همین راستا، اثربخشی امنیت سیستم‌های اطلاعاتی نیز به میزان دستیابی به اهداف برنامه‌های امنیت سیستم

1. Bjorck
2. Sen & Samanta
3. Kokolakis et al.

اطلاعات اشاره دارد که در این برنامه‌ها اطلاعات سازمانی به‌اندازه کافی محافظت می‌شود (هوانگ و چوی[1]، ۲۰۱۷). همچنین در کنار حفاظت از اطلاعات، استفاده مداوم از اقدامات امنیتی مانند روش‌ها و سیاست‌های امنیتی اطلاعات و اقدامات و ابزارهای کنترلی نیز در برنامه‌های امنیت اطلاعات لحاظ می‌گردد (کناپ و همکاران[2]، ۲۰۰۷). به مسئله امنیت اطلاعات از جنبه‌ها و زاویه‌های گوناگونی نگاه می‌شود .امنیت سیستم‌های اطلاعاتی را می‌توان از دو جهت بررسی کرد که عبارت‌اند از فناوری و افراد. گونزالز عامل اصلی در امنیت اطلاعات را عوامل انسانی خوانده است. همچنین شرکت IBM عنوان کرده است که در سال‌های آتی ضمن این‌که حملاتِ کوچک‌تر و پنهان کارانه تری به سیستم‌های اطلاعاتی سازمان‌ها صورت خواهد گرفت، مرکز توجه نفوذ گران "سهل‌انگاری و ساده‌اندیشی کاربران " خواهد بود؛ بنابراین "کاربر " همچنان به‌عنوان سست‌ترین عنصر آسیب‌پذیر در مدل‌های امنیتی، مورد سوءاستفاده قرار می‌گیرد.

تلاش‌های سازمان برای ارتقاء اثربخشی امنیت سیستم اطلاعات، مانند انگیزه، پاداش و مجازات، ممکن است انگیزه‌های خارجی را برای اعضای سازمانی جهت پیروی از سیاست‌ها و شیوه‌های امنیتی فراهم نماید. بااین‌حال، انگیزه‌های داخلی آن‌ها که لزوماً ناشی از استراتژی‌ها و سیاست‌های سازمانی است، برای اثربخشی امنیت سیستم اطلاعات حیاتی‌تر هستند (بولگرکو و همکاران[3]، ۲۰۱۰). الزامات امنیتی سیستم اطلاعات که همواره با تغییر همراه است، به‌عنوان یک فرایند پویا و ادامه‌دار، دائماً می‌تواند از طریق فشارهای نهادی مورد مشروعیت و یا مورد مقاومت و عدم پذیرش اعضای سازمان قرار گیرد (چوی و همکاران، ۲۰۱۸)

اقدامات امنیتی و رفتارهای سازمانی برای تأمین اثربخشی امنیت سیستم اطلاعات ضروری است و به‌شدت به یکدیگر وابسته و متصل می‌باشند. عوامل رفتاری سازمان عبارت‌اند از آموزش کاربر، فرهنگ امنیتی، پیوند سیاست و اجرای آن و حمایت مدیریت ارشد (ناپا و همکاران، ۲۰۰۷). علاوه بر این، اثربخشی سیستم امنیتی اطلاعات می‌تواند با اجرای چنین اقدامات امنیتی

1. Hwang & Choi
2. Knapp et al.
3. Bulgurcu

مانند سیاست‌های امنیتی اطلاعات، رویه‌ها، اقدامات کنترل، ابزارها و روش‌ها و افزایش آگاهی کارکنان بهبود یابد (هاگن و همکاران[1]، ۲۰۰۸). آگاهی‌رسانی به کارکنان شامل آموزش و تعلیم، کمپین‌های آگاهی‌رسانی، مشارکت کاربران، درگیر شدن و حمایت مدیریت عالی و یادگیری از تجربیات و اشتباهات است (چوی و همکاران، ۲۰۱۸).

تئوری نهادی رویکردی جامع ارائه می‌دهد، زیرا عواملی مانند تأثیرات نهادی، عوامل سازمانی، فرایندهای سیاست‌گذاری و مفاهیم فنی را مطرح می‌کند. علاوه بر این، رفتار شهروندی سازمانی و مشروعیت سازمانی نیز عوامل اجتماعی- سازمانی هستند که بر اثربخشی امنیت سیستم اطلاعاتی تأثیر می‌گذارد. رفتار مفهوم شهروندی سازمانی مشارکت‌های فردی در محل کار فراتر از الزامات نقش و دستاوردهای شغلی با پاداش غیرمتعارف را در بر می‌گیرد که عملکرد کارکنان را بهبود می‌بخشد و به‌طور قابل‌توجهی در اثربخشی سازمان و ارتباطات اجتماعی در سازمان نقش دارد (لاوی و لیتمن[2]، ۲۰۱۷). مشروعیت نیز موجب وفاداری فرد به سازمان شده و منجر به تعهد بیشتر اعضای سازمان نسبت به سیاست‌ها، اقدامات و تغییرات سازمانی می‌شود (پاولو و فیگنسون[3]، ۲۰۰۶).

مشروعیت سازمانی و رفتار شهروندی سازمانی در اثربخشی امنیت سیستم اطلاعاتی

تئوری نهادی تأکید می‌کند که تغییر سازمانی برای عملکرد سازمانی بهتر انجام نمی‌شود، بلکه برای کسب مشروعیت بیشتر است (اشورس، ۲۰۰۹). هم‌شکلی نهادی نیازمند تغییر در هنجارها، عقاید، ساختارها، شیوه‌ها و فرآیندهای سازمانی است و مشروعیت سازمانی این تغییرات را توجیه می‌کند. اعضای سازمان مشروعیت ایجاد شده از طریق هم‌شکلی را به‌عنوان یک اقدام سازگار برای بقای خود قبول می‌کنند (سئو و کرید[4]، ۲۰۰۲). تنها در بعد هم‌شکلی تقلیدی اتخاذ سیستم‌های جدید یا روش‌هایی که از سایر سازمان‌ها به تقلید گرفته می‌شود، الزاماً تغییرات عمده‌ای در باورها، هنجارها و فرهنگ اعضای سازمان که نشانه‌های مشروعیت سیستم جدید است، ایجاد نمی‌کنند؛ زیرا در اکثر مواقع تقلید بدون بازنگری دقیق از منابع داخلی،

1. Hagen et al.
2. Lavy & Littman
3. Pavlou & Fygenson
4. Seo & Creed

ظرفیت، هنجارها و باورها صورت پذیرفته و کارکنان این‌گونه تغییرات را تهدید به‌حساب می‌آورند (چوی و همکاران، ۲۰۱۸).

رویکرد استراتژیک اشاره می‌کند که سازمان‌ها از مشروعیت به‌عنوان یک منبع عملیاتی برای کمک به دستیابی به اهداف خود استفاده می‌کنند. هنگامی‌که هم‌شکلی نهادی در قالب فشارهای هنجاری و اجباری، سازمان‌ها را به سمت به‌کارگیری الزامات امنیت سیستم اطلاعاتی سوق می‌دهد، مشروعیت، اعضای سازمان را به سمتی پیش می‌برد که روش‌های جدید امنیت سیستم اطلاعات را به‌عنوان "سیستمی اجتماعی از هنجارها، باورها و تعاریف " می‌پذیرد. بر این اساس فرضیات زیر بیان می‌شود:

H1: هم‌شکلی تقلیدی تأثیر منفی بر مشروعیت سازمانی ISS دارد.

H2: هم‌شکلی هنجاری تأثیر مثبت بر مشروعیت سازمانی ISS دارد.

H3: هم‌شکلی اجباری تأثیر مثبت بر مشروعیت سازمانی ISS دارد.

واژه رفتار شهروندی سازمانی (OCB) اولین بار به‌وسیله بتمن و ارگان[1] (۱۹۸۳) مطرح گردید ولی پیش از آن، این مفهوم توسط سایر نویسندگان در قالب تمایل به همکاری و عملکرد و رفتارهای خودجوش و فراتر از انتظارات نقش تعریف شده است. ارگان (۱۹۸۹)، رفتار شهروندی سازمانی را به‌عنوان رفتارهای تحت اختیار فرد تعریف کرده و بیان می‌کند این دسته از رفتارها به‌طور مستقیم تحت تأثیر سیستم‌های پاداش رسمی قرار نمی‌گیرند ولی موجب ارتقاء اثربخشی کارکردهای سازمان می‌شوند. اختیاری بودن، بیانگر این است که این رفتارها، شامل رفتارهای مورد انتظار در نیازمندی‌های نقش و یا شرح شغل نیست (نازارس و چوی[2]، ۲۰۱۵).

مشروعیت سازمانی منجر به رفتارهای شهروندی سازمانی[3] اعضای سازمان و همچنین تعهد سازمانی و رضایت شغلی می‌شود (ایوانز و نویسویچ[4]، ۲۰۱۰). ممکن است کاربران به همان اندازه که به وظایف اصلی شغل خود اهمیت می‌دهند به امنیت اهمیت ندهند. وقتی این

1. Bateman & Organ
2. Nazareth & Choi
3. Organizational Citizenship Behavior
4. Evans & Novicevic

اتفاق بیفتد، امنیت به‌عنوان یک بخش اضافی از شغل تلقی می‌شود و درنتیجه رفتار شهروندی سازمانی در رابطه با مسائل امنیتی کمتر بروز پیدا می‌کند. حال‌آنکه اگر کارکنان وظایف امنیتی را به‌عنوان جزئی از نقش خود تلقی کنند و آن را دارای مشروعیت بدانند احتمالاً تلاش‌های بیشتری نیز در قبال آن انجام می‌دهند تا امنیت را حفظ کنند و این موضوع می‌تواند به رفتار شهروندی سازمانی از طریق پذیرش الزامات امنیت منجر شود (تورل و همکاران[1]، ۲۰۱۷)

علاوه بر این رفتار شهروندی سازمانی می‌تواند انطباق فرد با سیاست‌های امنیت اطلاعات را بهبود بخشد و به موفقیت در سیستم‌های اطلاعاتی منجر شود (ین و همکاران[2]، ۲۰۰۸). این موضوع تائید شده است که رفتار شهروندی سازمانی به‌طور مثبت با اثربخشی، کارایی و موفقیت سازمان مرتبط است (سان و همکاران[3]، ۲۰۱۵). رفتار شهروندی سازمانی کارمندان را تشویق می‌کند که تغییرات را پذیرفته و تصمیمات سازنده‌ای برای حل مشکلات پیدا کنند. همچنین به کارمندان کمک می‌کند تا با یکدیگر همکاری کرده و قدرت را در سیاست‌های سازمان به اشتراک بگذارند .علاوه بر این، رفتار شهروندی سازمانی می‌تواند تمایل افراد برای حل اختلافات را افزایش دهد و آن‌ها را به سازمان خود متعهد کند، به‌گونه‌ای که به دنبال منافع شخصی خود و یا گروه‌هایی که در آن شرکت می‌کنند نباشند (کی و وی[4]، ۲۰۰۸)

در بحث سیستم‌های اطلاعاتی، رفتار شهروندی سازمانی در ابعاد فردی و سازمانی بروز می‌یابد. در بعد فردی بیانگر افرادی است که به‌طور فعال به اعضای دیگر در مورد نحوه استفاده از سیستم‌های امنیت سیستم اطلاعاتی توصیه می‌کند؛ این دسته افراد از نوع‌دوستی و حسن نیت در کار برخوردار هستند. علاوه بر این، در بعد سازمانی سازمان‌ها را هدف قرار می‌دهد، مانند یک عضو سازمانی که داوطلبانه ایمیل‌های هک شده را به سازمان اعلام می‌کند و این موضوع نشان‌دهنده مسئولیت اجتماعی و فضیلت مدنی آن شخص است. بر اساس مطالعات قبلی، این مطالعه پیش‌بینی می‌کند که رفتار شهروندی سازمانی تأثیر مثبت بر اثربخشی امنیت سیستم

1. Turel et al.
2. Yen et al.
3. Sun et al.
4. Ke & Wei

اطلاعاتی داشته و آن را بهبود بخشد (وحیدی و همکاران[1]، ۲۰۱۴)؛ بنابراین، این مطالعه فرضیات زیر را پیشنهاد می‌کند:

H4: مشروعیت سازمانی ISS بر رفتار شهروندی سازمانی تأثیر مثبت دارد.

H5: رفتار شهروندی سازمانی بر اثربخشی ISS تأثیر مثبت دارد.

بدبینی سازمانی نسبت به ISS و رفتار ضد شهروندی سازمانی در اثربخشی امنیت سیستم اطلاعاتی

افراد به‌ندرت از تغییرات استقبال می‌کنند. مقاومت کارکنان در برابر تغییر دلیل عدم موفقیت بسیاری از پروژه‌ها شناخته شده است (هسیه[2]، ۲۰۱۶ و مرهی و اهلوالیا[3]، ۲۰۱۵). تحقیقات نشان می‌دهد که تغییرات در افراد مقاومت ایجاد می‌کند چراکه افراد ادامه وضع را ترجیح می‌دهند و مقاومت آن‌ها بیشتر به دلیل پیامدهای منفی تغییراتی است که توسط فناوری اطلاعات و ارتباطات جدید ایجاد شده است (هسیه، ۲۰۱۶). مردم تمایل دارند در مقابل تغییرات مقاومت کنند و نسبت به هر چیزی که در وضعیت زندگی روزمره و زندگی کاری آن‌ها خلل ایجاد نماید، بدبین می‌شوند (شارما و همکاران[4]، ۲۰۱۰). هنگامی‌که با فشارهای نهادی در جهت تغییرات سازمانی مواجه می‌شویم که در این مورد، پیاده‌سازی سیاست‌های امنیت سیستم‌های اطلاعاتی است، کارکنان در جایگاه شک و بدبینی قرار می‌گیرند. بدبینی سازمانی به‌عنوان پدیده‌ای شایع در سازمان‌ها شناخته شده است و اخیراً توجه بیشتری را در تحقیقات تغییرات سازمانی به دست آورده است (برگستروم و همکاران[5]، ۲۰۱۴). بدبینی سازمانی نگرش منفی به تغییر و تسهیل‌کنندگان تغییر تعریف می‌شود و با این دیدگاه می‌توان بدبینی سازمانی را با تغییر سازمانی مرتبط دانست (وارینگ[6]، ۲۰۰۹). برگستروم و همکاران (۲۰۱۴) بدبینی سازمانی را به‌عنوان یک شکل مقاومت در پی ناکامی از تغییرات سازمانی و به‌عنوان نگرشی منفی به مدیریت تعریف می‌کنند. درنهایت بدبینی سازمانی منجر به رفتارهای منفی مختلف در محل

1. Vahidi et al.
2. Hsieh
3. Merhi & Ahluwalia
4. Sharma et al.
5. Bergström et al.
6. Waring

کار مانند عدم حضور مکرر، عملکرد ضعیف و نارضایتی و مشارکت غیرفعال در فعالیت‌های تغییر سازمانی می‌شود (وانوس و همکاران[1]، ۲۰۰۰)

مطالعات در زمینه بررسی بدبینی سازمانی نسبت به سیستم‌های اطلاعاتی بسیار کم بوده است، اما متغیر مقاومت در این زمینه مستند شده است .در این مقاله بدبینی سازمانی به‌عنوان یک نوع مقاومت معرفی می‌شود و در طی بررسی ادبیات موضوع، بدبینی سازمانی را به مقاومت در ادبیات سیستم‌های اطلاعاتی بسط می‌دهد.

هم‌شکلی هنجاری منجر به حرفه‌ای شدن اعضای سازمان می‌شود و جهت‌گیری‌های مشابه در میان اعضا را از طریق تجربیات آموزشی و مشارکت در شبکه‌های حرفه‌ای ایجاد می‌کند (هو و همکاران، ۲۰۰۶). فشارهای هنجاری در میان سایر فشارهای نهادی از پذیرش بیشتری برخوردار هستند و دلیل آن هم ناشی شدن این فشارها از تجارب و جهت‌گیری‌های تسهیم شده‌ی مشابه میان کارکنان است؛ بنابراین فرض بر این است که فشارهای هنجاری احتمالاً بدبینی سازمانی را کاهش می‌دهند.

هم‌شکلی اجباری ناشی از فشارهای رسمی و غیررسمی است که توسط مقامات بالادست بر سازمان‌ها اعمال می‌شود و چنین فشارهایی ممکن است موجب احساس عدم ثبات در وضعیت فعلی قدرت شود و در نتیجه موجب می‌شود که اعضا در مقابل تغییراتی که باید اجرا شود، مقاومت کنند (مارتینکو و همکاران[2]، ۲۰۰۲). به‌طورکلی، دستورالعمل‌های امنیت سیستم اطلاعاتی که توسط مقامات خارجی و بالادست تعیین می‌شود انتظار می‌رود که با مقاومت گیرنده پیام مواجه شوند؛ اما بااین‌وجود تصویب قوانین و مقررات مناسب در راستای اجرای مؤثر، نظارت و کنترل رفتار فردی از سوی مقامات بالادست و دولت‌ها می‌تواند مسائل مربوط به حفظ حریم خصوصی و ارزیابی رسمی و ساختاریافته‌ی رفتارهای فردی در راستای حفظ امنیت سیستم اطلاعاتی را تسهیل نماید. لذا به همین دلیل می‌تواند منجر به کاهش بدبینی سازمانی نسبت به امنیت سیستم اطلاعات در سازمان شود.

1. Wanous et al.
2. Martinko

اما هم‌شکلی تقلیدی به علت عدم اطمینان بالا رخ می‌دهد که یک محرک قدرتمند در متقاعد ساختن سازمان‌ها برای تقلید و پیروی از مدل‌های سایر سازمان‌های برجسته است (کوتر[1]، ۲۰۰۷). زمانی که فن‌آوری‌ها برای سازمان قابل‌درک نیستند، اهداف تغییرات مبهم هستند و یا پیامدهای فن‌آوری جدید مشخص نیست، سازمان‌ها به پیروی از سازمان‌های دیگر، به‌ویژه رهبران فنّاوری، روی می‌آورند (دیماجیو و پاول، ۱۹۸۳). هم‌شکلی تقلیدی ممکن است سطح بدبینی سازمانی را بسته به علت تقلید، افزایش یا کاهش دهد. هنگامی‌که این دلیل منطقی و از نظر افراد به نفعشان است، مقاومت کمتری نشان می‌دهند. این در حالی است که اگر علت تغییرات به‌وضوح برای کارکنان توضیح داده نشود و یا قابل توجیه نباشد، در مقابل آن مقاومت کرده یا به‌صورت منفعلانه عمل می‌کنند (جاشی[2]، ۱۹۹۱)؛ اما با توجه به اینکه امنیت سیستم‌های اطلاعاتی، اهداف، فرآیندها و سیاست‌های آن مستقیماً به فعالیت‌های کاری کارکنان در اکثر سازمان‌ها مربوط نیست؛ بنابراین مزیت آن برای اکثر کارکنان مبهم است. به‌این‌ترتیب، می‌توان گفت که هم‌شکلی تقلیدی ممکن است بدبینی سازمانی را افزایش دهند.

H6: هم‌شکلی تقلیدی تأثیر مثبت بر بدبینی سازمانی نسبت به ISS دارد.

H7: هم‌شکلی هنجاری تأثیر منفی بر بدبینی سازمانی نسبت به ISS دارد.

H8: هم‌شکلی اجباری تأثیر منفی بر بدبینی سازمانی نسبت به ISS دارد.

بدبینان سازمانی سازمان خود را به دلیل عدم صداقت، عملیات ناعادلانه و رفتار غیرواقعی شایع مورد انتقاد قرار می‌دهند. گرچه بدبینی سازمانی نمی‌تواند به‌عنوان عدم تعهد سازمانی شناخته شود، اما تأثیر منفی بر تعهد سازمانی دارد (چوی و همکاران، ۲۰۱۵). بدبینی سازمانی به‌عنوان مانعی برای اجرای تغییرات سازمانی است و همچنین به‌عنوان واکنش اعضای سازمان به تغییرات نامناسب اجرا شده و عدم توانایی مدیریتی تعریف می‌شود. برگستروم و همکارانش (۲۰۱۴) استدلال می‌کنند که مهم‌ترین نتیجه بدبینی سازمانی این است که مشروعیت رهبری ممکن است تضعیف شود. علاوه بر این، بدبینی سازمانی باعث می‌شود کارکنان برنامه‌ها و روش‌های جدید را نادیده بگیرند.

1. Kotter
2. Joshi

ریچرز و همکاران[1] (۱۹۹۷) استدلال می‌کنند که بدبینی سازمانی نسبت به تغییرات می‌تواند سبب کاهش انگیزه کارکنان، رضایت شغلی و وفاداری آن‌ها شود. بر این اساس، کارکنان تمایل دارند در رفتارهای ضد شهروندی سازمانی شرکت کنند که این رفتارها به‌عنوان اقدامات داوطلبانه که هنجارهای سازمانی قابل‌توجهی را نقض می‌کنند و با منافع قانونی سازمان مخالف هستند، تعریف می‌شود.

این فرضیه که عوامل انسانی از اهداف بدخواهانه‌ای برخوردارند، تحقیقات امنیت سیستم اطلاعات در زمینه‌های بررسی چگونگی رفتارهای مرتبط با این موضوع متمرکز کرده است. از جمله این رفتارها، عملکرد ضداجتماعی یا مشکوک کارکنان، مانند خرابکاری اطلاعات سازمانی، غیرفعال کردن سیستم‌های امنیتی یا نابود کردن یا حذف داده‌ها است (بند و همکاران[2]، ۲۰۰۶). اثرات منفی این‌گونه رفتار می‌تواند به‌صورت فردی از عملکردهای شناختی گرفته تا رفتارهای پرخاشگرانه بروز یابد و افراد در این موقعیت قادر به پردازش صحیح اطلاعات نیستند و تصمیمات اشتباهی اتخاذ می‌کنند. علاوه بر این این‌گونه افراد ناامیدی روانی و محرومیت را تجربه می‌کنند که در نتیجه آن توانایی همدلی با دیگران را از دست می‌دهند و رفتارهای پرخاشگرانه نسبت به دیگران و سازمان نشان می‌دهند (یانگ و تریدوی[3]، ۲۰۱۸)؛ بنابراین، بدبینی سازمانی نسبت به سیاست‌ها و شیوه‌های امنیت سیستم اطلاعات، رفتارهای ضد شهروندی سازمانی کارکنان در جهت اختلال در امنیتی سیستم را افزایش می‌دهد که باعث کاهش اثربخشی امنیت سیستم اطلاعات خواهد شد.

H9: بدبینی سازمانی نسبت به ISS تأثیر مثبت بر رفتار ضد شهروندی سازمانی دارد.

H10: رفتار ضد شهروندی سازمانی تأثیر منفی بر اثربخشی ISS دارد.

فرهنگ نوآورانه و اثربخشی امنیت سیستم اطلاعاتی

فرهنگ‌سازمانی می‌تواند اعضای سازمان را به پذیرش نوآوری و تغییرات سازمانی به‌عنوان بخشی از ارزش‌های مشترک سازمان دعوت کند و رفتار نوآورانه و نوآوری مؤثر را

1. Reichers et al.
2. Band et al.
3. Yang et al.

در میان اعضای سازمان تسهیل نماید (هارتمن، ۲۰۰۶). در این راستا، فرهنگ‌سازمانی می‌تواند یک هسته مرکزی برای نوآوری مؤثر در امنیت سیستم‌های اطلاعاتی در سازمان‌ها باشد. نوآوری اثربخش بر تعامل میان فشارهای نهادی و فرهنگ‌سازمانی استوار است (هو و همکاران، ۲۰۱۰).

لیندر و کیورس (۲۰۰۶) معتقدند شرکت‌ها تمایل دارند تا سیستم‌های امنیت اطلاعات را در مقیاس‌های پذیرفته‌شده در فرهنگ‌سازمانی خود بکار گیرند. لی و همکاران (۲۰۱۰) در تحقیقات خود بیان می‌کنند که فرهنگ‌سازمانی می‌تواند نقش میانجی بین فشارهای نهادی (هم‌شکلی) و پذیرش یا انتشار نوآوری‌های سازمانی داشته باشد. جاشاوالا و ساشیتال (۲۰۰۲) نشان دادند که فرهنگ نوآورانه ابتکار عمل، خلاقیت و ریسک‌پذیری را افزایش می‌دهد و اعتماد اعضای سازمان، حس برابری، احساس رفتار عادلانه، حس خودی بودن به‌عنوان فردی که در فرآیند نوآوری و تغییرات سازمان حضور داشته است را فراهم می‌آورد.

برای حصول موفقیت سازمان، نوآوری ISS باید بیش از تغییرات فنی صورت پذیرد. نوآوری در ISS نه‌تنها شامل نوآوری‌های فنّاورانه است و بر پیشرفت‌های فن‌آوری در زمینه امنیت اطلاعات متمرکز است بلکه یک فلسفه نوآوری اداری است که شامل توسعه برنامه‌های مدیریت امنیت، تغییرات فرهنگی و تغییرات رفتاری در میان سهامداران نیز است. نوآوری امنیت سیستم‌های اطلاعاتی همچنین شامل راه‌اندازی روش‌های جدید و پیچیده امنیت سیستم اطلاعاتی جدید است.

اعضای سازمان ممکن است در مقابل نوآوری‌هایی که با فرهنگ‌سازمانی سازگار نیستند، مقاومت کنند (مارکوس و شولر[1]، ۲۰۰۴) که این امر منجر به خاتمه دادن نوآوری در زمینه امنیت سیستم‌های اطلاعاتی نیز می‌شود. فرهنگ امنیت اطلاعاتی که به‌عنوان یک تعهد در میان مدیران ارشد برای امنیت اطلاعات ایجاد می‌شود، می‌تواند بر اهداف حرفه‌ای برای رعایت امنیت اطلاعات ایجاد می‌شوند، تأثیر بگذارد (گرین و دارکی، ۲۰۱۰). گاهی اعضای سازمان به دلیل عدم تغییرات فرهنگی، نگرش و رفتارهای مناسبی در زمینه امنیت سیستم اطلاعات نشان نمی‌دهند، که این فقدان فرهنگ سازمان می‌تواند بخشی از مدیریت نابسامان امنیت سیستم‌های اطلاعاتی را توضیح دهد. بدون فرهنگ حمایتی در جهت امنیت سیستم‌های اطلاعاتی، اعضای سازمان ممکن است تمایلی به دنبال کردن شیوه‌های جدید نداشته باشند. در نتیجه، فرهنگ

1. Marcus & Schuler

نوآورانه در امنیت سیستم‌های اطلاعاتی نقشی حیاتی در اثربخشی امنیت سیستم‌های اطلاعاتی ایفا می‌کند. با توجه به این ادبیات فرضیات زیر در این پژوهش تعریف شده است:

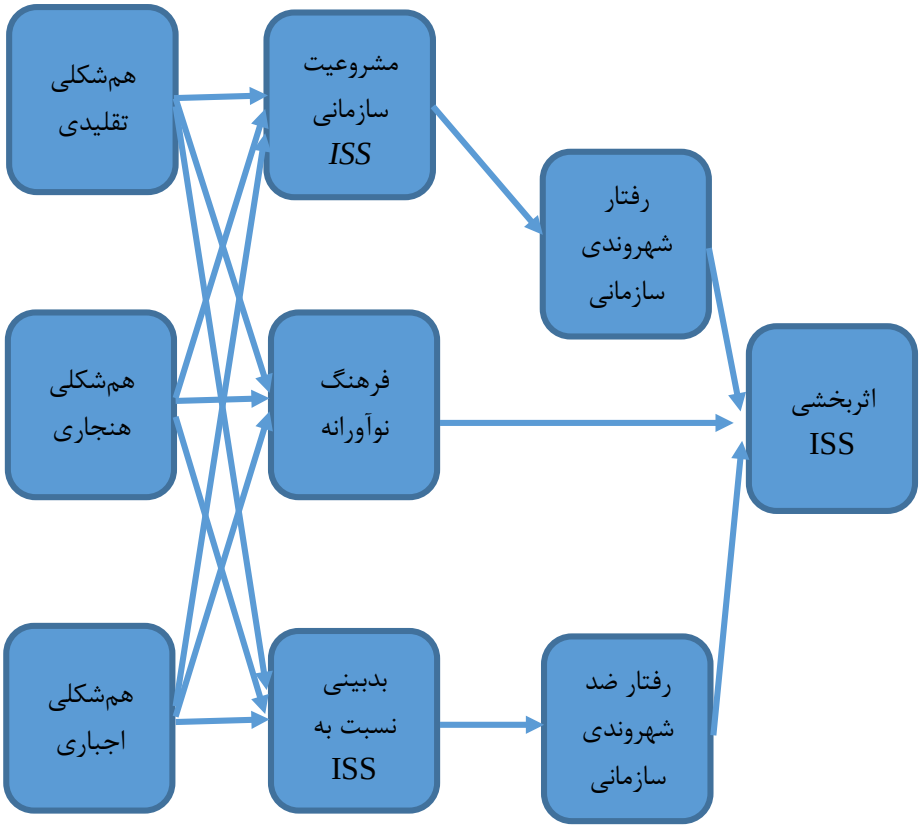
H11: هم‌شکلی تقلیدی تأثیر مثبت بر فرهنگ نوآورانه دارد.

H12: هم‌شکلی هنجاری تأثیر مثبت بر فرهنگ نوآورانه دارد.

H13: هم‌شکلی اجباری تأثیر مثبت بر فرهنگ نوآورانه دارد.

H14: فرهنگ نوآورانه تأثیر مثبت بر اثربخشی ISS دارد.

بر اساس مبانی نظری و فرضیات بیان‌شده در این بخش مدل پژوهش به‌صورت زیر تعریف می‌شود.



شکل ۱: مدل مفهومی پژوهش

روش‌شناسی پژوهش

پژوهش حاضر از حیث هدف کاربردی و از حیث روش توصیفی- پیمایشی است. جامعه آماری پژوهش شامل کارشناسان فناوری اطلاعات شهرداری مشهد است. به جهت تعیین حجم نمونه از فرمول کوکران برای جامعه معلوم استفاده شد. در این روش ابتدا یک نمونه‌ی اولیه شامل ۳۰ پرسش‌نامه از کارکنان، مورد پیش‌آزمون قرار گرفته و با جایگذاری انحراف معیار آن به میزان ۶/. در فرمول کوکران با دقت برآورد و سطح اطمینان ۹۵/. و میزان خطای ۰/۰۵ حداقل حجم نمونه ۱۰۵ نفر تعیین گردید. با توجه به اینکه عدم بازگشت دادن پرسش‌نامه‌ها پیش‌بینی می‌گردید، ۱۲۰ پرسش‌نامه به‌طور تصادفی ساده در بین کارکنان توزیع شد و از این تعداد، ۱۰۹ پرسش‌نامه برگشت داده شد که در فرایند تجزیه‌وتحلیل مورداستفاده قرار گرفت.

قبل از برازش مدل معادلات ساختاری پژوهش، مدل‌های اندازه‌گیری با اجرای تحلیل عاملی تأییدی در نرم‌افزار آموس، مورد ارزیابی قرار گرفتند. این ارزیابی‌ها با استفاده از شاخص‌های برازش خروجی نرم‌افزار و معناداری بارهای عاملی گویه‌های سازه‌های مختلف پرسش‌نامه صورت گرفت. در ابتدا هریک از مدل‌های اندازه‌گیری به‌طور جداگانه بررسی شدند و سپس مدل اندازه‌گیری کلی نیز مورد بررسی قرار گرفت. با توجه به اینکه در مدل تحلیل عاملی تأییدی برازش یافته، بار عاملی تمامی گویه‌ها معنادار بودند، هیچ‌یک از گویه‌ها از فرایند تجزیه‌وتحلیل کنار گذاشته نشدند. مبنای معناداری گویه‌ها این است که سطح معناداری برای آن‌ها زیر ۰/۰۵ باشد. ازاین‌رو در نهایت، ۵۰ گویه از پرسشنامه، تجزیه‌وتحلیل شد. نتایج تحلیل عاملی تأییدی برای گویه‌های معنادار به همراه شاخص‌های برازش مدل تحلیل عاملی تأییدی در جدول شمارهٔ ۱ ارائه شده است. این شاخص‌ها نشان از برازش مطلوب مدل‌های اندازه‌گیری داشته و بر این اساس معناداری بار شدن هر متغیر مشاهده‌شده به متغیر مکنون مربوطه، تأیید شد.

جدول ۱: نتایج تحلیل عاملی تأییدی برای گویه‌های پرسشنامه

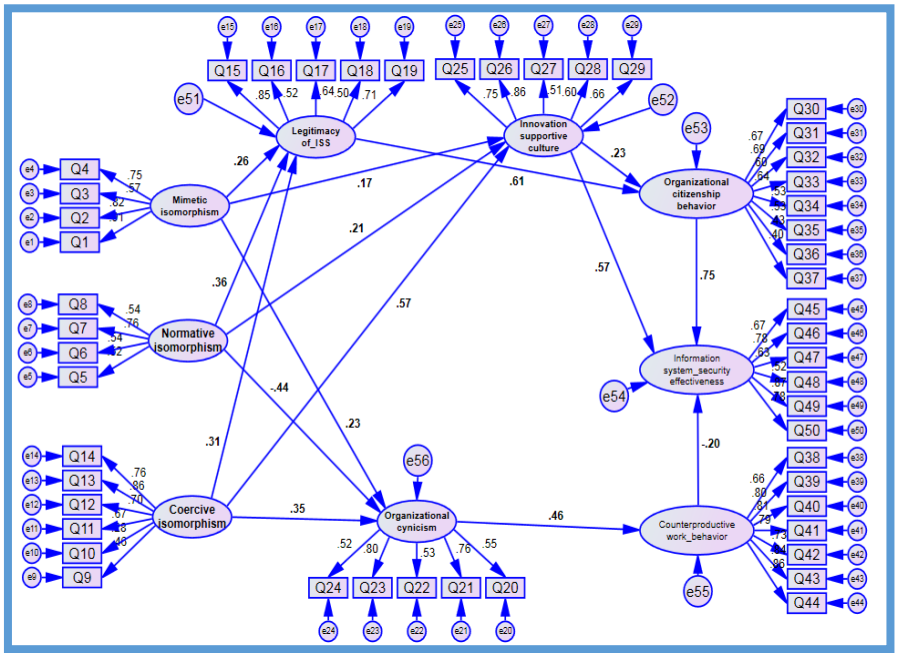
نام متغیرها	گویه	بار عاملی	سطح معناداری	نتیجه	آلفای کرونباخ	نام متغیرها	گویه	بار عاملی	سطح معناداری	نتیجه	آلفای کرونباخ
هم‌شکلی تقلیدی	Q1	۰/۹۱۲	۰/۰۰۰	معنادار	۰/۸۴۷	فرهنگ نوآورانه	Q25	۰/۷۷۵	۰/۰۰۰	معنادار	۰/۸۲۷
	Q2	۰/۸۱۴	/۰۰۰	معنادار			Q26	۰/۸۷۴	۰/۰۰۰	معنادار	
	Q3	۰/۵۸۹	/۰۰۰	معنادار			Q27	۰/۵۲۶	۰/۰۰۰	معنادار	
	Q4	۰/۷۳۷	/۰۰۰	معنادار			Q28	۰/۶۱۶	۰/۰۰۰	معنادار	
هم‌شکلی هنجاری	Q5	۰/۷۰۹	/۰۰۰	معنادار	۰/۷۶۴		Q29	۰/۶۹۳	۰/۰۰۰	معنادار	
	Q6	۰/۵۷۳	/۰۰۰	معنادار		رفتار شهروندی سازمانی	Q30	۰/۶۳۷	۰/۰۰۰	معنادار	۰/۷۹۳
	Q7	۰/۶۸۰	/۰۰۰	معنادار			Q31	۰/۶۹۴	۰/۰۰۰	معنادار	
	Q8	۰/۵۳۶	/۰۰۰	معنادار			Q32	۰/۵۹۴	۰/۰۰۰	معنادار	
هم‌شکلی اجباری	Q9	۰/۴۹۹	/۰۰۰	معنادار	۰/۸۴۷		Q33	۰/۶۶۷	۰/۰۰۰	معنادار	
	Q10	۰/۶۶۸	/۰۰۰	معنادار			Q34	۰/۵۶۱	۰/۰۰۰	معنادار	
	Q11	۰/۷۲۵	/۰۰۰	معنادار			Q35	۰/۵۳۷	۰/۰۰۰	معنادار	
	Q12	۰/۷۱۶	/۰۰۰	معنادار			Q36	۰/۴۸۷	۰/۰۰۰	معنادار	
	Q13	۰/۸۲۶	۰/۰۰۰	معنادار			Q37	۰/۴۶۴	۰/۰۰۰	معنادار	
	Q14	۰/۷۴۰	۰/۰۰۰	معنادار		رفتار ضد شهروندی سازمانی	Q38	۰/۶۵۶	۰/۰۰۰	معنادار	۰/۹۲۱
مشروعیت سازمانی ISS	Q15	۰/۸۵۴	۰/۰۰۰	معنادار	۰/۷۷۹		Q39	۰/۸۱۱	۰/۰۰۰	معنادار	
	Q16	۰/۵۵۲	۰/۰۰۰	معنادار			Q40	۰/۸۰۵	۰/۰۰۰	معنادار	
	Q17	۰/۶۶۸	۰/۰۰۰	معنادار			Q41	۰/۷۷۹	۰/۰۰۰	معنادار	
	Q18	۰/۵۱۹	۰/۰۰۰	معنادار			Q42	۰/۷۳۲	۰/۰۰۰	معنادار	
	Q19	۰/۷۳۱	۰/۰۰۰	معنادار			Q43	۰/۸۵۰	۰/۰۰۰	معنادار	
بدبینی نسبت به ISS	Q20	۰/۵۵۱	۰/۰۰۰	معنادار	۰/۷۶۹		Q44	۰/۸۶۷	۰/۰۰۰	معنادار	
	Q21	۰/۷۵۹	۰/۰۰۰	معنادار		اثربخشی ISS	Q45	۰/۶۸۹	۰/۰۰۰	معنادار	۰/۸۷۷
	Q22	۰/۵۳۶	۰/۰۰۰	معنادار			Q46	۰/۷۸۲	۰/۰۰۰	معنادار	
	Q23	۰/۸۲۲	۰/۰۰۰	معنادار			Q47	۰/۶۱۸	۰/۰۰۰	معنادار	
	Q24	۰/۵۵۲	۰/۰۰۰	معنادار			Q48	۰/۵۰۴	۰/۰۰۰	معنادار	
							Q49	۰/۹۱۶	۰/۰۰۰	معنادار	
							Q50	۰/۷۹۸	۰/۰۰۰	معنادار	

تجزیه‌وتحلیل یافته‌ها

پس از ارزیابی مدل‌های اندازه‌گیری، مدل ساختاری پژوهش با استفاده از نرم‌افزار آموس مورد بررسی قرار گرفت و نسبت به تأیید یا رد فرضیات اقدام شد. شاخص‌های برازش مدل، حاکی از برازش مطلوب آن به داده‌های پژوهش است که در جدول شماره ۲ نشان داده شده است. تمام شاخص‌های برازش الگوی نهایی، از نقاط برش پیش‌گفته مطلوب‌ترند که از برازش کاملاً رضایت‌بخش مدل حکایت دارد.

جدول ۲: شاخص‌های برازش مدل اندازه‌گیری و مدل ساختاری

نام شاخص	نماد	مقدار قابل قبول	مقدار ایده ال	مدل اندازه‌گیری	مدل ساختاری
درجه آزادی	(df)	–	–	۱۱۳۹	۱۱۶۰
کای اسکوئر	(χ^2)	$2df \leq \chi^2 \leq 3df$	$0 \leq \chi^2 \leq 2df$	۳۱۷۰/۹۲۱	۳۲۴۰/۲۹۵
کای اسکوئر بهینه شده	(χ^2/df)	$2 < \chi^2/df \leq 3$	$0 \leq \chi^2/df \leq 2$	۲/۷۸۳	۲/۷۹۳
نیکوئی برازش	(GFI)	$.80 \leq GFI < .95$	$.95 \leq GFI \leq 1.00$	۰/۸۴۳	۰/۸۲۶
ریشه میانگین مربعات باقی‌مانده	(RMR)	$0 < RMR \leq .10$	$0 \leq RMR \leq .05$	۰/۰۸۶	۰/۰۸۹
شاخص برازش تطبیقی	(CFI)	$.90 \leq CFI < .97$	$.97 \leq CFI \leq 1.00$	۰/۹۳۳	۰/۹۲۱
ریشه‌ی میانگین مربعات خطای برآورد	(RMSEA)	$.05 < RMSEA \leq .08$	$0 \leq RMSEA \leq .05$	۰/۰۸۹	۰/۰۸۴
شاخص نیکویی برازش ایجازی	(PGFI)	$.50 \leq PGFI < .60$	$.60 \leq PGFI \leq 1.00$	۰/۵۸۵	۰/۵۷۹
شاخص برازش ایجازی هنجارشده	(PNFI)	$.50 \leq PNFI < .60$	$.60 \leq PNFI \leq 1.00$	۰/۵۱۱	۰/۵۸۱



شکل ۲: الگوی معادلهٔ ساختاری

در مدل برازش یافته تمام اثرهای مستقیم بین متغیرها در سطح اطمینان ۰/۹۵ مثبت و معنادارند ($p<0/05, t>1/96$). برای آزمون فرضیه از دو شاخص p-value و t-value استفاده شده و شرط معنادار بودن یک رابطه این است که مقدار شاخص اول برای رابطهٔ مدنظر کمتر از ۰/۰۵ و مقدار شاخص دوم خارج از بازه ۱/۹۶± باشد. همان‌گونه که در جدول ۳ و همچنین شکل ۲ مشاهده می‌شود همه ضرایب در نظر گرفته شده شرایط گفته‌شده را دارا می‌باشند و همگی آن‌ها تأیید می‌شود. همچنین قوی‌ترین ضریب اثر مربوط به اثر رفتار شهروندی سازمانی بر اثربخشی ISS و ضعفت ترین مقدار نیز مربوط به ضریب اثر هم‌شکلی تقلیدی بر فرهنگ نوآورانه است که البته با توجه به دو شاخص p-value و t-value معنادار است. نتیجهٔ آزمون فرضیه‌های ۱ تا ۱۴ پژوهش، به‌طور خلاصه در جدول ۳ نشان داده شده است.

جدول ۳: خلاصهٔ نتایج آزمون فرضیه‌های پژوهش

نتایج / فرضیه	ضریب استاندارد	عدد معناداری	سطح معناداری	نتیجهٔ آزمون
۱. هم‌شکلی تقلیدی ← مشروعیت سازمانی ISS	۰/۳۶۱	-۳/۶۶۷	۰/۰۰۴	تأیید
۲. هم‌شکلی هنجاری ← مشروعیت سازمانی ISS	۰/۳۷۲	۲/۹۹۳	۰/۰۰۳	تأیید
۳. هم‌شکلی اجباری ← مشروعیت سازمانی ISS	۰/۲۹۳	۲/۷۰۳	۰/۰۰۷	تأیید
۴. مشروعیت سازمانی ISS ← رفتار شهروندی سازمانی	۰/۶۳۲	۵/۳۵۸	۰/۰۰۰	تأیید
۵. رفتار شهروندی سازمانی ← اثربخشی ISS	۰/۷۳۴	۵/۶۵۶	۰/۰۰۰	تأیید
۶. هم‌شکلی تقلیدی ← بدبینی سازمانی	۰/۲۲۸	۲/۲۲۸	۰/۰۲۶	تأیید
۷. هم‌شکلی هنجاری ← بدبینی سازمانی	-۰/۴۱۸	-۴/۵۸۷	۰/۰۰۰	تأیید
۸. هم‌شکلی اجباری ← بدبینی سازمانی	-۰/۱۵۴	-۲/۰۰۴	۰/۰۴۴	تأیید
۹. بدبینی سازمانی ← رفتار ضد شهروندی	۰/۴۶۵	۳/۷۲۳	۰/۰۰۰	تأیید
۱۰. رفتار ضد شهروندی ← اثربخشی ISS	-۰/۱۹۸	-۲/۰۱۳	۰/۰۴۰	تأیید
۱۱. هم‌شکلی تقلیدی ← فرهنگ نوآورانه در زمینه ISS	۰/۳۵۱	۳/۵۴۱	۰/۰۰۰	تأیید
۱۲. هم‌شکلی هنجاری ← فرهنگ نوآورانه در زمینه ISS	۰/۲۱۵	۲/۱۵۸	۰/۰۳۰	تأیید
۱۳. هم‌شکلی اجباری ← فرهنگ نوآورانه در زمینه ISS	۰/۵۵۵	۴/۰۵۲	۰/۰۰۰	تأیید
۱۴. فرهنگ نوآورانه در زمینه ISS ← اثربخشی ISS	۰/۵۸۶	۴/۴۴۶	۰/۰۰۰	تأیید

بحث و نتیجه‌گیری

در عصر حاضر، کشوری می‌تواند به توسعه پایدار و همه‌جانبه دست یابد که مردم آن کشور در مسیر رشد بلوغ فکری گام بردارند و این امر تنها از طریق آسان‌سازی در دسترسی و تسهیم دانش و اطلاعات میسر خواهد شد و از همین رو ضرورت توجه به فناوری اطلاعات بشدت احساس می‌گردد تا با استفاده از توانمندی‌های آن، زندگی شهروندان تسهیل گردد و اهداف عالیه کشور نیز با کمک مزایای حاصله از ایجاد و حفظ و گسترش شهرداری الکترونیک محقق گردد. یکی از مهم‌ترین چالش‌های پیش رو در مبحث شـــهرداری الکترونیک، امنیت فضای

تبادل اطلاعات است که خود ضرورت ایجاد و توسعه سیستم مدیریت امنیت اطلاعات را موجب می‌گردد.

تعداد کمی از مطالعات امنیت سیستم‌های اطلاعات از نظریه نهادی استفاده کرده‌اند و اکثر این مطالعات نظریه نهادی را تنها در مفهوم مورد استفاده قرار داده‌اند. حال‌آنکه این مطالعه به‌صورت تجربی به بررسی نظریه نهادی در امنیت سیستم اطلاعاتی می‌پردازد. علاوه بر این در این مطالعه از سازه‌های رفتار شهروندی سازمانی (OCB) و رفتار ضد شهروندی سازمانی (CWB) برای توضیح اثربخشی امنیت سیستم اطلاعاتی (ISS) استفاده شده است.

این مطالعه سه نیروی هم‌شکلی اجتماعی بر پایه تئوری نهادی شامل هنجاری، اجباری و تقلیدی را به‌عنوان پیشینه‌های اساسی اجرای اثربخش امنیت سیستم اطلاعاتی معرفی می‌کند. علاوه بر این، یک مدل دوطرفه، به‌عنوان مکانیسم میانجی در نهادینه‌سازی امنیت سیستم اطلاعات توسعه یافته است. یک مسیر از طریق مشروعیت سازمانی امنیت و رفتار شهروندی سازمانی اتفاق می‌افتد، درحالی‌که مسیر دیگر از طریق بدبینی سازمانی و رفتار ضد شهروندی سازمانی رخ می‌دهد. همچنین ازآنجاکه بدون فرهنگ حمایتی در جهت بهبود روش‌های امنیت سیستم‌های اطلاعاتی، اعضای سازمان ممکن است تمایلی به دنبال کردن شیوه‌های جدید نداشته باشند، لذا فرهنگ نوآورانه به‌عنوان یک فلسفه نوآوری شامل توسعه برنامه‌های مدیریت امنیت، تغییرات فرهنگی و ... متأثر از فشارهای نهادی می‌تواند بر اثربخشی امنیت سیستم‌های اطلاعاتی تأثیرگذار باشد که این مسیر نیز مورد بررسی قرار گرفت.

داده‌ها به‌طورکلی از مدل تحقیق پیشنهادی حمایت می‌کنند و این موضوع نشان‌دهنده کاربرد تئوری نهادی در اثربخشی امنیت سیستم اطلاعاتی است. نیروهای اجباری تأثیر مطلوبی بر ایجاد مشروعیت ISS و کاهش بدبینی سازمانی نسبت به تغییرات سازمانی نوآورانه در زمینه

امنیت سیستم‌های اطلاعاتی دارد؛ بنابراین با تصویب قوانین و مقررات مناسب امنیتی از سوی دولت‌ها و شرکای تجاری و تمرکز بر اجرای مؤثر، نظارت و کنترل رفتار افراد در سازمان می‌توان اثربخشی امنیت سیستم‌های اطلاعات را تقویت نمود.

نیروهای هنجاری، شبکه‌ها و عملکرد حرفه‌ای سازمان در زمینه امنیت سیستم اطلاعات را ارتقا می‌دهند و می‌توانند نقش مهمی را در اجرای مقررات و سیاست‌های حمایتی در جهت امنیت سیستم اطلاعات ایفا کنند. این موضوع به دلیل وجود متخصصین و شبکه‌های امنیت سیستم اطلاعات به‌عنوان عوامل متقاعدکننده در سازمان، ممکن است بدبینی و مقاومت سازمانی را کاهش دهد و توافق و مشارکت را در ایجاد مقررات و سیاست‌های حمایتی پیاده‌سازی ISS ایجاد کند. اعضای سازمان هم‌شکلی هنجاری را به‌مثابه ایجاد یک فرهنگ مناسب با ارتباطات رسمی، غیررسمی و گفتمانی در نظر می‌گیرند که به آموزش کارشناسان و متخصصین امنیت سیستم اطلاعات از طریق انجمن‌های آکادمیک و کمیته‌های علمی و کمیته‌های دولتی می‌پردازد. همچنین تغییرات سازمانی رادیکال و سریع را به کارکنان و سازمان تحمیل نمی‌کند. لذا این بعد از تئوری نهادی مشروعیت زیادی برای امنیت سیستم اطلاعات به همراه دارد.

در ادامه یافته‌های پژوهش این نتیجه حاصل شد که فشارهای تقلیدی به مشروعیت سازمانی امنیت سیستم اطلاعاتی منجر نمی‌شود. چراکه فشارهای تقلیدی از جمله اتخاذ سیستم‌ها و روش‌های جدید از سایر سازمان‌ها و در مورد مطالعه این پژوهش از شهرداری سایر شهرها و مناطق، اعتقادات، هنجارها و فرهنگ اعضای سازمان که ریشه‌های مشروعیت هستند را تغییر نمی‌دهد. هم‌شکلی تقلیدی اعضای سازمان را از طریق تقلید بدون بازنگری دقیق در منابع داخلی، ظرفیت‌های سازمانی، هنجارها و باورهایشان، تهدید می‌کند.

هنگامی که این سه نیروی نهادی با یکدیگر رقابت می کنند تا بر روند فرایندهای فناوری و اداری امنیت سیستم اطلاعات که منجر به تغییرات سازمانی می‌شوند، تأثیر بگذارد، اعضای سازمان به نیرویی که بیشترین انعطاف‌پذیری و کمترین میزان تهدید را جهت ایجاد تغییرات سازمانی دارد، واکنش مثبت نشان می‌دهند. اگرچه استراتژی اجباری به‌طور مؤثر برای تغییرات مکانیکی در فرآیندهای کسب‌وکار اثربخش است، استراتژی هنجاری برای مواردی مانند تغییرات امنیتی سیستم‌های اطلاعاتی که در آن بهتر است کارکنان به‌طور داوطلبانه تغییرات را بپذیرند، عملکرد مناسب‌تری دارد.

به نظر می‌رسد که کسب آگاهی به‌صورت عملی در تخصص‌های مختلف بسیار مهم‌تر از داشتن تکنسین‌ها و فناوری‌های مرتبط با آن است (در این مقاله بحث امنیت سیستم‌های اطلاعات مدنظر است). در این زمینه سبک رهبری تحول‌آفرین به‌عنوان راهکاری برای رسیدن به هم‌شکلی هنجاری می‌تواند بسیار مفید واقع شود. دلیل اهمیت رهبری تحول‌آفرین این است که سازگاری و بقای سازمان مستلزم ایجاد و نهادینه‌سازی سیستم‌ها و روندهای جدیدی است و این امر بدون رهبری مؤثر امکان‌پذیر نخواهد بود. این سبک رهبری منجر به ایجاد انجمن‌ها یا کمیته‌های حرفه‌ای در زمینه امنیت سیستم اطلاعات شده و از طریق گسترش شبکه‌های ISS می‌تواند به ایجاد هنجارها، فرهنگ، اعتقادات و استانداردها کمک کند. رهبران تحول‌گرا نه‌تنها باید دیدگاهی مناسب از سیاست‌های امنیت سیستم اطلاعات جهت بالا بردن تمرکز استراتژیک و انگیزشی کارکنان فراهم کنند، بلکه باید تعهد کارکنان را به الزامات امنیت سیستم اطلاعات از طریق رهبری کاریزماتیک افزایش دهند. رهبری تحول‌آفرین بدبینی کارکنان نسبت به تغییرات سازمانی را از دو طریق مدیریت می کند: بهبود ادراکات کارکنان از موفقیت‌های آینده و ایجاد اعتماد از طریق بیان مزایای امنیت سیستم اطلاعات در کسانی که مسئول ایجاد تغییرات

هستند؛ بنابراین رهبری تحول‌آفرین به‌مثابه تسهیل‌کننده فرهنگ حمایتی در امنیت سیستم اطلاعاتی می‌باشند که باعث تشویق رفتار شهروندی سازمانی کارکنان در راستای الزامات امنیت می‌شود. بنا بر نتایج پژوهش رفتار شهروندی سازمانی عامل مهمی در افزایش اثربخشی امنیت سیستم‌های اطلاعات است. لذا سازمان‌ها باید به افزایش رفتارهای شهروندی سازمانی در قالب رفتارهای وظیفه‌شناسی، جوانمردی، نوع‌دوستی و ادب اهتمام ورزند.

همان‌طور که نتایج تحقیق نشان می‌دهد فرهنگ نوآوری مناسب در امنیت سیستم اطلاعات منجر به اثربخشی امنیت سیستم اطلاعات در شهرداری‌ها می‌شود؛ بنابراین شهرداری باید به بروز و ظهور نمادهای فرهنگی از جمله ارتباطات درون‌سازمانی قوی، داستان‌سرایی در زمینه امنیت سیستم‌های اطلاعاتی، برگزاری گفتمان‌های رسمی و غیررسمی در این زمینه، حمایت‌های ضمنی و صریح مدیران از مباحث امنیت سیستم‌های اطلاعاتی و استفاده نمادهای فیزیکی که اعضای سازمان را به اهمیت موضوع امنیت سیستم‌های اطلاعاتی، توجه نماید. به جهت برنامه‌ریزی برای ایجاد فرهنگ نوآورانه امنیت سیستم‌های اطلاعاتی به‌عنوان پایه و اساس امنیت سیستم اطلاعات اثربخش در شهرداری‌ها، تجمیع سیاست‌های نوآوری امنیت IS و مصنوعات فرهنگی سازمان می‌تواند راهگشا باشد. جهت ایجاد نوآوری در امنیت سیستم‌های اطلاعاتی، سازمان تلاش می‌کند تا فرهنگ نوآورانه امنیت شامل یک فرهنگ امنیتی اطلاعات را ایجاد نماید. مفاهیم فرهنگی، ارزش‌ها و باورهای مشترک از طریق ارتباطات رسمی و غیررسمی و گفتمان روزمره ایجاد می‌شود؛ بنابراین، برای تقویت فرهنگ نوآورانه امنیت سیستم اطلاعات ضروری است که گفتمان و ارتباطات در مورد اهمیت امنیت اطلاعات و نوآوری امنیت سیستم‌های اطلاعاتی تسهیل گردد. از سوی دیگر این گفتمان‌ها رفتار شهروندی سازمانی را در کارکنان تقویت می‌نماید (هوانگ و چوی، ۲۰۱۷). همچنین ممکن است کارکنان

محدودیت‌های حاصل از الزامات امنیت و تلاش‌های سازمان در جهت ایجاد این الزامات را به‌عنوان موانع و بروکراسی اداری درک کنند و رفتارهای ضد شهروندی از خود بروز دهند؛ بنابراین نیاز است با کارکنان ارتباط برقرار شود تا در مورد اهمیت امنیت سیستم‌های اطلاعاتی و مسائل مربوط به حریم خصوصی آگاهی یابند و دیدگاهی مثبت در این زمینه پیدا کنند (لارسون و گرونلاند[1]، ۲۰۱۶)

1. Larsson & Grönlund

منابع

نعمتیان، سیدمحمد .(۱۳۹۴). جایگاه واهمیت امنیت اطلاعات در شهرداری الکترونیک. *دوماهنامه شهرنگار*، شماره ۷۰-۷۱.

مشبکی اصفهانی، اصغر؛ خدامی سهیلا و تقوی شوازی، الهه .(۱۳۸۹). نظریه نهادی نوین تلفیقی و نقش آن در کسب مزیت رقابتی. پژوهشنامه *مدیریت اجرایی*، ۱۰(۱). ۱۷۴-۱۴۹

وظیفه، زهرا؛ مهدی، محمد و وکیلی، نادیا .(۱۳۹۷). الگوی امکان‌سنجی و استقرار اثربخش سیستم مدیریت امنیت اطلاعات بر مبنای روش فراترکیب. *مطالعات مدیریت کسب‌وکار هوشمند ۷*(۲۶)،۹۹-۷۱.

Ashworth, R., Boyne, G. & Delbrige, R. (2009). Escape from the iron cage? Organizational change and isomorphic pressures in the public sector. *J. Public Adm. Res. Theory*, 19, 165–187.

Bjorck, F. (2004). Institutional Theory: A New Perspective for Research into IS/IT Security in Organisations. *In Proceedings of the 37th Hawaii International Conference on System Sciences*, Big Island, Hawaii, 5–8 January.

Bulgurcu, B., Cavusoglu, H., Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. (2010). *MIS Q*. 34, 523–548

Bateman, T. & Organ, D. (1983). "Job Satisfaction And The Good Soldier: The Relationship Between Affect And Employee Citizenship", *Academy Of Management Journal*, 26(4).

Bergström, O., Styhre, A., Thilander, P. (2014). Paradoxifying organizational change: Cynicism and resistance in the Swedish armed forces. J. Chang. Manag, 14, 384–404

Band, S.R., Cappelli, D.M., Fischer, L.F., Moore, A.P., Shaw, E.D., Trzeciak, R.F. (2006). Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis, Technical Report CMU/SEI-2006-TR-026, ESC-TR-2006-091, Defense Technical Information Center: Fort Belvoir, VA, USA

Choi, M., Lee, J., Hwang, K. (2018). Information Systems Security (ISS) of E-Government for Sustainability: A Dual Path Model of ISS Influenced by Institutional Isomorphism. Sustainability, 10, 1555.

Coursey, D., Norris, D.F.(2008). Models of E-government: Are they correct? An empirical assessment. Public Adm. Rev. 68, 523–536

Currie, W.L. (2012). Institutional isomorphism and change: The national programme for IT—10 years on. J. Inf. Technol. 27, 236–248.

Dalal, R.S. (2005). A meta-analysis of the relationship between organizational citizenship behavior and counterproductive work behavior. Am. Psychol. Assoc. 2005, 90, 1241–1255. [CrossRef] [PubMed]

DiMaggio, P.J., Powell, W.W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. Am. Sociol. Rev. 1983, 48, 147–160

Evans, W.R., Novicevic, M.M. (2010). Legitimacy of HRM practices: Managerial perceptions of economic and normative value. J. Appl. Manag. Entrep. 15, 13–27

Feng, N., Wang, H.J., Li, M. (2014). A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. Inf. Sci. 25

Hagen, J.M., Albrechtsen, E., Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. Inf. Manag. Secur. 16, 377–397.

Hill, L.B. Pemberton, J.M. (1995). Information security: An overview and resource guide for information managers. Rec. Manag. Q., 29, 14–24

Hsieh, P. J. (2016). An empirical investigation of patients' acceptance and resistance toward the health cloud: The dual factor perspective. Computers in Human Behavior, 63, 959-969

Hu, Q., Hart, P., Cooke, D. (2007). The role of external and internal influences on information systems security—A neo-institutional perspective. J. Strateg. Inf. Syst. 2007, 16, 153–172

Hu, Q., Hart, P., Cooke, D. (2006). The Role of External Influences on Organizational Information Security Practices: An Institutional Perspective. In Proceedings of the Annual Hawaii International Conference on System Sciences, Kauai, Hawaii, 4–7 January, Volume 6, pp. 1–10.

Hwang, K., & Choi, M. (2017). Effects of innovation-supportive culture and organizational citizenship behavior on e-government information system security stemming from mimetic isomorphism.Government Information Quarterly, 34(2), 183–198

Joshi, K.(1991). A model of users' perspective on change: The case of information systems technology implementation. MIS Q., 15, 229–242

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), 37–60.

Ke, W., Wei, K.K. (2008). Organizational culture and leadership in ERP implementation. Decis. Support Syst. 45, 208–218.

Kokolakis S.A. Demopoulos A.J. Kiountouzis E.A. (2000). The use of business process modelling in information systems security analysis

and design", Information Management & Computer Security, Vol. 8 Iss 3 pp. 107 – 116

Kotter, J.P. (2007). Leading change: Why transformation efforts fail. Harv. Bus. Rev, 85, 96–103.

Lavy, S., & Littman-Ovadia, H. (2017). My Better Self: Using Strengths at Work and Work Productivity, Organizational Citizenship Behavior, and Satisfaction. Journal of Career Development, 44(2), 95–109.

Leiter, J. (2005). Structural isomorphism in Australian nonprofit organizations. Int. J. Volunt. Nonprofit Org, 16, 1–31

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

Markus, M.L (1983). Power, politics, and MIS implementation. Commun. ACM, 26, 430–444

Martinko, M.J., Gundlach, M.J., Douglas, S.C. (2002). Toward an integrative theory of counterproductive workplace behavior: A causal reasoning perspective. Int. J. Sel. Assess. 10, 36–50

Marcus, B., Schuler, H. (2004). Antecedents of counterproductive behavior at work: A general perspective. J. Appl. Psychol. 89, 647–660

Merhi, M.I., & Ahluwalia, P. (2015). Top management can lower resistance toward information security compliance. Proceedings of International Conference on Information Systems, Fort Worth, Texas.

National Security Institute. (2009). Cyber Security: Keeping Up with the Threat, National Security Institute: Medway, MA, USA, 6, 57–73.

Nazareth, D.L., Choi, J. (2015). A system dynamics model for information security management. Inf. Manag.52, 123–134

Nikrerk J.F. and Solms, Van.(2017). Information security culture: a management perspective. Computer & security, 5, 142-144.

Organ, D.W. (1988). Organizational Citizenship Behavior: The Good Soldier Syndrome, Lexington Books/D. C. Heath and Co.: Lexington, MA, USA

PricewaterhouseCoopers. (2013). Key Findings from the 2013 US State of Cybercrime Survey, PricewaterhouseCoopers: Delaware, DE, USA,

Pavlou, P.A., Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. MIS Q. 30, 115–143.54.

Reichers, A.E., Wanous, J.P., Austin, J.T. (1997). Understanding and managing cynicism about organizational change. Acad. Manag. Exec. 11, 48–59.

Sen, S., & Samanta, S. (2014). Information security.International Journal of InnovativeResearch in Technology, 1(11), 224–231.

Seo, M., Creed, W.D. (2002). Institutional contradictions, praxis, and institutional change: A dialectical perspective. Acad. Manag. Rev. 2002, 27, 222–247.

Scott, W.R. Institutions and Organizations, 2nd ed., Sage: Thousand Oaks, CA, USA, 2001

Sun, P.L., Ku, C.Y., Shih, D.H. (2015). An implementation framework for E-government 2.0. Telemat. Inform, 32, 504–520

Sharma, U., Lawrence, S., Lowe, A. (2010). Institutional contradiction and management control innovation: A field study of total quality management practices in a privatized telecommunication company. Manag. Account. Res 21, 251–264

Turban E. Leidner, McLean E. Wetherbe J.(2018), Information technology for management, New York: John Willy and Sons.

Turel, Ofir & Xu, Zhengchuan & Guo, Ken. (2017). Organizational Citizenship Behavior Regarding Security: Leadership Approach Perspective. Journal of Computer Information Systems. 1-15. 10.1080/08874417.2017.1400928.

Vahidi, A, kakavand, S, Tarokh, M. (2014). The influence of Organizational Citizenship Behavior on Information Security Behaviors. International Journal of Information and Communication Technology Research, March, Volume 4 No. 3

Wanous, J.P., Reichers, A.E., Austin, J.T. (2000). Cynicism about organizational change measurement, antecedents, and correlates. Group Org. Manag, 25, 132–153

Waring, B. (2009). Displaced Pride: Attacking Cynicism at the United States Air Force Academy. A Research Report, Air Command and Staff College Air University, Maxwell Air Force Base: Montgomery, AL, USA

Yang, Jun & Treadway, Darren. (2018). A Social Influence Interpretation of Workplace Ostracism and Counterproductive Work Behavior. Journal of Business Ethics. 148.

Yen, H.R., Li, E.Y., Niehoff, B.P. (2008). Do organizational citizenship behaviors lead to information system success? Testing the mediation effects of integration climate and project management. Inf. Manag. 45, 394–402.