نشریه علمی مطالعات مدیریت کسب و کار هوشمند- سال نهم ـ شماره ۳۴ـ زمستان ۱۳۹۹
مقاله پژوهشی/ صفحات ۲۴۶- ۲۱۵

Doi: 10.22054/IMS.2020.52669.1735

مزایا، ملاحظات و راهکارها تأمین امنیت گذرگاه تبادل اطلاعات دولت جمهوری اسلامی ایران

رضا یوسفی زنوز *
سید سجاد نجفی اصفهانی **
ابراهیم کولیوند ***

چکیده

بسترسازی و توسعه دولت الکترونیک درعین‌حال که می‌تواند موجب بهبود امنیت کشور و مبارزه با فساد باشد، از سوی دیگر می‌تواند خود بستری برای جرائم و فسادهای جدید و حتی تسهیل‌کننده فسادهای قبل باشد. این پژوهش با هدف شناسایی و اولویت‌بندی الزامات امنیتی درگاه تبادل اطلاعات دولت (GSB) به‌عنوان یکی از الگوهای دولت الکترونیک انجام شد. در این راستا پس از بررسی کتابخانه‌ای، مصاحبه‌های اختصاصی با دستگاه‌های ذی‌ربط انجام شد و سپس با تحلیل محتوای مصاحبه‌ها و دیگر منابع موجود، نیازمندی‌های امنیتی بازیگران امنیت فناوری اطلاعات کشور راجع به این درگاه، پالایش شد. در این مرحله و بر اساس پرسشنامه تحقیق، سه دسته نیازمندی راهبردی، فنی و تأثیر روی امنیت ملی، شناسایی شد. نیازمندی‌های راهبردی مواردی مثل تشکیل کمیته امنیت GSB، تنظیم لوایح و قوانین مورد نیاز و نظارت بر اجرای صحیح الزامات امنیتی شناسایی هستند. در مرحله بعد، به‌وسیله مدل کانو و ابزار QFD نیازمندی‌ها تحلیل و اولویت‌بندی شده و همچنین ارتباط بین نیازمندی‌ها و الزامات امنیتی مشخص شد. نتایج این پژوهش نشان داد که روش GSB در مقایسه با روش‌های P2P و روش تبادل اطلاعات کاغذی، در تمامی نیازمندی‌های امنیتی به‌جز وجود «سند الزامات امنیتی» ارجحیت دارد.

کلید واژگان: درگاه تبادل اطلاعات دولت، دولت الکترونیک، امنیت اطلاعات، مدل کانو، گسترش عملکرد کیفیت (QFD).

---

* عضو هیئت‌علمی، گروه مدیریت عملیات و فناوری اطلاعات، دانشکده مدیریت، دانشگاه خوارزمی، تهران، ایران.
(نویسنده مسئول) reza.zenouz@gmail.com

** کارشناسی ارشد، مدیریت استراتژیک، دانشکده مدیریت، دانشگاه خوارزمی، تهران، ایران.

*** عضو هیئت‌علمی، گروه مهندسی فناوری اطلاعات، دانشگاه پیام نور، تهران، ایران.

تاریخ دریافت:۱۳۹۹/۰۳/۱۱ **تاریخ پذیرش:۱۳۹۹/۰۸/۲۰**

مقدمه

فساد، عبارت است از «سوءاستفاده از اختیارات دولتی برای منافع شخصی یا گروهی» که اثرات منفی بر رشد تولید ناخالص داخلی، نرخ بیکاری و اعتبار کشور داشته و باعث کاهش میزان سرمایه‌گذاری خارجی می‌شود (هادوی نژاد و جاوید، ۱۳۹۳). مبارزه با فساد، بسیار پیچیده و دشوار است. یکی از راه‌حل‌های ممکن برای کاهش فساد، پیاده‌سازی دولت الکترونیک است؛ که این امر نیز با کاهش تعامل میان ادارات و مردم میسر می‌شود (نزاکووا و لینهارتورا[1]، ۲۰۱۲). ورود به عصر فناوری اطلاعات و ارتباطات، چالش‌های فراوانی را فرا روی جوامع بشری گسترده است (قناد، ۱۳۹۱) که لازم است متناسب با این چالش‌ها، ملاحظات امنیتی جدیدی را در نظر داشته و به کار گرفت (شهبازی نیا و عبداللهی، ۱۳۸۸). در کنار فواید بسیاری که مکانیزه شدن فرایندها در عصر ارتباطات به وجود آورده است، این پدیده همچون هر پدیده دیگری موجبات سوءاستفاده برخی را نیز فراهم نموده است (گرایلی، ۱۳۸۹). این موضوع در پژوهش‌های دیگری همچون (موسی و همکاران[2]، ۲۰۱۲؛ الکسوپولوس و همکاران[3]،۲۰۰۷) نیز بررسی شده است. با وجود اهمیتی که اشتراک‌گذاری اطلاعات دولت-دولت[4] در عملیات دولت دارد، هنوز این موضوع به‌صورت چالشی برای متخصصان فناوری اطلاعات در سراسر جهان وجود دارد (فان و همکاران[5]، ۲۰۱۴).

بر اساس بند «ب» ماده ۴۶ قانون برنامه پنجم توسعه بند و «ث» ماده ۶۷ قانون برنامه ششم توسعه جمهوری اسلامی ایران، مرکز ملی تبادل اطلاعات باید برای به اشتراک‌گذاری خدمات الکترونیکی بین دستگاهی در بستر شبکه ملی اطلاعات ایجاد شود و کلیه دستگاه‌های اجرایی کشور موظف‌اند امکان تبادل الکترونیکی اطلاعات و پاسخگویی الکترونیکی به استعلام‌ها را طبق این قانون به‌صورت رایگان فراهم کنند.

1. Knezackova & Linhartora
2. Musa et al.
3. Alexopoulos et al.
4. Government to Government (G2G)
5. Fan et al.

اما با ورود به این عرصه جدید، همان‌طور که ایران زاده و داودی (۱۳۹۱) نشان داده‌اند، فساد نمی‌رودتغییر ماهیت نمی دهد و همچنان وجود دارد؛ بنابراین، باید ملاحظات امنیتی متناسب با چالش‌های جدیدی که پیرامون جعل اسناد با تعریف جدید خودش در این عرصه جدید به وجود می‌آید نیز موردتوجه و پیش‌بینی قرار گیرد. با توجه به موارد پیش‌گفته، در این پژوهش قصد داریم تا مزایا، الزامات امنیتی و راهکارهای تأمین امنیت درگاه خدمات دولت یا GSB[1] را مورد بررسی قرار دهیم. همچنین لازم به ذکر است که چارچوب مفهومی که برای پیشبرد این پژوهش در نظر گرفته شده است، دیدگاه مشتری محور گسترش تابع کیفیت[2] است.

مروری بر مبانی نظری پژوهش

دولت الکترونیک و الگوهای آن

دولت الکترونیک مفهومی عام است و شامل این موارد است:G2C یا تعامل میان دولت و شهروندان، G2G یا تعامل میان سازمان‌های دولتی، G2B یا تعامل میان سازمان‌های دولتی و کسب‌وکارها، G2E یا تعامل میان دولت و کارمندان دولت (فرهادی نژاد، ۱۳۸۵). در این پژوهش روی الگوی دولت-دولت و شکل خاص آن یعنی درگاه تبادل اطلاعات دولت و ویژگی‌های امنیتی آن متمرکز شده است.

امنیت اطلاعات

استاندارد مدیریت امنیت اطلاعات

استاندارد ملی ISIRI-ISO/IEC 27001 که برای ایجاد، پیاده‌سازی، اجرا، پایش، بازنگری و نگهداری و بهبود سیستم مدیریت امینت اطلاعات سازمان‌ها به وجود آمد، دیدگاه فرآیندی دارد. این استاندارد ملی، بر اساس استاندارد بین‌المللی ISO/IEC 27001:2005 تدوین شده است و معادل آن به زبان فارسی است. صرف‌نظر از روشی که این استاندارد ملی برای مدیریت امنیت اطلاعات سازمان در پیش گرفته است، یک سری الزامات یا ملاحظات امنیتی از پیوست

1. Government Service Bus
2. Quality Function Deployment

الف این استاندارد با عنوان «اهداف کنترلی و کنترل‌ها» احصاء شده است. تحلیل این ملاحظات توسط خبرگان بعد الزامات یا HOW را در ماتریس خانه‌های کیفیت می‌سازند.

طرح امن سازی افتا

بر اساس ماده ۲۳۱ قانون پنجم توسعه به‌منظور ارتقاء سطح حفاظت از اطلاعات رایانه‌ای و امنیت فناوری‌ها و اجرای سند امنیت فضای تبادل اطلاعات، کلیه دستگاه‌های دارای زیرساخت‌های حیاتی موظف‌اند در چارچوب سند امنیت فضای تبادل اطلاعات (افتا) امنیت فضای تبادل اطلاعات خود را ارتقاء بخشند و نسبت به اجرای دستورالعمل‌های و استانداردهای افتا اقدام نمایند. یکی از مأموریت‌های راهبردی این مرکز، تدوین طرح ایمن‌سازی زیرساخت‌های حیاتی و نظارت در اجرای طرح است. طرح امن سازی زیرساخت های حیاتی در قبال حملات سایبری، از بخش‌های مختلفی تشکیل شده است کهسازمان‌ها می‌شود

قسمت «الزامات طرح امن سازی» این سند، متناسب با این بخش می باشد که از آن به عنوان یکی از مبانی نظری این پژوهش بهره برده شده است.

پیشینه پژوهش

بهشتی نیا و وزیری (۱۳۹۴) در پژوهش خود به مدل‌سازی فرآیند ارائه خدمات پلیس، با استفاده از روش‌های QFD و تحلیل سلسله مراتبی و مسئله کوله‌پشتی با رویکرد فازی پرداخت. در این پژوهش، ابتدا انتظارات مشتریان از خدمات پلیس شناسایی شده و پس از تعیین میزان اهمیت آن‌ها با استفاده از روش تحلیل سلسله مراتبی گروهیفازی، آن ها را در سطرهای خانه کیفیت قرار داده است. فرآیندهای اصلی پلیس نیز به‌عنوان الزامات فنی در ستون‌های خانه کیفیت جایگذاری شده است و سپس بر اساس مدل کوله‌پشتی، اولویت‌بندی اقدامات اجرایی به‌منظور افزایش کیفیت خدمات پلیس ارائه می شود. درور و همکاران[1] (۲۰۱۴) از ابزار QFD برای طراحی ویژگی‌های امنیتی در ارتباط با حملات تروریستی و مجرمانه به سازمان‌ها مخصوصاً هتل‌ها بهره گرفتند. یوسفی زنوز (۱۳۹۴) در پژوهش خود با عنوان «ارائه مدلی جهت

1. Dror et al.

اولویت‌بندی ریسک‌های امنیت اطلاعات سازمانی با استفاده از تحلیل سلسله مراتبی فازی و شبکه بیزین در صنعت بانکداری» به اولویت‌بندی ریسک‌های امنیت اطلاعات سازمانی، به‌منظور ارائه راهکاری برای ارتقا وضعیت امنیت اطلاعات سازمانی پرداخته است. در فرآیند ارزیابی ریسک، شدت اثر ریسک‌ها با استفاده از تحلیل سلسله مراتبی فازی و احتمال آن‌ها با استفاده از شبکه بیزین، محاسبه شده و سرانجام ریسک‌ها اولویت‌بندی شده‌اند. یافته‌های این پژوهش نشان داد که در سازمان مورد بررسی، ریسک عدم آگاهی و عدم ارائه آموزش‌های مناسب در حوزه امنیت اطلاعات، بالاترین اولویت و بیشترین نیاز به توجه را دارد. در این مقاله از ساختار استاندارد ISIRI-ISO/IEC 27001 به‌عنوان چارچوب اولیه برای شناسایی ریسک‌های امنیتی استفاده شده است.

اصغرنیا (۱۳۸۸) در پژوهش خود، روش‌های کنترل فساد اداری را مورد بررسی قرار داد و عنوان کرد که این روش‌ها عبارت‌اند از: کاهش تقاضا برای خدمات اداری، افزایش هزینه‌های ارائه خدمات فساد آمیز برای کارکنان فاسد و افزایش احتمال کشف و دستگیری عاملان فاسد.

هادوی نژاد و جاوید (۱۳۹۳) در پژوهش خود به بررسی رابطه بین متغیر فناوری اطلاعات با فساد اداری که شامل فساد مالی، فساد رفتارهای اداری و فساد قانونی است، با حضور متغیر تعدیل گر وجدان کاری پرداختند. این پژوهش نشان داد که فناوری اطلاعات با فساد اداری و به دنبال آن با فساد مالی، رفتارهای اداری و فساد قانونی، رابطه منفی معناداری دارد.

دانایی‌فرد (۱۳۸۳) در پژوهش خود، به نقد یکی از دیدگاه‌های اندیشمندان دولتی برای مدیریت فساد به نام «دیدگاه زندان تمام دید» پرداخته است. بر اساس این دیدگاه، فناوری اطلاعات به مدیران این امکان را می‌دهد که همه فعالیت‌های پنهان و آشکار کارکنان خود را تحت نظر داشته و بدین ترتیب، فساد را پایش و نظارت کنند؛ اما در این پژوهش با ارائه چندین مثال به نقد دیدگاه فوق پرداخته و استنباط می‌شود که فناوری اطلاعات نه‌تنها اثر قابل‌توجهی بر مدیریت فساد ندارد، بلکه در برخی موارد خود فرصت‌های جدیدی را برای فساد ایجاد می‌کند؛ بنابراین برای استفاده از فناوری اطلاعات به‌عنوان ابزاری برای مبارزه با فساد، باید به عوامل دیگری نیز توجه کرد.

در پژوهش ایران زاده و داودی (۱۳۹۱) که بر اساس پژوهش (دانایی‌فرد، ۱۳۸۳) انجام شده است دیدگاه مدیریت شیشه‌ای که بر اساس آن فناوری اطلاعات، کلید اصلی کنترل فساد تصور می‌شود مورد بررسی و نقد قرار گرفته شده است. در این پژوهش نتیجه گرفته شد که فساد اداری پدیده‌ای است که ریشه در اوضاع‌واحوال سیاسی، فرهنگی و اقتصادی دارد و استقرار دولت الکترونیک به‌تنهایی نمی‌تواند فساد اداری را در بخش دولتی حذف کند.

لگزیان و همکاران (۱۳۹۲) در پژوهشی، چالش‌ها و عوامل تأثیرگذار بر نحوه و میزان اشتراک‌گذاری اطلاعات میان سازمان‌های دولتی را بررسی کرده‌اند. یافته‌های پژوهش بیانگر تأثیر بالای رهبری سطح بالا، ارتباط و تعامل دوجانبه، سازگاری، حمایت مدیریت عالی، هزینه‌های مالی، فرآیند امنیت، مزایا و ریسک‌های مورد انتظار بر میزان اشتراک اطلاعات میان سازمان‌های دولتی است؛ اما قوانین و سیاست‌ها، اعتماد بین سازمانی و قابلیت‌های فناوری اطلاعات تأثیر معناداری بر میزان اشتراک اطلاعات میان سازمان‌های دولتی نداشته است.

متفکر آزاد و همکاران (۱۳۹۲) پژوهشی خود،تأثیردر بین ۳۴ کشور منتخب عضو سازمان کنفرانس اسلامی طی سال‌های ۲۰۰۳ تا ۲۰۱۱ انجام داده اند که تاثیر دولت الکترونیکی بر فساد را بررسی کرده است. نتیجه این تحقیق نشان داد که تقویت دولت الکترونیکی، فساد اقتصادی موجود در کشورها را کاهش می‌دهد.مهرگان و همکاران (۱۳۹۴) نیز که روی ۷۷ کشور با درآمد متوسط طی دوره زمانی بین ۲۰۰۷ تا ۲۰۱۳ پژوهشی مشابه انجام داده‌اند، نشان دادند که با افزایش شاخص توسعه فناوری اطلاعات و ارتباطات و دو مؤلفه دسترسی و استفاده از آن، فساد اداری کاهش یافته است؛ اما مؤلفه مهارت شاخص توسعه فناوری اطلاعات و ارتباطات، اثر منفی روی سطح فساد اداری در کشورهای نمونه دارد. همچنین نتایج این تحقیق نشان می‌دهد، افزایش درآمد سرانه و دموکراسی، موجب کاهش فساد اداری می‌گردد.

بهبودی و همکاران (۱۳۹۶) در پژوهشی با عنوان «طراحی مدل تحلیل تفسیری-ساختاری علل مؤثر بر فساد اداری دولت الکترونیک در ایران» نشان دادند که شاخص‌های ویژگی‌های ساختاری شناسایی شده در بخش کیفی، شامل عدم وجود دانش کافی، فقدان

برنامه‌های اجرایی، عدم وجود حمایت‌های فنی، عدم بازخورد اطلاعات به تمام واحدها، به‌عنوان مهم‌ترین علل ایجاد فساد اداری در دولت الکترونیک محسوب می‌شوند.

پژوهش بیگدلی و همکاران[1] (۲۰۱۳) به دنبال ایجاد یک چارچوب مفهومی از عوامل مؤثر بر اشتراک اطلاعات الکترونیکی در الگوی G2G بوده است. این پژوهش نشان داد اشتراک اطلاعات الکترونیکی در سازمان‌های دولتی محلی متأثر از ترکیبی از عوامل محیطی، سازمانی، فرآیند کسب‌وکار و مسائل فنی و فنّاورانه است و این مورد نباید فقط از نظر فنّاورانه بررسی گردد.

در پژوهش کمال و همکاران[2] (۲۰۱۲) عوامل مؤثر بر اشتراک اطلاعات میان ادارات در دولت الکترونیکی مورد بررسی قرار گرفته است. سه حوزه عواملی که در مقاله شناسایی شده‌اند عبارت‌اند از عوامل فردی، عوامل سازمانی و عوامل فنّاورانه هستند.

در پژوهش گیل گارسیا و سایوگو[3] (۲۰۱۶) برخی عوامل مهم موفقیت طرح‌های همکاری‌های بین سازمانی و اشتراک اطلاعات طریق تحلیلی تجربی شناسایی و آزمون شد. نتایج نشان داد دو عامل زیرساخت فنی و مدیران پروژه به‌عنوان دو عامل مهم پیش‌بینی کننده موفقیت در طرح‌های اشتراک‌گذاری اطلاعات بین سازمانی می باشد.

پژوهش اکبولوت و همکاران[4] (۲۰۰۹) به دنبال فهم عوامل مؤثر بر اشتراک اطلاعات الکترونیکی سازمان‌های محلی بوده است نتایج این پژوهش نشان داد مجموعه‌ای از عوامل فنّاورانه، درون‌سازمانی و محیطی است که باعث ترفیع یا منع اشتراک اطلاعات الکترونیکی توسط سازمان‌های محلی می‌شود.

در مقاله پاتیل و پاتیل[5] (۲۰۰۸) به فساد یقه‌سفیدها و چگونگی مقابله و کنترل این فسادها به کمک دولت الکترونیک پرداخته شده است. محققین این پژوهش معتقدند دولت الکترونیک با دموکراتیک کردن اطلاعات، مؤثر ساختن طرح‌های دولتی و ایجاد شفافیت به کنترل این

1. Bigdeli et al.
2. Kamal et al.
3. Gil-Garcia & Sayogo
4. Akbulut et al.
1. Patil & Patil.

فسادها کمک می‌کند. این مقاله یک مقاله کیفی بوده است که در ابتدا با بررسی کتابخانه‌ای، به جرائم یقه‌سفیدها در حوزه‌های مختلف و در تخصص‌های مختلف در کشور هند اشاره می‌کند. در بخش بعدی، عوامل محرک یا انگیزاننده یقه‌سفیدها برای انجام جرم و فساد را دسته‌بندی می‌کند و نهایتا نقش دولت الکترونیک را در کاهش و کنترل جرم یقه‌سفیدها تبیین می‌کند که شامل این موارد است: دولت الکترونیک با توجه به دسترسی به پایگاه داده‌های مختلف و تجارب بین آن‌ها، به‌مثابه یک مرکز تصمیم‌گیری مؤثر و قابل‌اعتماد و مرکزی برای کشف فسادها با ابزار است و دولت الکترونیک می‌تواند به نظارت و مانیتورینگ بهتر پروژه‌ها و قراردادها برای به حداقل رساندن هزینه و زمان و اجرای مؤثر آن‌ها کمک کند.

در پژوهش میستری و جلال[1] (۲۰۱۲)، رابطه بین دولت الکترونیک و فساد در کشورهای درحال‌توسعه و توسعه‌نیافته بررسی شده است. نتایج این پژوهش نشان داد با استفاده از دولت الکترونیک، فساد کاهش می‌یابد. همچنین نتایج نشان داد که تأثیر دولت الکترونیک در کشورهای درحال‌توسعه برای یک دوره زمانی هفت‌ساله ۲۰۰۳-۲۰۱۰ بیشتر از کشورهای توسعه‌یافته است.

در مطالعات (ماچووا و همکاران[2]، ۲۰۱۸؛ ازیانی و آسوگوا[3]، ۲۰۱۸؛ نزاکووا و لینهارتورا[4]، ۲۰۱۲؛ سوکیم و همکاران[5]، ۲۰۱۵؛ لوپو و لازار[6]، ۲۰۱۵) تأثیر دولت الکترونیک روی فساد یا رابطه این دو در زمینه‌ها و حوزه‌های مختلف بررسی شده است.می‌توانهرچندمی‌تواندپیاده‌سازیبه‌تنهاییتضمین‌کننده می‌تواندزمینه‌سازجرائمکلاه‌برداری

نوآوری پژوهش

اکثر مقالات و کارهای پژوهشی در این حوزه (ایران زاده و داودی، ۱۳۹۱، لگزیان و همکاران، ۱۳۹۲؛ محسنی، ۱۳۹۲؛ مهرگان و همکاران، ۱۳۹۴؛ متفکر آزاد و همکاران، ۱۳۹۲؛ هادوی نژاد

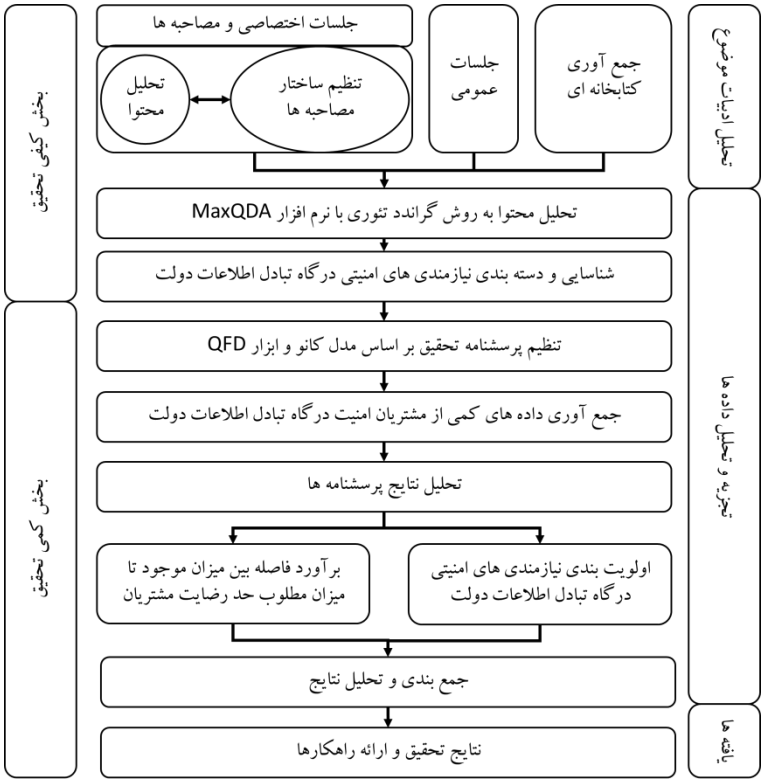
2. Mistry & Jalal
3. Machova et al.
4. Ezeani & Asogwa
5. Knezackova & Linhartora
6. Sokim et al.
7. Lupu & Lazar

و جاوید، ۱۳۹۳؛ اصغر نیا، ۱۳۸۸؛ موسی و همکاران، ۲۰۱۲؛ اکبولوت و همکاران، ۲۰۰۹؛ پاتیل و پاتیل، ۲۰۰۸؛ نزاکووا و لینهارتورا، ۲۰۱۲) معطوف به دولت الکترونیک به طور عام و پرداختن به شاخص‌های بالادستی و بررسی تأثیر و رابطه دولت الکترونیک روی فساد یا کلاه‌برداری بوده است. نیازهای امنیتی در حوزه دولت الکترونیک و مخصوصاً GSB مورد بررسی قرار نگرفته است. اکثر پژوهش‌های پیشین به بررسی شاخص‌های منتشرشده از سوی دولت‌ها بسنده کرده‌اند. نوآوری‌های این پژوهش در قالب موارد زیر قابل‌طرح است: اولویت‌بندی ویژگی‌های امنیتی درگاه تبادل اطلاعات دولت (دولت الکترونیک)، نگاه به ویژگی‌های امنیتی از دیدگاه مشتری محور، استفاده از ابزار کانو برای شناسایی و دسته‌بندی نیازهای امنیتی و همچنین بهره‌گیری از QFD برای حصول راهکارهای تأمین امنیت GSB و ارتباط بین الزامات و نیازمندی‌های امنیتی.

روش‌شناسی پژوهش

این تحقیق از منظر هدف، کاربردی است. همچنین از منظر شیوه گردآوری داده‌ها، از نوع بررسی میدانی و به‌طورکلی از نوع پیمایشی است.

این پژوهش از نوع آمیخته بوده و از دو بخش کیفی و کمی تشکیل شده است. ابتدا با بررسی ادبیات موضوع و جلسات مصاحبه، نیازمندی‌های امنیتی سیستم استخراج شد. سپس با بهره‌گیری از مدل کانو این نیازمندی‌ها، دسته‌بندی و اولویت‌بندی شد. در انتها با بهره‌گیری از ماتریس‌های خانه کیفیت ارتباط بین نیازمندی‌های امنیتی و الزامات امنیتی GSB برقرارشده و درنهایت راهکارهای ارتقاء امنیت استخراج شد. فرآیند اجرای تحقیق در شکل ۱ نشان داده شده است.



شکل ۱: فرآیند اجرایی پژوهش

جامعه آماری

جامعه آماری این پژوهش، مشتریان امنیت درگاه تبادل اطلاعات دولت یعنی نهادها و سازمان‌هایی هستند که راجع به امنیت این سامانه، ملاحظ دارند. در یک بررسی اولیه مشتریان امنیت درگاه تبادل اطلاعات دولت به‌خوبی مشخص شده اند. این مشتریان مدیران ارشد و عالی مرتبط با امنیت دستگاه‌های دولتی و حاکمیتی هستند. در بخش کیفی تحقیق به دلیل مصاحبه با خبرگان، نمونه‌گیری انجام نشده است. نمونه‌گیری قسمت کمی تحقیق، نمونه‌گیری تصادفی طبقه‌بندی شده است، چون از هرکدام از مدیران سازمان‌ها و دستگاه‌های دولتی مختلف، فرد یا افرادی برای پاسخگویی به سؤالات پرسشنامه‌ها به‌تصادف انتخاب شده‌اند.

روش گردآوری داده‌ها

مشاهده: محقق شخصاً در جلسات متعدد مرتبط با موضوع پژوهش حضور داشته و موضوع را از نزدیک مورد بررسی و مطالعه قرار داده است.

جمع‌آوری کتابخانه‌ای: در ابتدای پژوهش بر اساس مطالعات و پژوهش‌های داخلی و بین‌المللی در حوزه دولت الکترونیک و فناوری اطلاعات، بررسی اسناد و مدارک و استاندارد ISIRI-ISO/IEC 27001 و اسناد طرح امن سازی افتای ریاست جمهوری مزایا و ملاحظات امنیتی دولت الکترونیک جمع‌آوری گردید.

جلسات اختصاصی و مصاحبه‌ها: جلساتی با خبرگان و متصدیان امنیت درگاه تبادل اطلاعات دولت برگزار گردید که به مصاحبه‌های دقیق‌تر و موشکافانه‌تری نسبت به ابعاد پنهان موضوع پرداخته شد. چارچوب مصاحبه‌ها باز در نظر گرفته شد ولی برای پیشبرد بحث در مصاحبه‌ها، داده‌های اولیه تحقیق که جمع‌آوری شده بود اساس مصاحبه‌ها را شکل داد. در طول هر مصاحبه، یادداشت‌های گسترده‌ای از اظهارات مصاحبه‌شوندگان انجام گرفته است.

پرسشنامه: بررسی مقدماتی داده‌ها و مستندات افتا و استاندارد ISIRI-ISO/IEC 27001 و پژوهش‌های قبلی صورت گرفته در حوزه امنیت دولت الکترونیک باعث شد تا درک نزدیک و تقریباً کامل‌تری در مورد موضوع تحقیق ایجاد گردد که در تهیه پرسشنامه‌های این پژوهش بسیار کمک‌کننده بود. برای پالایش بیشتر پرسشنامه‌های طراحی‌شده، از نظرات خبرگان و همکاران پژوهش (اساتید محترم راهنما و مشاور) این پژوهش به‌صورت شفاهی دریافت شد و نظرات ایشان در پرسشنامه اعمال گردید. پرسشنامه‌ها بر اساس جداول مطرح‌شده در مدل کانو و جدول اول QFD تنظیم گردیده است.

روش تجزیه‌وتحلیل داده‌ها

مرحله تجزیه‌وتحلیل داده‌ها با شروع مصاحبه‌ها آغاز شد و بعد از پایان مصاحبه‌ها نیز ادامه داشت به این صورت که پس از انجام هر مصاحبه، بر اساس تحلیل محتوا و کدگذاری که روی مصاحبه انجام شد، نکات جدید در مصاحبه‌های بعدی به‌عنوان سؤال از مصاحبه‌شوندگان

پرسیده می‌شد و نظر ایشان نیز راجع به آن موضوع دریافت می‌شد. نتایج جمع‌آوری داده‌ها کیفی در نرم‌افزار MaxQDA وارد شدند تا به کمک این نرم‌افزار، تحلیل محتوای نهایی انجام شود.

تحلیل داده‌ها به‌صورت تکراری در طول پژوهش و دوران مصاحبه‌ها انجام شد. پس از هر مصاحبه، یادداشت‌های میدانی یا اسناد و نامه‌های جدیدی که در دسترس قرار می‌گرفت، مطالب مورد تحلیل قرار می‌گرفت و درصورتی‌که نیازمندی جدیدی شناخته می‌شد، به این لیست اضافه می‌شدند. مصاحبه‌ها بر همین اساس اصلاح و به‌روزرسانی می‌شدند تا نیازمندی‌های نوظهور در مصاحبه‌های بعدی موردتوجه قرار گیرند. در دور دوم تحلیل داده‌ها که پس از تکمیل همه مصاحبه‌ها انجام شد به رویکردی جامع‌تر رسیدیم. در طی این مرحله، انبوه تجزیه‌وتحلیل از مصاحبه‌های فردی، در کنار دیگر نیازمندی‌های شناسایی شده در مراحل قبلی بررسی قرار گرفته و تکامل یافت. بعد از رسیدن به یک لیست نیازمندی‌های امنیتی نهایی، برای اظهارنظر در اختیار همکاران پژوهش قرار گرفت تا نظر تخصصی و دیدگاه خودشان را راجع به این لیست بیان کنند. بعد از اعمال‌نظر ایشان لیست نهایی تدوین گردید.

در تحلیل نهایی، روند کدگذاری مجدد آغاز گردید. محتوای هر جمله یا پاراگراف از نزدیک مورد بررسی قرار گرفت. داده‌هایی که به موضوع پژوهش، یعنی نیازمندی‌های امنیتی درگاه تبادل اطلاعات دولت، بی‌ارتباط بودند، کنار گذاشته شدند، داده‌های دیگر کدگذاری شدند. این روند تا زمانی ادامه یافت که داده‌های جدید دیگر عوامل ناشناخته‌ای را آشکار نکردند و به اشباع نظری رسیدیم. هیچ‌یک از نیازمندی‌های مطرح‌شده در این مقطع از تحقیق حذف نشد و حتی نیازمندی‌هایی که تنها در یک مصاحبه به آن اشاره‌شده بود هم در لیست نیازمندی‌های امنیتی قرار گرفت.

کدگذاری اطلاعات در این پژوهش فقط به‌منظور احصای نیازمندی‌های امنیتی خبرگان و ایجاد پرسشنامه برای استفاده در قسمت کمی تحقیق است. بر اساس مفاهیم استخراج‌شده از تحلیل محتوا، پرسشنامه‌ای طراحی گردید که درواقع حلقه وصل بخش کمی و کیفی تحقیق است. قسمت کمی تحقیق و تحلیل داده‌ها با استفاده از ابزار QFD انجام شده است.

تجزیه‌وتحلیل داده‌ها

توصیف اطلاعات جمعیت‌شناسی پژوهش

بعد از تنظیم پرسشنامه‌ها، بین ۶۰ نفر از مدیران عالی و مدیران میانی دستگاه‌های مختلف دولتی و حاکمیتی توزیع گردید. پاسخ ۱۸ نفر از این خبرگان تا زمان تدوین این اوراق، دریافت گردید. پاسخ‌دهندگان ۹۵ درصد مرد و ۵ درصد زن بودند که از این تعداد ۹۵ درصد متأهل و ۵ درصد مجرد بودند. افراد بین ۳۰ تا ۴۰ سال، ۴۵ درصد از پاسخ‌دهندگان را در بر می‌گرفتند و افراد بین ۴۰ تا ۵۰ سال ۳۳ درصد و بالای ۵۰ سال ۲۲ درصد از پاسخ‌دهندگان بودند. ۱۷ درصد از افراد دارای مدرک کارشناسی، ۶۱ درصد کارشناسی ارشد و ۲۲ درصد دکتری داشتند. از نظر سابقه کاری در حوزه مدیریت/امنیت فناوری اطلاعات نیز ۳۳ درصد بیش از ده سال، ۵۰ درصد بیش از ۱۵ سال و ۱۷ درصد بیش از بیست سال سابقه فعالیت مستقیم در این حوزه داشتند.

تحلیل محتوایی داده‌ها

یادداشت‌برداری: یادداشت‌ها در تمام مراحل تحقیق از مصاحبه‌ها و دیگر منابع صورت می‌گرفت. مثالی از این یادداشت‌برداری‌ها مصاحبه‌ها به‌صورت زیر است:

جدول ۱: مثالی از یادداشت‌برداری از مصاحبه‌ها

استناد پذیری تبادل اطلاعات
موضوع بعدی استناد پذیری این سامانه است، نمی‌توان از قوانین و مقررات تخطی کرد، در خصوص GSB زمانی موضوع استناد پذیری را منع کرده بودند هرگونه ذخیره‌سازی اطلاعات، یعنی ما هیچ‌چیز نداشتیم که اطلاعاتی ذخیره بشود و یکی از تضمین‌هایی که بارها اعلام شده بود اینکه ما اصلاً هیچ کاری به ذخیره اطلاعات نداریم که چه کسی از چه کسی در چه تاریخی چه اطلاعاتی را گرفته است. فقط زیرساخت فنی را فراهم می‌کردیم ولی در محتوا ورود نداشتیم. سال گذشته شورای عالی فضای مجازی یک آیین‌نامه استعلامات ماده ۶۷ را ابلاغ کرد که در آنجا گفتند برای این‌که اگر بعد از استعلام در دعاوی نیاز شد که استناد بشود به فلان استعلام، سوابق آن وجود داشته باشد و سازمان فناوری اطلاعات باید سؤال‌کننده را در سوابق ذخیره کند.

کدگذاری داده‌ها: برای کدگذاری داده‌ها از نرم‌افزار MaxQDA بهره گرفته شد. تمامی ورودی‌های پژوهش ازجمله جمع‌آوری‌های کتابخانه‌ای، جلسات عمومی و جلسات اختصاصی و مصاحبه‌ها به تفکیک تایپ شده و در نرم‌افزار وارد شدند.

نتیجه این تحلیل محتوا، به سمع و نظر سه نفر از خبرگان حوزه امنیت فناوری اطلاعات (همکاران پژوهش) رسید و نظرات آن‌ها برای اصلاح، دسته‌بندی و مرتب کردن این مفاهیم و مقولات اعمال گردید و نتیجه نهایی به‌صورت جدول زیر قابل‌ارائه شد.

جدول ۲: مقوله‌های مختلف نیازمندی‌های امنیتی درگاه تبادل اطلاعات دولت

مقوله	مفهوم	واقعه	نیازمندی‌های مشتریان	شماره
نیازمندی‌های امنیتی درگاه تبادل اطلاعات دولت	راهبردی	طرح امن سازی	نیاز به تدوین سند الزامات امنیتی و ایجاد طرح امن سازی کلان و حکومتی	۱
			نیاز به تضمین اجرای صحیح و کامل طرح امن سازی	۲
			نیاز به تضمین امنیت از سمت سرویس گیرندگان مطابق طرح امن سازی	۳
			نیاز به تضمین امنیت پایگاه‌های داده سرویس‌دهندگان مطابق طرح امن سازی	۴
		حاکمیتی	نیاز به نظارت و ممیزی حاکمیتی روی امنیت و هماهنگی امنیت	۵
			نیاز به قوانین و مقررات و جرم انگاری و مسائل حقوقی	۶
	فنی	تضمین تداوم	نیاز به مدیریت حوادث و رویدادهای امنیت اطلاعات	۷
			نیاز به مدیریت آسیب‌پذیری‌های فنی	۸
			نیاز به تضمین تداوم کسب‌وکار و داشتن نسخه پشتیبان و نسخه حوادث امنیتی (disaster)	۹
			نیاز به تضمین تمامیت داده‌ها و عدم آسیب به محتوای داده‌ها	۱۰
		محرمانگی	نیاز به محرمانگی اطلاعات بین سرویس‌دهنده و سرویس گیرنده	۱۱
			نیاز به حفاظت فیزیکی اسناد بایگانی شده و پایگاه‌های داده در مقابل حملات فیزیکی	۱۲
			نیاز به ایزوله بودن شبکه‌های درون دولت و بیرون دولت مثل GSB و (PGSB)	۱۳
		تصدیق هویت	نیاز به سطح‌بندی دسترسی‌ها بر اساس سطح محرمانگی اطلاعات	۱۴

			نیاز به سطح‌بندی تصدیق هویت بر اساس حجم اطلاعات مورد دسترس	۱۵
		استناد پذیری	نیاز به استناد پذیری استعلام‌ها در مقاطع بعدی در دعاوی احتمالی	۱۶
		دسترس‌پذیری	نیاز به دسترسی سریع و آسان به اطلاعات	۱۷
		حریم شخصی	نیاز به حفظ حریم شخصی	۱۸
	تأثیر روی امنیت ملی	فراداده	نیاز به فراداده‌ها برای تحلیل‌های آماری به‌منظور برنامه‌ریزی و تصمیم‌گیری بهتر	۱۹
			نیاز به فراداده‌ها برای تحلیل‌های آماری به‌منظور کشف فساد اداری	۲۰
		مقایسه پذیری	نیاز به مقایسه پذیری پایگاه‌های داده مختلف به‌منظور خالص‌سازی اطلاعات با هدف بهبود برنامه‌ریزی و تصمیم‌گیری	۲۱
			نیاز به مقایسه پذیری مبادلات اطلاعات پایگاه‌های داده مختلف به‌منظور کشف فساد اداری	۲۲
		ترویج	نیاز به آگاه کردن و آموزش سرویس‌دهندگان و سرویس‌گیرندگان از مزایا و منافع پیوستن به این روش به‌منظور فراگیر کردن استفاده از آن	۲۳
			نیاز به ساده‌سازی فرآیندهای پیوستن به این روش برای سرویس‌دهندگان و سرویس‌گیرندگان	۲۴
			نیاز به اهرم فشار به دستگاه‌هایی که به دلیل فساد اداری تمایلی برای پیوستن به این روش ندارند	۲۵

تحلیل کمی داده‌ها

مدل کانو

در این تحقیق برای اولویت‌بندی و دسته‌بندی نیازمندی‌های امنیتی از مدل کانو بهره گرفته شد. در این راستا ابتدا حدود ارزیابی کانو را تشکیل می‌دهیم. پاسخ‌های موجود در جدول کانو بر اساس جدول مرجع آن دسته‌بندی می‌شوند (صفری، ۱۳۹۶).

در مدل کانو دسته‌بندی نیازمندی‌ها بر اساس احساس پاسخ‌دهنده‌ها نسبت به وجود یا عدم وجود هر نیازمندی، به سه دسته *انگیزشی، عملکردی و اساسی* صورت می‌گیرد. این پاسخ‌ها، در کنار میزان اهمیت و میزان رضایت مشتریان نسبت به هر نیازمندی ورودی‌های ماتریس QFD می‌باشند که در مرحله بعدی به آن می‌پردازیم.

یکی از روش‌های تحلیل پرسشنامه کانو، تحلیل پاسخ‌ها بر اساس بیشترین فراوانی به ازای هر پاسخ است (صفری، ۱۳۹۶). به‌این‌ترتیب، نیازمندی‌های انگیزشی و اساسی به‌صورت زیر شناسایی و دسته‌بندی شد.

جدول ۳: نیازمندی‌های انگیزشی

نیازمندی‌های انگیزشی	نیاز به دسترسی سریع و آسان به اطلاعات
	نیاز به فراداده‌ها برای تحلیل‌های آماری به‌منظور برنامه‌ریزی و تصمیم‌گیری بهتر
	نیاز به مقایسه پذیری پایگاه‌های داده مختلف به‌منظور خالص‌سازی اطلاعات با هدف بهبود برنامه‌ریزی و تصمیم‌گیری
	نیاز به مقایسه پذیری مبادلات اطلاعات پایگاه‌های داده مختلف به‌منظور کشف فساد اداری
	نیاز به آگاه کردن و آموزش سرویس‌دهندگان و سرویس‌گیرندگان از مزایا و منافع پیوستن به این روش به‌منظور فراگیر کردن استفاده از آن
	نیاز به ساده‌سازی فرآیندهای پیوستن به این روش برای سرویس‌دهندگان و سرویس‌گیرندگان

جدول ۴: نیازمندی‌های اساسی

نیازمندی‌های اساسی	نیاز به تدوین سند الزامات امنیتی و ایجاد طرح امن سازی کلان و حکومتی
	نیاز به تضمین اجرای صحیح و کامل طرح امن سازی
	نیاز به تضمین امنیت از سمت سرویس‌گیرندگان مطابق طرح امن سازی
	نیاز به تضمین امنیت پایگاه‌های داده سرویس‌دهندگان مطابق طرح امن سازی
	نیاز به نظارت و ممیزی حاکمیتی روی امنیت و هماهنگی امنیت
	نیاز به قوانین و مقررات و جرم انگاری و مسائل حقوقی
	نیاز به مدیریت حوادث و رویدادهای امنیت اطلاعات
	نیاز به مدیریت آسیب‌پذیری‌های فنی
	نیاز به تضمین تداوم کسب‌وکار و داشتن نسخه پشتیبان و نسخه حوادث امنیتی(disaster)
	نیاز تضمین تمامیت داده‌ها و عدم آسیب به محتوای داده‌ها

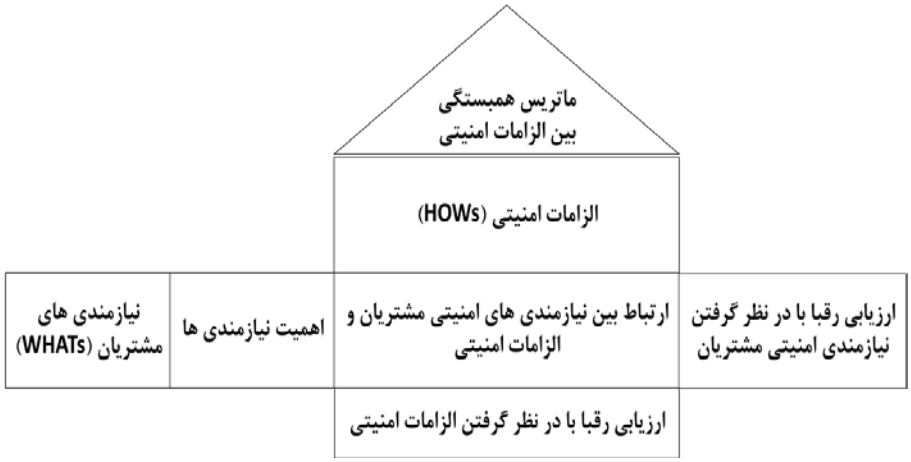
	نیاز به محرمانگی اطلاعات بین سرویس‌دهنده و سرویس‌گیرنده
	نیاز به حفاظت فیزیکی اسناد بایگانی شده و پایگاه‌های داده در مقابل حملات فیزیکی
	نیاز به ایزوله بودن شبکه‌های درون دولت و بیرون دولت مثل GSB و (PGSB)
	نیاز به سطح‌بندی دسترسی‌ها بر اساس سطح محرمانگی اطلاعات
	نیاز به سطح‌بندی تصدیق هویت بر اساس حجم اطلاعات مورد دسترس
	نیاز به استناد پذیری استعلام‌ها در مقاطع بعدی در دعاوی احتمالی
	نیاز به حفظ حریم شخصی
	نیاز به فراداده‌ها برای تحلیل‌های آماری به‌منظور کشف فساد اداری
	نیاز به اهرم فشار به دستگاه‌هایی که به دلیل فساد اداری تمایلی برای پیوستن به این روش ندارند

اهمیت و رضایت

یکی از روش‌های سامانمند شناسایی نیازها و خواسته‌های مشتریان، گسترش عملکرد کیفیت[1] یا QFD است. این ابزار به شناسایی کامل نیازها و خواسته‌های مشتریان می‌پردازد و درواقع به ترجمه این نیازها به ویژگی‌های محصول پرداخته و در ادامه به طراحی فرایندهای تولید محصول یا ارائه خدمت با توجه به خواسته مشتری و در راستای تأمین نیازهای وی می‌پردازد.

ماتریس خانه کیفیت، مورداستفاده در شکل ۲ ارائه شده است. اطلاعات لازم برای تکمیل ماتریس خانه کیفیت از طریق پرسشنامه‌های مربوطه گردآوری شد.

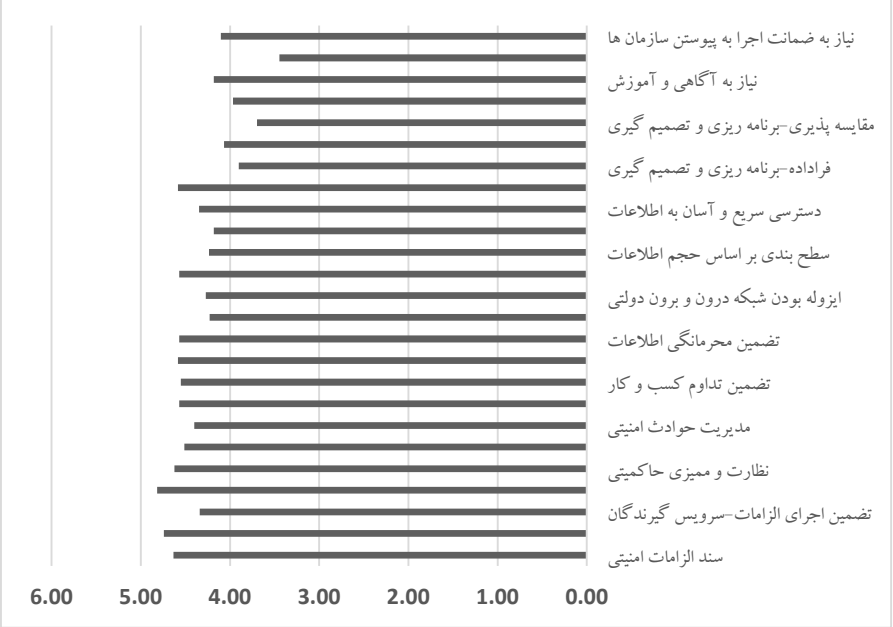
1. Quality Function Deployment



شکل ۲: معرفی جداول خانه کیفیت

تحلیل ماتریس برنامه‌ریزی با استفاده از نمودار

با استفاده از روابط حاکم بر جداول خانه کیفیت، وزن مطلق و وزن نسبی هر نیازمندی محاسبه شد. شکل ۳ میزان اهمیت نیازمندی‌ها را نشان می‌دهد. درواقع در این شکل پاسخ خام پرسشنامه به میزان اهمیت نیازمندی‌ها نمایش داده شده است. شکل‌های ۴ و ۵ و ۶ میزان رضایت پاسخ‌دهندگان در ابعاد مختلف از GSB در مقایسه با رقبا را نشان می‌دهند.



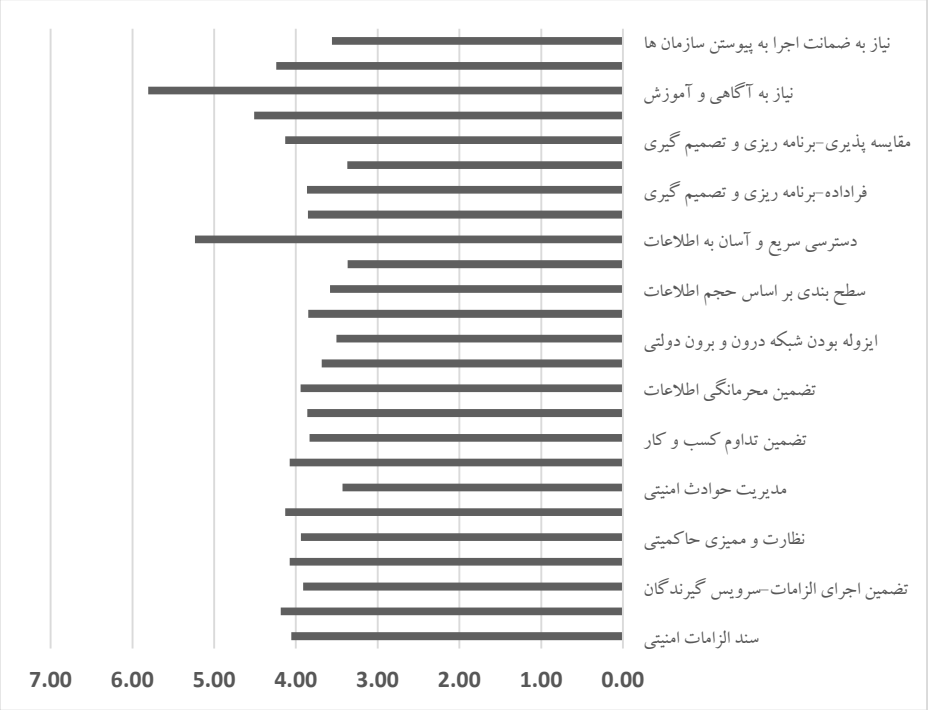
شکل ۳: میزان اهمیت نیازمندی‌ها

شکل ۴: میزان رضایت پاسخ‌دهندگان از امنیت GSB و دیگر روش‌ها (نیازمندی‌های راهبردی)

شکل ۵: میزان رضایت پاسخ‌دهندگان از امنیت GSB و دیگر روش‌ها (نیازمندی‌های فنی)

شکل ۶: میزان رضایت پاسخ‌دهندگان از امنیت GSB و دیگر روش‌ها (نیازمندی‌های تأثیر روی امنیت ملی)

بعد از واردکردن نتایج مدل کانو (انگیزشی، عملکردی، اساسی) به ترتیب با ضریب‌های ۱/۵، ۱/۲ و ۱ به‌عنوان ضریب تصحیح و همین‌طور نسبت بهبود (میزان فاصله با مقدار مطلوب) محاسبه شده است. این نتایج در شکل ۷ نشان داده شده است.



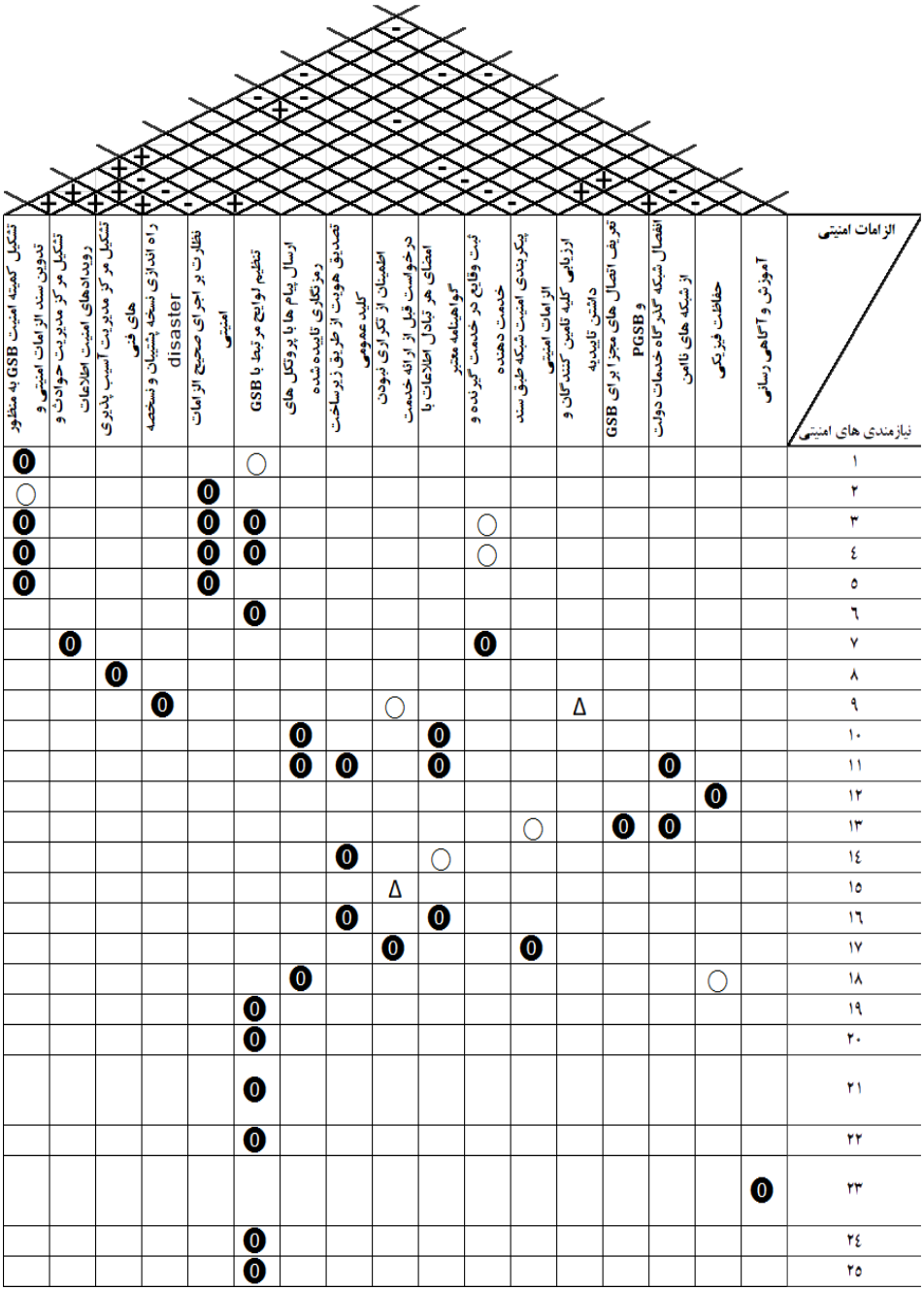
شکل ۷: مقایسه وزن نسبی نیازمندی‌های امنیتی با هم

تعیین الزامات امنیتی (چطورها- HOWs)

الزامات امنیتی توسط گروه QFD متشکل از محققان و خبرگان انتخاب‌شده از دو سازمان دولتی تعیین شد. با استفاده از «ماتریس روابط» و «ماتریس همبستگی» ارتباط نیازمندی امنیتی و الزامات امنیتی با کمک نمادهای زیر مشخص می‌شود. این ارتباطات در شکل ۸ نشان داده شده است.

جدول ۵: نمادهای مورداستفاده در جدول روابط و همبستگی

۱ = Δ (ضعیف)
۳ = ⓪ (متوسط)
۹ = ◎ (قوی)
+ همبستگی زیاد
− همبستگی کم



شکل ۸:ماتریس روابط و همبستگی

وزن الزامات امنیتی یا اهداف طراحی

با استفاده از روابط حاکم بر جداول خانه کیفیت، وزن مطلق و وزن نسبی هر الزام امنیتی محاسبه شده است که در شکل شماره ۹ نشان داده شده است.

شکل ۹: مقایسه وزن نسبی الزامات امنیتی با هم

بحث و نتیجه‌گیری

فساد در دولت، بدون شک، از جدی‌ترین تهدیدگران تمامیت اخلاقی یک ملت و مانع توسعه و پیشرفت است. از دیگر عوارض جانبی بی‌شمار فساد، می‌توان به تضعیف قوانین و مقررات طراحی‌شده در راستای افزایش مسئولیت‌پذیری و پاسخگویی اداری و اجتماعی نهادها و مؤسسات مختلف اشاره کرد. برای مبارزه با فساد، راهکارهای گوناگونی پیشنهاد شده است. از مهم‌ترین آن‌ها می‌توان از شفافیت، تعهد سیاسی، پاسخگویی اداری، ساده‌سازی شکلی و مشارکت در جامعه مدنی نام برد. استفاده از فناوری اطلاعات در سطح وسیع، در راستای کاهش و پیشگیری از فساد نقش دارد. البته لازم به ذکر است که فناوری اطلاعات نیز مانند هر پدیدهٔ دیگر، دارای مجموعه‌ای از ابعاد و کاربردهای مثبت و منفی بوده و صرفاً واجد آثار ضد فساد

نیست (محسنی، ۱۳۹۲).

علیرغم قوانین بالادستی، قوانین پنج‌ساله توسعه و مصوبات شورای عالی فضای مجازی و مرکز ملی فضای مجازی مبنی بر تأکید بر استفاده انحصاری از درگاه تبادل اطلاعات دولت به‌منظور تبادل اطلاعات بین دستگاه‌های دولتی، هیچ اقدام قابل دفاع و مدونی راجع به امنیت این زیرساخت مهم و حیاتی در کشور انجام نشده است و هیچ‌گونه ارتباط مؤثری بین این دستگاه‌های مهم فوق‌الذکر به‌منظور تدوین سیاست‌های کلان امنیتی درگاه تبادل اطلاعات دولت انجام نشده است. این در حالی است که بر اساس تمام مستندات و استانداردهای امنیت فناوری اطلاعات، لازم است قبل از ایجاد یک چنین زیرساخت اساسی و حیاتی در کشور این جنبه‌ها موردتوجه و مداقه و چکش‌کاری قرار گیرد تا در میانه میدان ضربات امنیتی غیرقابل‌جبران وارد نشود.

از مصاحبه‌هایی که با خبرگان انجام شد و بعد از تحلیل کیفی داده‌ها، سه مفهوم اصلی در ارتباط با امنیت درگاه تبادل اطلاعات دولت به دست آمد. تحلیل کیفی داده‌ها فقط به‌منظور استخراج سؤالات پرسشنامه و دسته‌بندی آن‌ها در گروه‌های معنادار و مرتبط انجام شد. در این تحلیل محتوا به این مفاهیم کلی زیردست پیدا کردیم:

مفهوم راهبردی: این مفهوم شامل دو واقعه اصلی «طرح امن سازی» و «حاکمیتی» است. نیازهایی که از سوی خبرگان مرتبط با تدوین اسناد و مدارک اجرایی برای امنیت درگاه تبادل اطلاعات دولت بیان شدند، ذیل «طرح امن سازی» در نظر گرفته شدند. مواردی نیز که به طرح موضوعات حاکمیتی مثل تدوین قوانین و ساختارهای بالادستی برای ایجاد اکوسیستم امنیت مورد نیاز بوده است در دسته‌بندی «حاکمیتی» قرار داده شدند.

مفهوم فنی: این مفهوم به دسته‌بندی عوامل فنی مؤثر در امنیت درگاه تبادل اطلاعات دولت پرداخته است. مواردی از قبیل «تضمین تداوم کسب‌وکار»، «محرمانگی»، «تصدیق هویت»، «استناد پذیری»، «دسترس‌پذیری» و «حفظ حریم خصوصی» ذیل این مفهوم قرار گرفته شدند که همگی از نوع نیازهایی هستند که به طور فنی قابل حصول هستند.

مفهوم تأثیر روی امنیت ملی: دو مفهوم قبلی، درواقع امن کردن خود «درگاه تبادل

اطلاعات دولت» است؛ اما نکات دیگری توسط خبرگان مطرح گردید که تجانسی با موارد بالا نداشت که این موارد ذیل مفهوم تأثیر درگاه تبادل اطلاعات دولت روی امنیت ملی کدگذاری شدند. مواردی از قبیل «فراداده»، «مقایسه پذیری» و «ترویج درگاه تبادل اطلاعات دولت» که چطور می‌توانند روی امنیت داخلی کشور نقش ایفا کند. به‌عبارت‌دیگر، در دو مفهوم اول، مواردی که برای امن کردن درگاه تبادل مهم است مطرح گردیده است و در این مفهوم، تأثیر درگاه تبادل روی امنیت ملی مدنظر مصاحبه‌شوندگان بوده است. گرچه همان‌طور که گفته شد این مفهوم تجانسی با دو مورد قبل ندارد، ولی به دلیل اهمیت، ما پرسشنامه‌ها را برای این مفهوم نیز تنظیم نمودیم.

تا به اینجا راجع به نتایج قابل‌استخراج از تحلیل‌های کیفی صحبت کردیم؛ اما بر اساس تحلیل‌هایی که به‌صورت کمی انجام شد، طبق مدل کانو، فقط دو نوع نیازمندی انگیزشی و نیازمندی اساسی شناخته شد و نیاز تک‌بعدی یا عملکردی شناخته نشد. نیازهای انگیزشی از نظر خبرگان نیازمندی‌هایی هستند که در درجه دوم اولویت هستند؛ یعنی اگرچه برای پاسخ‌دهندگان جذاب است اما الآن دغدغه اصلی آن‌ها نیست با نگاهی به این نیازمندی‌ها درمی‌یابیم در بعد تأثیر بر روی امنیت ملی تنها نیازمندی‌های «اهرم فشار به دستگاه‌هایی که دلیل فساد اداری تمایلی به پیوستن به GSB ندارند» و «نیاز به فراداده‌ها برای تحلیل‌های آماری به‌منظور کشف فساد اداری» جز نیازمندی‌های اساسی محسوب می‌گردد که عدم تأمین آن برای خبرگان امنیت، قابل‌قبول نیست.

در بعد نیازمندی‌های «حاکمیتی» و «فنی» غیر از «نیاز به دسترسی سریع و آسان به اطلاعات» بقیه جزء نیازمندی‌های اساسی شناخته شدند که از نظر پاسخ‌دهندگان وجود آن‌ها ضروری است و نبود آن غیرقابل‌تحمل است.

میزان رضایت خبرگان از امنیت هر یک از روش‌های تبادل داده، موضوع موردتوجه ماست. این روش‌های تبادل داده شامل GSB، P2P و روش تبادل داده سنتی یا کاغذی می‌باشند. به‌جز نیازمندی «سند الزامات امنیتی» در بقیه موارد، میزان رضایت پاسخ‌دهندگان برای امنیت GSB از دو روش دیگر بیشتر بوده است. این نشان می‌دهد که امنیت GSB به‌شدت

نیازمند «تدوین سند الزامات امنیتی» است.

اما از دیدگاه گروه QFD، مهم‌ترین الزامات امنیتی GSB، با استفاده از تحلیل نیازمندی‌هایی که نمودار اهداف طراحی و شکل شماره ۹ نشان داده شد، به ترتیب عبارت‌اند از: تنظیم لوایح مرتبط با GSB، تشکیل کمیته امنیت GSB و نظارت بر اجرای صحیح الزامات امنیتی؛ که همگی جزء الزامات امنیتی هستند که به نیازمندی‌های حاکمیتی پیوند می‌خورند. این نشان می‌دهد که دغدغه و نگرانی گروه QFD اصلاً مسائل فنی یا حتی ساختارهای فنی نیست، بلکه دغدغه‌های ساختاری کلان اهمیت فوق‌العاده‌ای دارد.

پیشنهادهایی بر اساس نتایج پژوهش

موارد حاکمیتی: این پیشنهادها بیشتر معطوف به الزامات حاکمیتی است:

تشکیل کمیته امنیت GSB: ایجاد یک ستاد کلان با حضور بازیگران امنیت کشور که راجع به مسائل کلان امنیتی هماهنگی‌های لازم و تدوین سندهای بالادستی را به عهده داشته باشند. طبیعتاً با توجه به اینکه سازمان‌های مختلفی بر اساس قانون، اطلاعات خودشان را روی این بستر تبادل می‌کنند لازم است تا نماینده‌ای از قسمت‌های امنیتی آن سازمان، در تدوین الزامات و مسائل کلان امنیت مشارکت داده شود.

نظارت بر اجرای صحیح الزامات امنیتی: چنین ساختاری در حال حاضر در کشور وجود دارد که تحت عنوان «مرکز مدیریت راهبردی افتا» فعالیت می‌کند که لازم است نقش تعیین‌کننده‌تر و مؤثرتری در ارتباط با موضوع امنیت GSB بازی کند.

تنظیم لوایح مرتبط با GSB: با بررسی قوانین و ساختارهای موجود در کشور، به نظر می‌رسد تنها مرجع رسمی شورای عالی فضای مجازی و مرکز ملی فضای مجازی به‌عنوان بازوی اجرایی آن مطرح است که لازم است دستگاه‌ها و سازمان‌های مختلف مشارکت بیشتری از جنبه‌های امنیتی روی آن داشته باشند.

تعیین سازوکاری برای اهرم فشار و ضمانت پیوستن دستگاه‌هایی که به دلیل فساد اداری تمایلی برای پیوستن به GSB ندارند.

موارد فنی: این موارد با الزامات فنی امنیتی مرتبط است که عمدتاً لازم است توسط سازمان فناوری اطلاعات انجام شود:

تشکیل مرکز مدیریت حوادث و رویدادهای امنیت اطلاعات

تشکیل مرکز مدیریت آسیب‌پذیری‌های فنی
راه‌اندازی نسخه پشتیبان و نسخه disaster
ارسال پیام‌ها با کدهای رمزنگاری تائید شده
تصدیق هویت خدمت دهنده و خدمت گیرنده از طریق زیرساخت کلید عمومی
امضای هر تبادل اطلاعات با گواهینامه معتبر به جهت استناد پذیری
ثبت وقایع در خدمت گیرنده و خدمت دهنده به جهت استناد پذیری
پیکربندی امنیت شبکه طبق سند الزامات امنیتی
ارزیابی کلیه تأمین‌کنندگان و داشتن تأییدیه از مراکز امنیتی

تعریف اتصال‌های مجزا برای GSB و PGSG

آموزش و اطلاع‌رسانی به ذینفعان راجع به امنیت GSB و راجع به تأثیراتی که GSB روی امنیت دارد و مزایایی که برای سازمان‌های خدمت دهنده و خدمت گیرنده به ارمغان می‌آورد.

سیاست‌گذاری‌های داخلی در سازمان‌ها و دستگاه‌ها و تدوین یک برنامه بلندمدت یا برنامه مهاجرت به GSB با رویکرد امنیت اطلاعات بر طبق سند الزامات امنیتی و الزام آن‌ها به اجرا و داشتن ضمانت اجرایی مطمئن

پیشنهاد برای تحقیقات آینده

بدون شک نتایج این پژوهش به‌تنهایی نمی‌تواند تمام جنبه‌های مرتبط با امنیت و درگاه تبادل اطلاعات دولت را بیان بکند و برای رفع تمام مسائل و مشکلات موجود در این حوزه، راه‌حل‌ها و پیشنهادهای مناسب ارائه کرد؛ بنابراین پیشنهاد می‌گردد در مورد موضوعات زیر تحقیقاتی صورت گیرد:

تکمیل جداول بعدی QFD برای پژوهش پیش رو
بررسی تأثیر دولت الکترونیک روی شاخص‌های توسعه ملی
بررسی دلایل عدم یا کندی پیوستن دستگاه‌ها به درگاه تبادل اطلاعات دو

منابع

شهبازی نیا، مرتضی؛ عبداللهی، محبوبه .(۱۳۸۸). احراز اصالت در اسناد الکترونیکی. *فصلنامه مدرس علوم انسانی-پژوهش های حقوقی تطبیقی*، ۱۳(۴)، ۱۴۱-۱۲۵.

صادقی نژاد، امیر .(۱۳۹۳). اعتبار سنجی اسناد الکترونیک. *فصلنامه پژوهش حقوق خصوصی*، ۳(۸)، ۱۰۰-۷۱.

حسین آبادی، فاطمه؛ کشمیری، عادله؛ حسین آبادی، زهرا .(۲۰۱۵). بررسی جعل اسناد امور ثبتی در حقوق کیفری ایران و راه‌های مقابله با آن. *کنفرانس بین‌المللی مدیریت و علوم انسانی*.

گرایلی، محمدباقر .(۱۳۹۰). بررسی جعل و تخریب و اخلال رایانه‌ای. *آموزه‌های حقوقی دانشگاه علوم اسلامی رضوی*، ۱۴.

قنّاد، فاطمه .(۱۳۹۱). جعل در بستر فناوری‌های اطلاعات و ارتباطات. *آموزه‌های حقوقی دانشگاه علوم اسلامی رضوی*، شماره ۲.

ایران زاده، سلیمان؛ داودی، کامل .(۱۳۹۱). بررسی رابطه استقرار دولت الکترونیک و سلامت نظام اداری کشور. *فراسوی مدیریت*. ۶(۲۲)، ۷۴-۵۵.

دانایی‌فرد، حسن .(۱۳۸۳). استراتژی مبارزه با فساد. *فصلنامه مدرس علوم انسانی*، ۹(۲)، ۱۱۷-۱۰۱.

لگزیان، محمد؛ یوسف پور، افسانه؛ تقوی، سیده فریماه .(۱۳۹۲). بررسی تأثیر عوامل مؤثر بر اشتراک‌گذاری اطلاعات G2G میان سازمان‌های دولتی. *فصلنامه دیدگاه‌های حقوقی قضایی*، ۶۱، ۱۷۴-۱۳۹.

خداداد حسینی، سید حمید؛ فرهادی نژاد، محسن .(۱۳۸۰). بررسی فساد اداری و روش‌های کنترل آن. *فصلنامه مدرس علوم انسانی*، ۵(۱)، ۵۳-۳۷.

محسنی، فرید .(۱۳۹۲). پیشگیری از فساد اداری با تأکید بر فناوری اطلاعات. *فصلنامه دیدگاه‌های حقوق قضایی*، ۶۱، ۱۷۴-۱۳۹.

مهرگان، نادر؛ سحابی، بهرام؛ محمدامینی، مریم .(۱۳۹۴) تأثیر شاخص توسعه فناوری اطلاعات و ارتباطات بر فساد اداری در کشورهای با درآمد متوسط. *فصلنامه نظریه‌های کاربردی اقتصاد*، ۲(۲)، ۶۰-۴۳.

متفکر آزاد، محمدعلی؛ جامه شورانی، زینب؛ حیدری داد، زینب .(۱۳۹۲). تأثیر دولت الکترونیکی بر کاهش فساد اقتصادی در کشورها منتخب اسلامی. *فصلنامه مدل‌سازی اقتصادی*، ۷(۴)، ۵۱-۳۷.

فرهادی نژاد، محسن .(۱۳۸۵). دولت الکترونیک و حکومت‌داری خوب. *مجله تدبیر*، ۱۶۹، ۲۷-۲۲.

هادوی نژاد، مصطفی؛ جاوید، زهرا .(۱۳۹۳). رابطه فناوری اطلاعات با فساد اداری. *فصلنامه اخلاق در علوم و فناوری*، ۱۰(۴)، ۷۴-۶۵.

خرم‌آبادی، عبدالصمد .(۱۳۸۶). کلاه‌برداری رایانه‌ای از دیدگاه بین‌الملل و وضعیت ایران. *فصلنامه حقوق مجله دانشکده حقوق و علوم سیاسی*، ۳۷(۲)، ۱۱۲-۸۳.

اصغرنیا، مرتضی .(۱۳۸۸). ضرورت توجه به دولت الکترونیک با نگاهی خاص به پدیده فساد اداری. *دانشکده حقوق و علوم سیاسی دانشگاه تهران*.

وصالی ناصح، مرتضی .(۱۳۹۴). سند رسمی الکترونیک (مطالعه تطبیقی امکان صدور سند رسمی الکترونیک در حقوق ایران و آمریکا. *دانشنامه حقوق و سیاست*، ۲۵، ۸۰-۶۱.

Nadianatra, M., Rosita, M. O., Dayang, H. A. I., & Inson, D. (2012). E-Government Services: The Formal, Technical and Informal components of E-Fraud Prevention for Government Agency. *IRACST- International Journal of Research in Management & Technology (IJRMT).*

Alexopoulos, P., Kafentzis, K., Benetou, X., Tagaris, T., & Georgolios, P. (2007). Toward a Generic Fraud ontology in eGovernment, Barcelona, Spain, July 28-31, ICE-B is part of ICETE - *The International Joint Conference on e-Business and Telecommunication*.

Christopher G. R. (2003). A two-stage model of e-government growth: Theories and empirical evidence for U.S. cities. *Government Information Quarterly. 21*.

Fan, J., Zhang, P., Yen, D (2014): G2G information sharing among government agencies. *Information & Management. 51.*

Bigdeli A. Z., Kamal, M. M., & Cesare, S. (2013). Electronic information sharing in local government authorities: Factors influencing the decision-making process. *International Journal of Information Management. 33.*

Wang, F. (2014). Explaining the low utilization of government websites: Usnig a grounded theory approach, *Government Information Quarterly. 31.*

Kamal, M. R., Singh, D. S. V., & Ahmad, K (2012). Factors Influencing interdepartmental information sharing practice in electronic government agencies. *Knowledge Management International Conference (KMICe).*

Gil-Garcia, J. R., & Sayogo D. S. (2016). Government inter-organizational information sharing initiatives: Understanding the main determinants of success. *Government Information Quarterly.*

Akbulut, A. Y, Kelle, P., Pawlowski, S. D., Schneider, H., & Looney, C. A (2009). To share or not to share? Examining the factors influencing local agency electronic information sharing. *Business Information Systems.*

Patil, H., Patil, S. (2008). E-Governance and White Collar Crime Control. *E-Governance in Practice.*

Mistry, J. J., & Jalal, A. (2012). An Empirical Analysis of the Relationship between e-government and Corruption. *The Industrial Journal of Digital Accounting Research.*

Ezeani, C. N., & Asogwa, B. E. (2018). E-Government Initiative in Sub Saharan Africa as a Strategy for Reducing Corruption in the Public Sector: A Comparative Assessment of SubRegional Performance.

Lupu, D., & Lazăr, C. G. (2015). Influence of e-government on the level of corruption in some EU and non-EU states. *Procedia Economics and Finance.*

Sokim, T., Xiaolin, X., & Dong, H. (2015). E-Government: Combatting Corruption and Contribute to Good Governance.3(6),42-47.

Abbie Griffin, A., Hauser, J. R. (1993). The Voice of the Customer.

Knězáčková, R., & Linhartová, V. (2012). Impact of E-Government at the level of Corruption. *7th International Days of Statistics and Economics.*

Máchová, R., Volejníková, J., & Lněnička, M. (2018). Impact of E-Government Development on the Level of Corruption: Measuring the Effects of Related Indices in Time and Dimensions. *Review of Economic Perspectives.*