

مدیریت ریسک‌های فناوریانه در سازمان‌های شهری هوشمند: چالش‌ها و راهکارها (مطالعه موردی: شهرداری تبریز)

قاسم زاده، راضیه (گروه جغرافیا و برنامه ریزی شهری، دانشکده علوم اجتماعی، دانشگاه محقق اردبیلی، اردبیل، ایران)

یزدانی، محمد حسن (دانشگاه محقق اردبیلی)

سبحانی، اقبال (کارشناسی ارشد شهرسازی، گرایش برنامه ریزی شهری مدرس دانشگاه جیهان واحد سلیمانیه)

چکیده

شهرهای هوشمند به‌عنوان الگوی نوین مدیریت شهری، به‌شدت متکی بر فناوری‌های اطلاعات و ارتباطات هستند و هرگونه اختلال در این زیرساخت‌ها می‌تواند پیامدهای گسترده مدیریتی، خدماتی و اجتماعی به دنبال داشته باشد. چالش‌های عمومی شهرهای هوشمند نظیر ازدحام ترافیک، ناکارآمدی مصرف آب و انرژی، تهدیدهای امنیتی و آلودگی هوا در بسیاری موارد ناشی از بروز ریسک‌های فناوریانه ازجمله خرابی تجهیزات حمل‌ونقل هوشمند، نقص امنیت سایبری در دوربین‌ها، اختلال در شبکه‌های هوشمند و ناسازگاری نرم‌افزارهای مدیریتی هستند. ازاین‌رو، مدیریت مؤثر ریسک در زیرساخت‌های فناوریانه نقش تعیین‌کننده‌ای در تاب‌آوری مدیریت شهری دارد. پژوهش حاضر باهدف شناسایی و اولویت‌بندی ریسک‌های فناوریانه در شهرداری تبریز انجام شد. برای شناسایی ریسک‌ها، ابتدا مرور نظام‌مند پیشینه پژوهش صورت گرفت و سپس به‌منظور اعتبارسنجی فهرست اولیه و تکمیل آن، مصاحبه نیمه ساختاریافته با ۱۲ نفر از خبرگان حوزه فناوری و هوشمند سازی شهرداری تبریز انجام شد و پس از اجماع، دسته‌بندی ریسک‌ها نهایی گردید. این مطالعه از نوع کاربردی، به روش توصیفی-پیمایشی و با رویکرد کمی اجرا گردید. ابزار گردآوری داده‌ها پرسشنامه محقق ساخته در دو بعد «احتمال وقوع» و «میزان تأثیر» بود که میان ۷۳ نفر از مدیران و کارشناسان حوزه فناوری و هوشمند سازی شهرداری تبریز با روش نمونه‌گیری در دسترس توزیع شد. داده‌ها با نرم‌افزارهای SPSS و AMOS تحلیل شدند. نتایج نشان داد که از نظر احتمال وقوع، ریسک‌های مربوط به تجهیزات حمل‌ونقل (۰/۹۵)، دوربین‌های هوشمند (۰/۹۱)، شبکه‌های هوشمند (۰/۸۸) و نرم‌افزارها (۰/۸۷) به ترتیب در اولویت قرار دارند؛ و از نظر میزان تأثیر، ریسک‌های شبکه‌های هوشمند (۰/۸۸)، تجهیزات حمل‌ونقل (۰/۸۵)، نرم‌افزارها (۰/۷۶) و دوربین‌های هوشمند (۰/۷۶) بیشترین اهمیت را دارند. به‌طورکلی یافته‌ها نشان می‌دهد که آسیب‌پذیری مدیریت شهری عمدتاً از اختلال در زیرساخت‌های ارتباطی و اطلاعاتی ناشی می‌شود و ارتقای امنیت سایبری، نگهداشت فناوری، یکپارچه‌سازی سامانه‌های هوشمند و سرمایه‌گذاری هدفمند در زیرساخت‌های ICT باید در اولویت سیاست‌گذاری شهرداری تبریز برای کاهش ریسک و افزایش تاب‌آوری شهر هوشمند قرار گیرد.

واژگان کلیدی: مدیریت شهری، ریسک‌های فناوریانه، شهر هوشمند، چالش‌ها

Technological Risk Management in Smart Urban Management Organizations: Challenges and Solutions (Case Study: Tabriz Municipality)

In the case of Tabriz Municipality, the expansion of smart city projects has highlighted the need for an effective technological risk management framework. This study seeks to identify, evaluate, and prioritize these risks to support resilient and sustainable urban governance. The study adopts an applied–descriptive research design with a quantitative approach. Data were collected through a structured questionnaire developed by the researchers, focusing on two main dimensions: the probability of occurrence and the impact level of technological risks. Eight indicators were analyzed—software, authentication, smart networks, big data, transportation equipment, smart cameras, operating systems, and cybersecurity. The statistical population consisted of 73 experts and managers from Tabriz Municipality. Data analysis was conducted using SPSS and AMOS software, employing descriptive statistics, one-sample t-tests, and second-order confirmatory factor analysis to validate the research model. Findings revealed that the mean values for the probability of technological risks were generally higher than those for their impact, indicating that participants perceived these risks as highly likely but only moderately damaging. Among the indicators, transportation equipment (0.95), smart cameras (0.91), smart networks (0.88), and software (0.87) had the highest probability scores. Regarding impact, smart networks (0.88), transportation equipment (0.85), software (0.76), and smart cameras (0.76) ranked highest. Model fit indices ($RMSEA = 0.053$ for impact and $RMSEA = 0.061$ for probability) confirmed the validity and reliability of the analysis. The results demonstrate that Tabriz Municipality faces significant technological risks in its transition toward a smart city. While the probability of such risks is high, mitigation and preparedness levels remain inadequate. This imbalance reflects the municipality's limited institutional readiness and lack of comprehensive risk management policies. Strengthening technical capacities, enhancing cybersecurity systems, integrating risk management frameworks across departments, and promoting inter-organizational collaboration are essential for improving resilience and ensuring sustainable smart urban governance.

Urban Management, Technological Risks, Smart City, Challenge, Solutions

۱. مقدمه

شهرهای هوشمند از نظر نوع خدمات ارائه شده با شهرهای سنتی تفاوت اساسی دارند؛ چراکه خدمات آنها صرفاً محدود به استفاده از اجزای فنی مانند حسگرها، عملگرها و دستگاه‌های هوشمند نیست، بلکه عناصر کلیدی دیگری نظیر داده‌ها، نرم‌افزارها، سیاست‌ها و ذی‌نفعان نیز نقش مهمی در ساختار این شهرها ایفا می‌کنند. با گسترش فناوری‌های نوآورانه،

سطح پیچیدگی و عدم قطعیت در محیط شهری افزایش یافته و ضرورت دارد که مدیریت ریسک در این فضا صرفاً به جنبه‌های فنی محدود نشود، بلکه ابعاد مدیریتی، ساختاری و سیاست‌گذاری نیز مورد توجه قرار گیرد. مطالعات نشان داده‌اند که بیش از نیمی از پروژه‌های فناوری اطلاعات به دلایل غیر فنی همچون سیاست‌گذاری نامناسب، ساختار ناکارآمد سازمانی و ضعف در مدیریت ریسک با شکست مواجه می‌شوند (سینگ و هلفرت^۱، ۱۳۹۸، ص. ۲۲۱). بنابراین، برای موفقیت در مسیر هوشمند سازی شهری، باید نگاهی جامع و بین‌رشته‌ای به موضوع ریسک داشت. در قرن اخیر، تمرکز جمعیت در شهرها و رشد سریع شهرنشینی، آن‌ها را به نظام‌هایی پیچیده و به هم پیوسته تبدیل کرده است که شامل زیرساخت‌های حیاتی، شبکه‌های اجتماعی و اقتصادی و نظام‌های حکمرانی درهم‌تنیده‌اند. این پیچیدگی موجب افزایش آسیب‌پذیری شهرها در برابر تهدیدات مختلف طبیعی، انسانی و فناورانه از جمله پاندمی‌ها، بحران‌های زیست‌محیطی و حملات سایبری شده است. در چارچوب شهرهای هوشمند، این آسیب‌پذیری‌ها ممکن است به دلیل وابستگی شدید سیستم‌ها به فناوری و داده‌ها، با شدت بیشتری گسترش یابد و موجب بروز اختلالات زنجیره‌ای در زیرساخت‌های حیاتی شود؛ بنابراین، ایجاد شهرهای تاب‌آوری که بتوانند از طریق تحلیل داده محور و سیستم‌های پشتیبان تصمیم‌گیری به مدیریت مؤثر ریسک‌ها بپردازند، از ضروریات توسعه پایدار شهری به شمار می‌آید (گارامینانا و همکاران^۲، ۱۴۰۳، ص. ۲).

از سوی دیگر، شهرهای هوشمند در پاسخ به چالش‌هایی نظیر رشد سریع جمعیت، کمبود منابع و محدودیت‌های مالی به وجود آمده‌اند و هدف آن‌ها بهبود کیفیت زندگی و افزایش پایداری شهری است. با این حال، این شهرها دارای ماهیتی دوگانه‌اند؛ زیرا در کنار مزایایی همچون افزایش کارآمدی، صرفه‌جویی در منابع و ارتقای امنیت، تهدیدات و آسیب‌پذیری‌های جدیدی نیز ایجاد می‌کنند. وابستگی شدید زیرساخت‌های شهری به شبکه‌های دیجیتال و سامانه‌های اطلاعاتی، شهرها را در برابر خطراتی چون جرائم سایبری، نفوذ داده‌ای و خطاهای نرم‌افزاری آسیب‌پذیر می‌سازد. درواقع، شهرهای هوشمند به عرصه‌ای رقابتی میان مدافعان امنیت سایبری و مهاجمان دیجیتال تبدیل شده‌اند؛ جایی که حملات موفق می‌تواند دسترسی به داده‌های میلیون‌ها شهروند یا ایجاد اختلال در خدمات حیاتی مانند آب، برق و حمل‌ونقل را در پی داشته باشد (کیتچین و دودگه^۳، ۱۳۹۸، ص. ۴۸). یکی از چالش‌های بنیادین در این زمینه، مدیریت حجم عظیم داده‌ها و یکپارچه‌سازی آن‌ها در سیستم‌های شهری است. اتصال میان داده‌های موجود در پایگاه‌های اطلاعاتی و داده‌های جدید تولیدشده توسط حسگرها، از یک‌سو فرصت‌هایی برای تصمیم‌گیری هوشمند فراهم می‌کند و از سوی دیگر، تهدیداتی در زمینه حریم خصوصی و امنیت اطلاعات به همراه دارد. دسترسی غیرمجاز به داده‌های حساس می‌تواند موجب بروز پیامدهای ناخواسته و آسیب‌های اجتماعی و اقتصادی شود؛ از این رو، ضرورت دارد که مسائل امنیتی و حریم خصوصی از مراحل اولیه طراحی و توسعه شهرهای هوشمند مورد توجه قرار گیرد (اسماگیلوا و همکاران^۴، ۱۳۹۹، ص. ۳۹۴). بسیاری از خدمات شهر هوشمند بر پایه معماری متمرکز^۵ عمل می‌کنند که در آن داده‌های حاصل از دستگاه‌ها و حسگرهای سطح

¹ Singh&Helfert

² Garraminana&etal

³ Kitchin&Dodge

⁴ Ismagilova&etal

⁵ Centralized Architecture

شهر به یک مرکز کنترل ارسال می‌شود تا ذخیره‌سازی و تحلیل شود. چنین ساختاری اگرچه امکان نظارت و تصمیم‌گیری سریع را فراهم می‌کند، اما به دلیل تمرکز داده‌ها، در برابر حملات سایبری و اختلالات فنی آسیب‌پذیر است. از این رو، مدیریت امنیت اطلاعات در این شهرها یکی از اولویت‌های اساسی محسوب می‌شود تا از صحت، دقت و اعتمادپذیری تبادل داده‌ها اطمینان حاصل گردد. درعین حال، فناوری اینترنت اشیا فرصت‌های جدیدی برای توسعه کاربردهای هوشمند همچون حمل و نقل، انرژی و ایمنی عمومی ایجاد کرده است، اما همین فناوری‌ها نیز تهدیدهای جدیدی در حوزه امنیت سایبری و پایداری سیستم‌ها به همراه دارند (دین و همکاران^۶، ۱۴۰۰، ص. ۱۰۰).

مدیریت شهری به عنوان مفهومی چندبعدی و پویا، مجموعه‌ای از سیاست‌ها، برنامه‌ها و روش‌های اجرایی را دربر می‌گیرد که هدف آن بهبود کارایی، ارتقای کیفیت زندگی شهروندان و تضمین دسترسی عادلانه به خدمات عمومی است. این نوع مدیریت، تلاشی برای ایجاد تعادل میان توسعه اجتماعی، اقتصادی و کالبدی شهر در چارچوب ساختار فضایی و تاریخی آن محسوب می‌شود و با توجه به پیچیدگی محیط شهری، نیازمند هماهنگی میان نهادهای مختلف و بهره‌گیری از فناوری‌های نوین است (بوتون^۷، ۱۳۸۰، ص. ۷۶). مدیریت ریسک به عنوان بخش مکمل و ضروری مدیریت شهری برای شناسایی، تحلیل، کنترل و کاهش خطرات بالقوه و افزایش تاب‌آوری در برابر تهدیدها محسوب می‌شود (زنجانی و همکاران، ۱۳۹۹: ۲۲۰). در پروژه‌های شهر هوشمند، استراتژی‌های کاهش ریسک شامل تقویت ظرفیت فنی از طریق آموزش و استانداردسازی فناوری، اجتماعی سازی مقررات با مشارکت ذی‌نفعان و افزایش شفافیت سیاستی و همچنین جلب مشارکت جامعه از طریق برنامه‌های آگاهی‌بخشی و مشارکت عمومی است (سانجایا و همکاران^۸، ۱۴۰۴، ص. ۴۱۸).

پژوهش‌ها در حوزه مدیریت ریسک و شهرهای هوشمند در سطح بین‌المللی طی سال‌های اخیر تمرکز ویژه‌ای بر نقش فناوری، حکمرانی و امنیت در تحقق شهرهای هوشمند داشته‌اند. در مطالعات خارجی سانجایا و همکاران (2025) که به بررسی مدیریت ریسک در توسعه شهرهای هوشمند در بالی پرداخته است. آنان با بهره‌گیری از روش تحقیق ترکیبی، به شناسایی ریسک‌های فنی، غیر فنی و زیست‌محیطی در پروژه‌های شهر هوشمند پرداختند. نتایج نشان داد که عواملی مانند خطاهای طراحی، شکست فناوری، تغییرات قانونی و مقاومت اجتماعی از موانع اصلی تحقق اهداف شهر هوشمند هستند. پژوهش همچنین تأکید می‌کند که موفقیت پروژه‌های شهر هوشمند نیازمند چارچوب مدیریت ریسک بومی سازی است که بتواند ویژگی‌های فرهنگی، اقتصادی و زیست‌محیطی منطقه را در نظر گیرد. مطالعه گاده و آیت‌هال (۲۰۲۲) تحت عنوان راه‌حل‌های مبتنی بر فناوری اطلاعات و ارتباطات و فناوری دیجیتال برای چالش‌ها و فرصت‌های شهر هوشمند یکی از پژوهش‌های بنیادی در حوزه استفاده از فناوری‌های اطلاعات و ارتباطات و دیجیتال برای مقابله با چالش‌های شهر هوشمند است. نویسندگان با رویکرد مروری و تحلیلی، مجموعه‌ای از چالش‌های عمده در توسعه و بهره‌برداری شهرهای

⁶ Din&etal

⁷ Button

⁸ Sanjaya&etal

هوشمند را شناسایی کردند؛ از جمله ازدحام ترافیکی، کمبود منابع آبی و انرژی، ضعف در مدیریت پسماند و مشارکت محدود شهروندان در مدیریت شهری.

پژوهش‌های داخلی عمدتاً بر مدیریت شهری، هوشمند سازی و تهدیدات فناورانه تمرکز داشته و ضرورت راهبردهای مدیریتی و سیاست‌گذاری صحیح را مورد توجه قرار داده‌اند. در مطالعات داخلی رضایی (۱۴۰۴) در تحقیق خود تحت عنوان واکاوی چالش‌ها و فرصت‌های مدیریت نوین در شهرداری‌ها با رویکرد بهره‌گیری از فناوری‌های هوشمند شهری بیانگر آن است که برای دستیابی به مدیریت شهری کارآمد و نوین، بهره‌گیری هدفمند از فناوری‌های هوشمند همراه با سیاست‌گذاری دقیق، آموزش نیروی انسانی و تقویت زیرساخت‌های ارتباطی امری ضروری است. این رویکرد می‌تواند زمینه ارتقای کیفیت مدیریت شهری و تحقق اهداف توسعه پایدار را فراهم آورد. خاکپور و همکاران (۱۴۰۳) در پژوهشی با عنوان شناسایی تهدیدات در حاکمیت شهرهای هوشمند با رویکرد^۹ TOE نمونه موردی: شهرداری مشهد به بررسی ریسک‌ها و تهدیدات مؤثر بر حاکمیت شهری در فرایند هوشمند سازی پرداختند و یافته‌ها نشان دادند که از میان ابعاد سه‌گانه، بعد سازمانی بیشترین سهم را در بروز تهدیدات حاکمیتی شهر هوشمند دارد. در بعد فناوری، مؤلفه‌های مرتبط باهوش مصنوعی (0.79)، نرم‌افزار (0.768)، حسگرها (0.767)، بیشترین وزن عاملی را داشتند. همچنین در بعد سازمانی، شاخص‌های تراکنش الکترونیک (0.820)، محرمانگی اطلاعات (0.760) و صحت اطلاعات (0.752) به عنوان مهم‌ترین تهدیدها شناسایی شدند.

با توجه به نقش شهرداری به عنوان نهاد اصلی مدیریت و ارائه خدمات عمومی در شهر، توجه به مدیریت ریسک در این سازمان اهمیتی دوچندان دارد. شهرداری‌ها به عنوان سازمان‌هایی عمومی و غیرانتفاعی، مأموریت دارند تا خدمات شهری کارآمد، ایمن و باکیفیتی ارائه دهند و رضایت شهروندان را افزایش دهند. در این میان، حرکت شهر تبریز به سمت هوشمند سازی و بهره‌گیری از فناوری‌های نوین، پیچیدگی محیط شهری و ماهیت تهدیدات فناورانه را افزایش داده است. سیستم‌های حیاتی شهری مانند آب، برق، حمل و نقل، پسماند و خدمات اداری به صورت شبکه‌ای به هم وابسته‌اند و اختلال در یکی از آنها می‌تواند پیامدهای زنجیره‌ای برای سایر بخش‌ها به همراه داشته باشد. به عنوان نمونه، حملات سایبری به شبکه برق می‌تواند عملکرد سامانه‌های حمل و نقل یا خدمات اضطراری را نیز مختل کند. از این رو، شناسایی و مدیریت ریسک‌های فناورانه در شهرداری تبریز، به‌ویژه در مسیر هوشمند سازی شهری، ضرورتی حیاتی دارد. این پژوهش باهدف بررسی چالش‌ها و ارائه راهکارهایی برای مدیریت ریسک‌های فناورانه در سازمان‌های مدیریت شهری، به‌طور خاص وضعیت شهرداری تبریز را به عنوان یکی از پیشگامان این حوزه مورد مطالعه قرار می‌دهد. نوآوری اصلی پژوهش در این است که با رویکردی میان‌رشته‌ای، داده محور و مشارکت گرا، ریسک‌های فناورانه شهر هوشمند را نه از منظر

⁹ Technology Organization Environmental

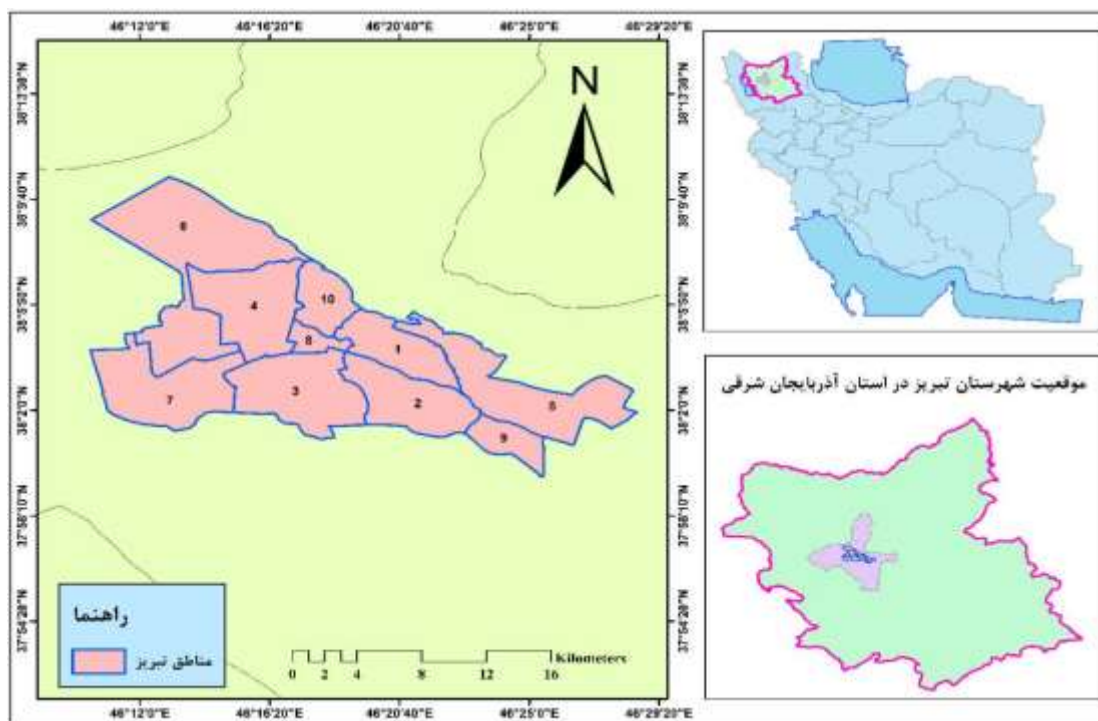
فناوری صرف، بلکه در پیوند با حکمرانی، ساختار سازمانی و امنیت اطلاعات بررسی کرده و در نهایت چارچوبی اجرایی و بومی سازی برای مدیریت این ریسک ها در شهرداری تبریز ارائه می دهد. پرسش های اصلی تحقیق عبارت اند از:

۱. مهم ترین چالش های شهر هوشمند تبریز در حوزه ریسک های فناورانه (از جمله حریم خصوصی و امنیت) از دیدگاه سه گروه ذی نفع اصلی شامل مدیران فناوری شهرداری، کارشناسان حوزه شهر هوشمند و شهروندان بهره بردار کدام اند؟
۲. وضعیت شهرداری تبریز در برابر حوادث و تهدیدات فناورانه غیرمنتظره از نظر میزان تأثیر و احتمال وقوع چگونه است؟

۲. متدولوژی

۱-۲. محدوده مورد مطالعه

شهر تبریز، به عنوان یکی از مهم ترین شهرهای شمال غربی ایران و مرکز استان آذربایجان شرقی، هسته اصلی کلان شهر تبریز را تشکیل می دهد. بر اساس آمار موجود، جمعیت این شهر حدود ۱,۵۹۳,۳۷۳ نفر برآورد شده است که معادل ۴۲ درصد جمعیت کل استان را شامل می شود. تبریز با وسعت ۲۴۴,۰۵۱ کیلومتر مربع (حریم شهر: ۱۰۱۴,۰۴۵ کیلومتر مربع) در ناحیه میانی آذربایجان و در بخش شرقی و شمالی دریاچه ارومیه واقع شده و در فاصله ای حدود ۶۱۹ کیلومتری از شهر تهران قرار دارد. شهرداری تبریز که تأسیس آن به سال ۱۲۸۶ هجری شمسی بازمی گردد، در حال حاضر دارای ده منطقه شهری است که در میان آنها، منطقه ۴ بیشترین جمعیت و منطقه ۹ کمترین جمعیت را در بردارد (زینالی عظیم، ۱۴۰۱: ۷۱). در این شهر، شهرداری نزدیک ترین نهاد اجرایی حاکمیت به شهروندان محسوب می شود و نقش اساسی در اداره و سامان دهی امور شهری دارد. اگرچه مدیریت واحد شهری در تبریز با چالش ها و محدودیت های مختلفی مواجه است، اما طی سال های اخیر اقداماتی در راستای توسعه شهر الکترونیک و خدمات هوشمند از سوی شهرداری صورت گرفته است. این اقدامات، زمینه ساز شکل گیری زیرساخت های لازم برای حرکت به سوی شهر هوشمند بوده و پتانسیل بالایی برای گسترش فناوری های نوین در مدیریت شهری ایجاد کرده اند (روستایی و همکاران، ۱۳۹۷: ۲۰۲).



شکل (۱). نقشه موقعیت جغرافیایی شهر تبریز

۲-۲. روش پژوهش

پژوهش حاضر از نظر هدف کاربردی و از نظر ماهیت و شیوه اجرا توصیفی-پیمایشی با رویکرد کمی است. جامعه آماری شامل کارشناسان و مدیران حوزه فناوری و هوشمند سازی شهرداری تبریز در سال ۱۴۰۴ هست. از آنجاکه تخصص و تجربه مرتبط شرط اصلی مشارکت در پژوهش بوده است، نمونه‌گیری در دو مرحله انجام شد: ابتدا فهرست افراد واجد صلاحیت استخراج شد و سپس از میان آنان نمونه‌گیری هدفمند (قضاوتی) با توجه به تخصص و سابقه فعالیت در حوزه ریسک‌های فناوریانه به کار گرفته شد تا احتمال سوگیری سیستماتیک و محدود شدن قابلیت تعمیم کاهش یابد. در نهایت، ۷۳ نفر مورد انتخاب قرار گرفتند و تمام پرسشنامه‌ها بدون نقص تکمیل و گردآوری شد. به منظور تعیین کفایت حجم نمونه برای تحلیل مدل یابی معادلات ساختاری، از نسبت ۵ تا ۱۰ مشاهده به ازای هر پارامتر قابل برآورد استفاده شد. با توجه به وجود ۳۰ گویه و ۸ مؤلفه در پرسشنامه، حداقل حجم نمونه لازم ۶۰ نفر برآورد گردید؛ بنابراین تعداد ۷۳ پاسخ‌دهنده بیش از حداقل لازم بوده و کفایت آماری لازم برای اجرای تحلیل عاملی و SEM را تأمین می‌کند.

ابزار گردآوری داده‌ها پرسشنامه محقق ساخته در دو بعد «احتمال وقوع» و «میزان تأثیر» ریسک‌های فناوریانه بود که مؤلفه‌های نرم‌افزارها، احراز هویت، شبکه‌های هوشمند، ابر داده، تجهیزات حمل و نقل، دوربین‌های هوشمند، سیستم‌عامل‌ها و امنیت سایبری را پوشش می‌داد. به منظور بررسی روایی محتوای پرسشنامه، آن در اختیار ۵ نفر از متخصصان حوزه

فناوری شهری و مدیریت ریسک قرار گرفت. شاخص CVR برای هر گویه بر اساس جدول لاوشه محاسبه شد و تمام گویه‌ها مقادیر بالاتر از حد آستانه ۰,۹۹ را کسب کردند. همچنین شاخص CVI برای هر گویه و کل پرسشنامه بر اساس معیارهای والتز و باسل محاسبه شد و همه گویه‌ها حداقل مقدار ۰,۷۸ را داشتند؛ بنابراین، روایی محتوای پرسشنامه تأیید شد. همچنین جهت ارزیابی روایی سازه، تحلیل عاملی تأییدی اجرا گردید که مقادیر میانگین واریانس استخراج شده (AVE) بزرگ‌تر از ۰,۵۰ و پایایی ترکیبی (CR) بزرگ‌تر از ۰,۷۰ برای تمامی مؤلفه‌ها به دست آمد؛ بنابراین روایی سازه پرسشنامه مناسب ارزیابی شد. برای بررسی پایایی ابزار اندازه‌گیری از ضریب آلفای کرون باخ استفاده شد. مقدار آلفای کل پرسشنامه ۰,۸۶ و مقدار آلفای مؤلفه‌ها در دامنه ۰,۷۸ تا ۰,۸۹ قرار داشت که بیانگر پایایی مناسب ابزار است. برای تحلیل داده‌ها از نرم‌افزارهای SPSS و AMOS بهره گرفته شد. در بخش آمار توصیفی از شاخص‌های میانگین و انحراف معیار و در بخش آمار استنباطی از آزمون T تک نمونه‌ای و مدل‌سازی معادلات ساختاری با رویکرد تحلیل عاملی مرتبه دوم استفاده گردید. مقادیر شاخص‌های برازش مدل شامل $\chi^2/df = 2.41$, $CFI = 0.92$, $TLI = 0.90$, $GFI = 0.91$ و $RMSEA = 0.053$ برای بعد «میزان تأثیر» و ۰,۶۱ برای بعد «احتمال وقوع» که بیانگر برازش مناسب مدل است.

جدول (۱). شاخص‌های مطالعاتی پژوهش و مصادیق

شاخص	مصادیق	منابع
نرم‌افزارها	(اختلال عملکردی، نقض امنیت)	(یولاه و همکاران ^{۱۰} ، ۱۴۰۰) و (کاظمی مهر، ۱۳۹۶)، و (طهماسبی زاده، رجب پور و فیلی، ۱۳۹۹)
احراز هویت	(داده‌های هویتی، مدیریت احراز هویت یکپارچه سرویس‌ها و سامانه‌های شهروندی)	(نام و همکاران ^{۱۱} ، ۱۴۰۰) و (کودین ^{۱۲} ، ۱۳۸۳) و (یولاه و همکاران ^{۱۳} ، ۱۴۰۰)
شبکه‌های هوشمند	(اختلال بین سیستم‌ها، ذخیره‌سازی، پردازش داده‌ها با حجم بالا)	(کودین ^{۱۲} ، ۱۳۸۳) و (یولاه و همکاران ^{۱۳} ، ۱۴۰۰)
ابر داده‌ها	(داده‌های بدون ساختار و ناقص، مدیریت زیرساخت‌های داده‌های بزرگ، مدیریت امنیت، بانک هوشمند، تمامیت داده‌ها)	(گزارش ریسک‌های جهان، ۲۰۲۲) و (یولاه و همکاران، ۱۴۰۰)
تجهیزات حمل‌ونقل	(چراغ‌های راهنمایی و رانندگی، ایمنی روشنایی، تخصیص پارکینگ هوشمند، فناوری تنظیم‌کننده ترافیک، سیستم کنترل مترو)	(لاکامبرا و همکاران ^{۱۴} ، ۱۳۹۷، ص ۱۰)

¹⁰ Ullah&etal

¹¹ Nam&etal

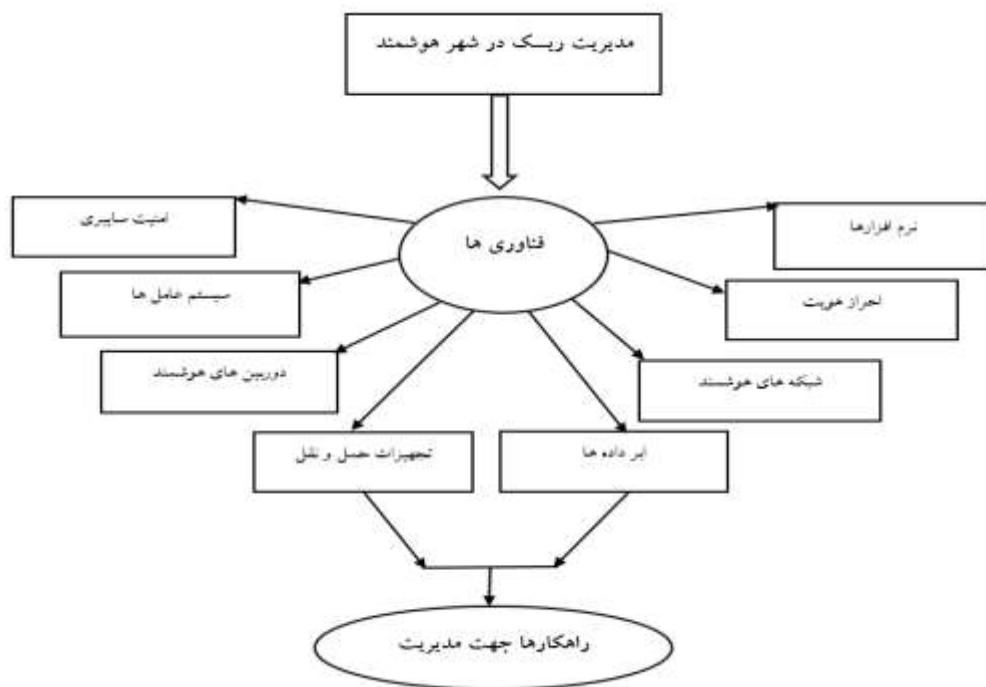
¹² Godin

¹³ Ullah&etal

¹⁴ Lacambra&etal

دوربین‌های هوشمند	(ازکارافتادگی دوربین‌ها با انواع حملات سایبری و فیزیکی، جرم و جنایت، سرقت)	(رضایی، علیزاده و نورمحمدی، ۱۳۹۹) و (روستایی و همکاران، ۱۳۹۶: ۱۹۹) و (استون برنز، گوگن و فرینگا، ۱۳۸۵)
سیستم‌عامل‌ها	(پاک کردن نرم‌افزارها، ویروس‌ها و بدافزارها، تجارت الکترونیک، شناسه دستگاه)	(اسکوتو و همکاران ^{۱۵} ، ۱۳۹۵، ص. ۳۵۹)
امنیت سایبری	(آسیب‌پذیری‌ها، نفوذپذیری، اختلال در ارتباطات، برداشت غیرمجاز اطلاعات، اختلال در زیرساخت)	(کیتچین و دودگه، ۱۳۹۸، ص. ۴۸) و (کومیتها ^{۱۶} ، ۱۳۹۹، ص. ۴)

مأخذ: یافته‌های پژوهش، ۱۴۰۴



شکل (۲). مدل مفهومی پژوهش

¹⁵ Scuotto&etal

¹⁶ Kummitha

۳. یافته‌ها

توصیف آماری ویژگی‌های نمونه نشان داد میانگین سابقه اشتغال برای مشارکت‌کنندگان برابر ۱۵/۰۳ سال بود. کمترین میزان سابقه برابر ۱ سال و بیشترین میزان آن برابر با ۲۹ سال به دست آمد (جدول ۲).

جدول (۲). سابقه اشتغال کارشناسان پاسخگو در نمونه مورد مطالعه (برحسب سال)

میانگین	میانه	مد	دامنه	کمترین	بیشترین
۱۵/۰۳	۱۵	۱۲	۲۸	۱	۲۹

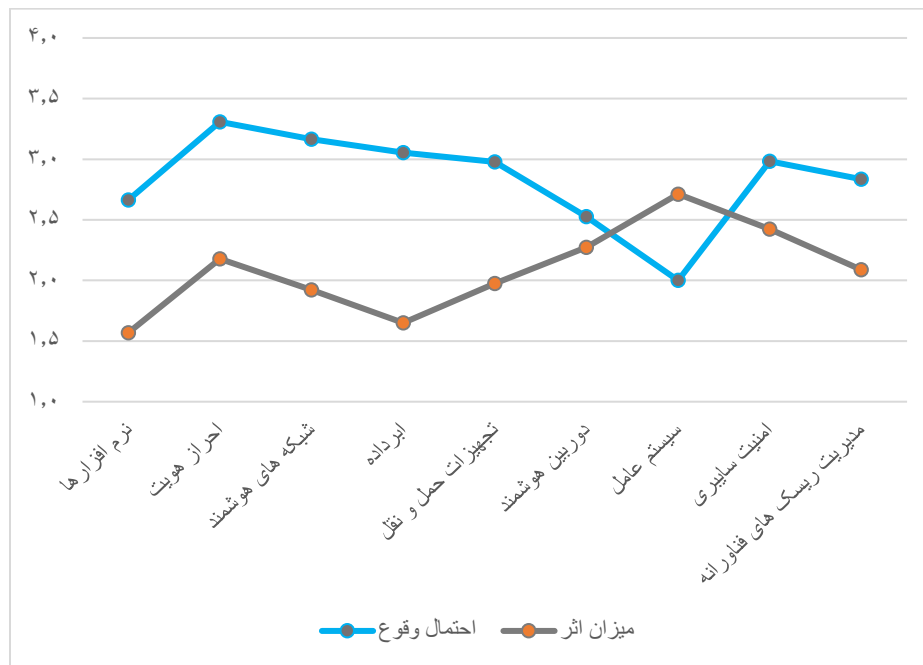
بر اساس جدول (۲) میانگین مؤلفه‌های مدیریت ریسک‌های فناورانه در سازمان‌های مدیریت شهری هوشمند در شهرداری تبریز مورد بررسی قرار گرفته است. در این زمینه، بیشترین میانگین در رابطه با احتمال وقوع، برای مؤلفه‌های احراز هویت برابر ۳/۳۱ و سپس شبکه حمل و نقل برابر ۳/۱۶ حاصل شد، در این زمینه کمترین میزان میانگین نیز برای مؤلفه سیستم عامل‌ها برابر ۲ به دست آمد. در رابطه با میزان تأثیر مؤلفه‌های مدیریت ریسک‌های فناورانه از نگاه مدیریت هوشمند شهری، بیشترین میزان میانگین برای مؤلفه سیستم عامل‌ها برابر ۲/۷۱ و سپس مؤلفه امنیت سایبری برابر ۲/۴۲ حاصل شد، در این زمینه کمترین میزان میانگین نیز برای مؤلفه نرم‌افزارها برابر ۱/۵۷ به دست آمد.

جدول (۳). آمار توصیفی مؤلفه‌های ریسک‌های فناورانه

مؤلفه / بعد	میزان تأثیر		احتمال وقوع	
	میانگین	انحراف معیار	میانگین	انحراف معیار
نرم‌افزارها	۱/۵۷	۰/۶۱	۲/۶۶	۰/۷۳
احراز هویت	۲/۱۸	۰/۴۹	۳/۳۱	۰/۵۷
شبکه‌های هوشمند	۱/۹۲	۰/۴۰	۳/۱۶	۰/۶۷
ابر داده	۱/۶۵	۰/۳۴	۳/۰۵	۰/۵۷
تجهیزات حمل و نقل	۱/۹۸	۰/۴۴	۲/۹۸	۰/۵۲
دوربین هوشمند	۲/۲۷	۰/۳۷	۲/۵۳	۰/۵۵
سیستم عامل	۲/۷۱	۰/۳۷	۲	۰/۵۶
امنیت سایبری	۲/۴۲	۰/۳۶	۲/۹۸	۰/۴۴
مدیریت ریسک‌های فناورانه	۲/۰۹	۰/۳۳	۲/۸۳	۰/۵۱

هم‌چنین، شکل (۳) به بررسی میانگین‌های به دست آمده پرداخته است. بر اساس نتایج به دست آمده مشخص شد که میانگین‌های ابعاد پژوهش در رابطه با میزان احتمال وقوع ریسک‌های فناورانه در سطحی بالاتر نسبت به میزان تأثیر آن از نگاه نمونه مورد مطالعه در

مدیریت شهر هوشمند در شهر تبریز دارد. در این رابطه مؤلفه سیستم‌عامل‌ها حالت معکوس نسبت به سایر شاخص‌ها داشت و میزان احتمال وقوع آن در سطحی کمتر قرار داشت.



شکل (۳): بررسی میانگین‌های مدیریت ریسک‌های فناورانه در مدیریت شهری شهرداری تبریز

برای ارزیابی وضعیت شاخص‌های پژوهش از منظر احتمال وقوع ریسک‌های فناورانه و میزان تأثیر مدیریت ریسک مدیریت شهری در رابطه با تهدیدات فناورانه از منظر شهر هوشمند در شهرداری تبریز از آزمون T تک نمونه‌ای استفاده شد. آزمون فوق در سطح اطمینان ۹۵٪ انجام شد. در این رابطه با توجه به ۵ طیفی بودن گویه‌ها، سنجش و تحلیل ابعاد در سطح نرمال (میانگین ۳) مورد ارزیابی قرار گرفت. در رابطه با میزان اثرگذاری مدیریت ریسک‌های فناورانه، نتایج بیانگر این بود که اثرگذاری مدیریت ریسک فناورانه در شهرداری تبریز برای تمام مؤلفه‌های مطرح‌شده در سطحی پایین‌تر از نرمال قرار گرفته و در وضعیت نامناسب است، میزان آماره t با درجه آزادی ۷۲ برای ابعاد پژوهش منفی و در سطح اطمینان یا معناداری $p \leq 0.01$ به دست آمد، در این خصوص بیشترین ضعف در مدیریت ریسک‌ها را می‌توان برای مؤلفه نرم‌افزار دانست که نگاه کارشناسان در زمینه مسائل مانند اختلال عملکردی و نقض امنیت (ویروسی شدن و ازکارافتادن نرم‌افزارها، دسترسی افراد ناشناس و کنترل نرم‌افزارها)، خوش‌بینانه نبود؛ جدول (۴).

جدول (۴). وضعیت میزان تأثیر مدیریت ریسک در رابطه با تهدیدات فناوریانه در شهرداری تبریز بر اساس آزمون T تک نمونه‌ای

Test value = 3 وضعیت نرمال						بعد / متغیر
وضعیت	معناداری P	آماره t	درجه آزادی	انحراف معیار	اختلاف میانگین	
کمتراز نرمال	۰/۰۰۰	-۱۹/۹	۷۲	۰/۶۱	-۱/۴۳	نرم‌افزارها
کمتراز نرمال	۰/۰۰۰	-۱۴/۱۷	۷۲	۰/۴۹	-۰/۸۲	احراز هویت
کمتراز نرمال	۰/۰۰۰	-۲۲/۶۵	۷۲	۰/۴	-۱/۰۷	شبکه‌های هوشمند
کمتراز نرمال	۰/۰۰۰	-۳۳/۸۶	۷۲	۰/۳۴	-۱/۳۴	ابر داده
کمتراز نرمال	۰/۰۰۰	-۱۹/۸۵	۷۲	۰/۴۴	-۱/۰۲	تجهیزات حمل‌ونقل
کمتراز نرمال	۰/۰۰۰	-۱۶/۷۳	۷۲	۰/۳۷	-۰/۷۲	دوربین هوشمند
کمتراز نرمال	۰/۰۰۰	-۶/۶۱	۷۲	۰/۳۷	-۰/۲۹	سیستم‌عامل
کمتراز نرمال	۰/۰۰۰	-۳/۳۸	۷۲	۰/۳۶	-۰/۵۷	امنیت سایبری
کمتراز نرمال	۰/۰۰۰	-۲۳/۱۳	۷۲	۰/۳۳	-۰/۹۱	مدیریت ریسک‌های فناوریانه

نتایج به‌دست‌آمده در رابطه با احتمال وقوع ریسک‌های فناوریانه در سازمان‌های مدیریت شهری در شهرداری تبریز بیانگر این بود که مؤلفه‌های شبکه‌های هوشمند با میزان آماره t ، $۲/۰۸$ در سطح اطمینان یا معناداری $p \leq ۰/۰۵$ و احراز هویت با میزان آماره $۴/۵۸$ در سطح اطمینان یا معناداری $p \leq ۰/۰۱$ ، در سطحی بالاتر از وضعیت نرمال قرار دارند، در رابطه با شبکه‌های هوشمند می‌توان به حملات سایبری به شبکه‌های آب و برق و گاز اشاره نمود که از منظر کارشناسان احتمال وقوع این حملات در سطحی فراتر از نرمال قرار دارد، هم‌چنین در رابطه با احراز هویت نیز می‌توان به حمله فیزیکی و آسیب به دستگاه‌ها اشاره نمود. در این خصوص احتمال وقوع تهدیدات و ریسک‌های فناوریانه در سازمان مدیریت شهری برای مؤلفه‌های تجهیزات حمل‌ونقل و ابر داده‌ها از نگاه کارشناسان در شهرداری تبریز در وضعیت نرمال یا تقریباً نرمال قرار داشتند، چراکه اختلاف میانگین مؤلفه‌های مطرح‌شده با سطح نرمال (۳) فاقد تفاوت معنادار بودند. هم‌چنین احتمال وقوع ریسک‌های فناوریانه در مؤلفه‌های نرم‌افزارها، دوربین هوشمند و سیستم‌عامل کمتر از سطح نرمال یا میانگین متوسط قرار دارند، میزان آماره t با درجه آزادی ۵۴ برای بعد پژوهش منفی و در سطح اطمینان یا معناداری $p \leq ۰/۰۱$ به دست آمد، جدول (۵).

جدول (۵). وضعیت احتمال وقوع ریسک‌های فناورانه از منظر مدیریت هوشمند در شهرداری تبریز بر اساس آزمون T تک نمونه‌ای

وضعیت	Test value = 3 وضعیت نرمال					بعد / متغیر
	معناداری P	آماره t	درجه آزادی	انحراف معیار	اختلاف میانگین	
کمتراز نرمال	۰/۰۰۰	-۳/۹۲	۷۲	۰/۷۳	-۰/۳۳	نرم‌افزارها
بیشتر از نرمال	۰/۰۰۰	۴/۵۸	۷۲	۰/۵۷	۰/۳۱	احراز هویت
بیشتر از نرمال	۰/۰۴۱	۲/۰۸	۷۲	۰/۶۷	۰/۱۶	شبکه حمل و نقل
در سطح نرمال	۰/۴۱۹	۰/۸۱	۷۲	۰/۵۷	۰/۰۵	ابر داده
در سطح نرمال	۰/۷۱۹	-۰/۳۶	۷۲	۰/۵۱	-۰/۰۲	تجهیزات حمل و نقل
کمتراز نرمال	۰/۰۰۰	-۷/۲۹	۷۲	۰/۵۵	-۰/۴۷	دوربین هوشمند
کمتراز نرمال	۰/۰۰۰	-۱۵/۰۳	۷۲	۰/۵۶	-۱	سیستم عامل
در سطح نرمال	۰/۷۴۲	-۰/۳۳	۷۲	۰/۴۴	-۰/۰۲	امنیت سایبری
کمتراز نرمال	۰/۰۰۷	-۲/۷۶	۷۲	۰/۵۱	-۰/۱۶	مدیریت ریسک‌های فناورانه

در این مبحث به شناسایی میزان اثرگذاری مدیریت ریسک و احتمال وقوع ریسک‌های فناورانه در شهرداری تبریز بر اساس مدل معادلات ساختاری در نرم‌افزار AMOS پرداخته شده است. با توجه این نکته که پژوهش حاضر فاقد متغیر ملاک و پیش‌بین بوده برای بررسی و شناسایی مهم‌ترین اثرات و تهدیدهای (احتمال وقوع) مدیریت ریسک‌های فناورانه در نمونه مورد مطالعه از ساختار عاملی (تحلیل عامل مرتبه دوم) به روش حداکثر درست‌نمایی استفاده شد.

برای تعیین اینکه کدام یک از شاخص‌های برازندگی برآورد بهتری از مدل فراهم می‌کند، توافق عمومی و کلی میان متخصصین معادلات ساختاری وجود ندارد؛ از این رو پیشنهاد می‌شود ترکیبی از ۵ شاخص گزارش شود. در پژوهش حاضر به منظور ارزیابی نیکویی-برازش مدل از شاخص‌های مطلق (برازندگی مدل) کای اسکور^{۱۷}، درجه آزادی^{۱۸}، سطح معناداری، نسبت کای اسکور به درجه آزادی و شاخص‌های نسبی ریشه خطای میانگین مجزورات برآورد^{۱۹}، شاخص برازش تطبیقی^{۲۰} و شاخص برازش تطبیقی مقتصد^{۲۱} استفاده شد. با توجه به تعداد نمونه مورد مطالعه می‌توان بیان کرد که شاخص‌های برازش مدل در محدوده قابل قبول قرار داشته و دارای برازش خوبی بوده و شاخص RMSEA که مهم‌ترین شاخص در این زمینه هست در رابطه با اثرات برابر ۰/۰۵۳ و احتمال وقوع برابر ۰/۰۶۱ به دست آمد که در محدوده کمترین و بیشترین فاصله اطمینان برای معناداری مدل، قرار داشتند و بیانگر

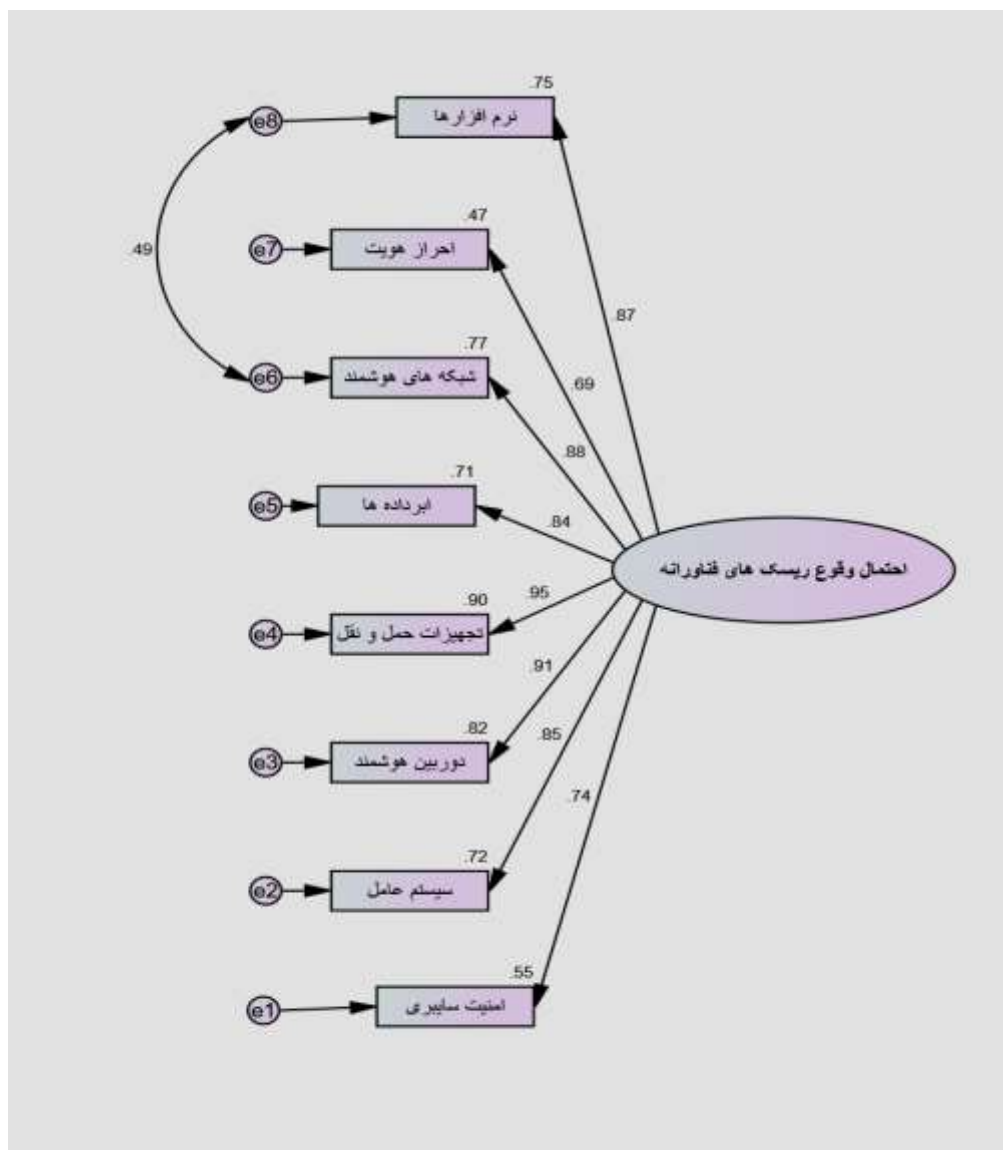
۱۷. χ^2
 ۱۸. df
 ۱۹. RMSEA
 ۲۰. CFI
 ۲۱. PCFI

این بود که مدل‌ها مذکور در سطح خوبی قرار دارند. برازش نهایی مدل پس از استراتژی‌های آرایشی و ترسیم مسیرهای پیشنهادی مدل برای برخی شاخص‌ها و مسیرهای پیشنهادی بیان شده است جدول (۶).

جدول (۶): شاخص‌های برازش مدل‌های پژوهش

مقدار به دست آمده		محدوده قابل قبول	معیار برازش مدل	نوع شاخص
احتمال وقوع	میزان اثر			
۸۲/۷۲	۳۴/۳۱	+	کای اسکوتر	شاخص‌های مطلق (برازندگی مدل)
۲۸	۲۶	+	درجه آزادی	
۰/۰۸۵	۰/۱۱۲	$< ۰/۰۵$	سطح معناداری	
۲/۹۴	۱/۹۱	بین ۱/۵ تا ۳/۵	نسبت کای اسکوتر به درجه آزادی	
۰/۰۶۱	۰/۰۵۳	$> ۰/۰۸$	ریشه خطای میانگین مجذورات	شاخص‌های نسبی
۰/۹۰۸	۰/۹۵۲	$\leq ۰/۹۰$	شاخص برازش تطبیقی	
۰/۷۱۳	۰/۶۱۲	$\leq ۰/۶۰$	شاخص برازش تطبیقی مقتصد	

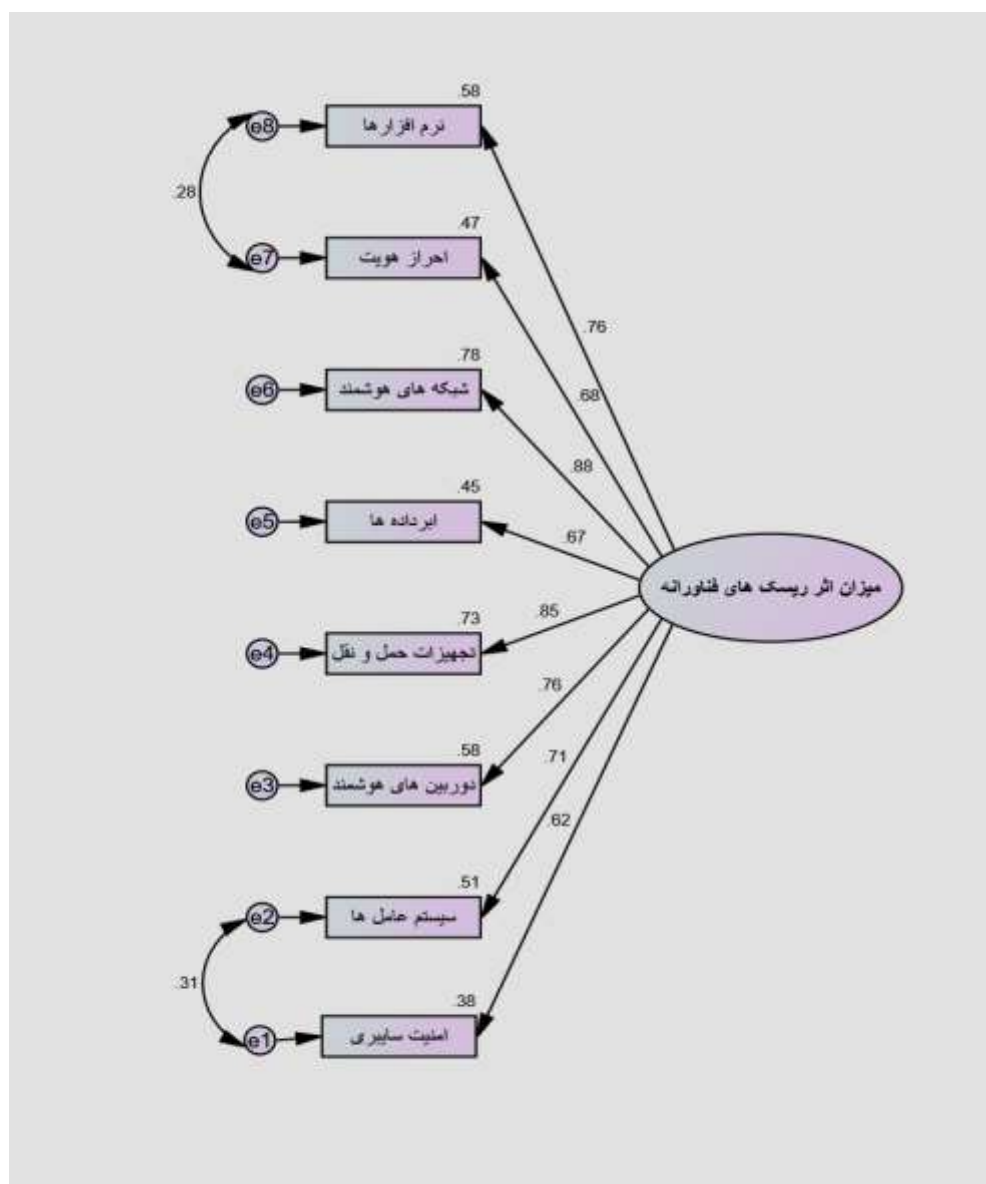
شکل (۴) به شناسایی احتمال وقوع ریسک‌های فناورانه در سازمان‌های مدیریت شهری در راستای مدیریت بهینه آن در شهرداری شهر تبریز پرداخته است. در این خصوص از روش تحلیل عامل مرتبه دوم، استفاده شد. بررسی و سنجش ابعاد پژوهش بیانگر این بود که مهم‌ترین ریسک بعد فناوری که احتمال وقوع آن از نگاه کارشناسان در شهرداری تبریز بیشتر است، تجهیزات حمل و نقل با میزان بار عاملی ۰/۹۵ در سطح معناداری ۰/۰۰۰ است. بنابراین از نگاه کارشناسان احتمال وقوع ریسک‌های فناورانه در این زمینه در بالاترین سطح ممکن در سازمان‌های مدیریت شهری قرار داشته که می‌تواند منجر به اختلال در رابطه با چراغ‌های راهنمایی و رانندگی، سیستم کنترل شبکه‌های حمل و نقل عمومی، فناوری تنظیم‌کننده ترافیک و ایمنی روشنی شده و سبب بروز چالش‌هایی در این زمینه گردد. پس از آن، می‌توان به مؤلفه دوربین‌های هوشمند اشاره نمود که احتمال وقوع در این زمینه به میزان بار عالی ۰/۹۱ بود که منجر به ایجاد اختلال در نظم عمومی جامعه و افزایش جرم و جنایت گردد. سپس، به ترتیب اولویت مؤلفه‌های شبکه‌های هوشمند با وزنی رگرسیونی ۰/۸۸، نرم‌افزارها به میزان وزن رگرسیونی یا بار عاملی ۰/۸۷، سیستم‌عامل‌ها با میزان بار ۰/۸۵، ابر داده‌ها با میزان اثر ۰/۸۴، امنیت سایبری به میزان ۰/۷۴ و در نهایت احراز هویت با بار عاملی ۰/۶۹ در سطح معناداری ۰/۰۰۰ اشاره نمود.



شکل (۴): مدل نهایی پژوهش در رابطه با احتمال وقوع ریسک های فناوریانه

شکل (۵) به شناسایی مؤلفه های مؤثر ریسک های فناوریانه در سازمان های مدیریت شهری در راستای مدیریت بهینه آن در شهرداری شهر تبریز پرداخته است. در این خصوص از روش تحلیل عامل مرتبه دوم، استفاده شد. بررسی و سنجش ابعاد پژوهش بیانگر این بود که مهم ترین ریسک های اثرگذار در سازمان مدیریت شهری در رابطه با بعد فناوری از نگاه کارشناسان در شهرداری تبریز، با اثرگذاری شگرف، شبکه های هوشمند با میزان بار عاملی $0/88$ در سطح معناداری $0/000$ است. بنابراین از نگاه کارشناسان مهم ترین اثرگذاری ریسک های فناوریانه می تواند منجر به اختلال بین سیستم ها، ذخیره سازی و پردازش داده ها در صورت حمله سایبری به شبکه های آب، برق و گاز اشاره نمود که سبب بروز چالش هایی در این زمینه می شود. پس از آن، می توان به مؤلفه تجهیزات حمل و نقل اشاره نمود که سبب اختلال در سیستم های شبکه حمل و نقل می گردد و شبکه حمل و نقل در مواقع بحران از مهم ترین عناصر کلیدی در ساختار فضایی هست که وزن رگرسیونی آن برابر $0/85$ حاصل شد. سپس، به ترتیب اولویت مؤلفه های دوربین های هوشمند و

نرم افزارها با وزنی رگرسیونی ۰/۷۶، سیستم عامل ها با میزان بتا ۰/۷۱، احراز هویت با بار عاملی ۰/۶۸، ابر داده ها با میزان اثر ۰/۶۷ و در نهایت امنیت سایبری با بار عاملی ۰/۶۲ در سطح معناداری ۰/۰۰۰ بودند.



شکل (۵): مدل نهایی پژوهش در رابطه با میزان اثرگذاری ریسک های فناوریانه

در نهایت در جدول (۷) به بررسی میزان احتمال وقوع و اثرگذاری ریسک های فناوریانه و مقایسه رتبه آن ها پرداخته شده است. بر اساس نتایج مشخص شد که نگاه کارشناسان بر ریسک های فناوریانه از لحاظ احتمال وقوع به ترتیب چهار مؤلفه ی: تجهیزات حمل و نقل، دوربین های هوشمند، شبکه حمل و نقل و نرم افزارها هست. از لحاظ میزان اثرگذاری نیز مؤلفه های: شبکه های هوشمند، تجهیزات حمل و نقل، نرم افزارها و دوربین های هوشمند بودند.

جدول (۷): بررسی میان احتمال وقوع و اثرگذاری ریسک‌های فناورانه

احتمال وقوع		مؤلفه	اثرگذاری	
رتبه در احتمال وقوع	بار عاملی		بار عاملی	رتبه در اثرگذاری
۴	۰/۸۷	نرم افزارها	۰/۷۶	۳
۸	۰/۶۹	احراز هویت	۰/۶۸	۶
۳	۰/۸۸	شبکه‌های هوشمند	۰/۸۸	۱
۶	۰/۸۴	ابر داده	۰/۶۷	۷
۱	۰/۹۵	تجهیزات حمل و نقل	۰/۸۵	۲
۲	۰/۹۱	دوربین هوشمند	۰/۷۶	۳
۵	۰/۸۵	سیستم عامل	۰/۷۱	۵
۷	۰/۷۴	امنیت سایبری	۰/۶۲	۸

۴. بحث

یافته‌های پژوهش حاضر نشان می‌دهد که ریسک‌های فناورانه مرتبط با تجهیزات حمل و نقل هوشمند، دوربین‌ها، شبکه‌های هوشمند و نرم افزارهای مدیریتی بیشترین احتمال وقوع و اثرگذاری را دارند. این موضوع حاکی از آن است که آسیب‌پذیری شهر هوشمند تبریز عمدتاً در حوزه‌هایی متمرکز است که بیشترین وابستگی به فناوری اطلاعات و ارتباطات دارند. تحلیل آماری نشان داد که علی‌رغم توسعه زیرساخت‌های فناورانه، ظرفیت نهادی و آمادگی سازمانی برای مدیریت تهدیدها پایین‌تر از سطح مطلوب است؛ به بیان دیگر، کارشناسان وقوع تهدیدهای فناورانه را محتمل می‌دانند اما توان مقابله و کاهش اثرات آن را ضعیف ارزیابی کرده‌اند. این شکاف میان احتمال وقوع بالا و اثرگذاری پایین نشان‌دهنده ضعف سیستماتیک در راهبردهای پیشگیرانه و تاب‌آوری دیجیتال شهری است. نتایج تفصیلی مؤلفه‌ها نیز نکات قابل توجهی را روشن می‌سازد: نرم افزارها پایین‌ترین سطح اثرگذاری را دارند که می‌تواند ناشی از نبود سیاست‌های به‌روزرسانی منظم، ضعف پشتیبانی و مدیریت آسیب‌پذیری‌های امنیتی باشد. در مقابل، احراز هویت و شبکه‌های هوشمند از نظر احتمال وقوع در وضعیت هشداردهنده قرار دارند که نشان‌دهنده افزایش تهدیدهای سایبری و حملات احتمالی به زیرساخت‌های

داده‌محور شهری است. اولویت‌بندی ریسک‌ها نیز نشان داد که از نظر احتمال وقوع، تجهیزات حمل‌ونقل، دوربین‌های هوشمند، شبکه‌های هوشمند و نرم‌افزارها در صدر هستند؛ اما از نظر میزان اثرگذاری، شبکه‌های هوشمند، تجهیزات حمل‌ونقل، نرم‌افزارها و دوربین‌های هوشمند اهمیت بیشتری دارند. این همپوشانی نسبی، تمرکز ریسک‌های فناورانه در بخش‌هایی با وابستگی حیاتی به ICT را تأیید می‌کند.

در مطالعات خارجی، سانجایا و همکاران (۲۰۲۵) ریسک‌های فنی، غیر فنی و زیست‌محیطی را بررسی کرده و اثر آن‌ها بر ابعاد اقتصادی، اجتماعی و محیط‌زیستی را تحلیل کرده‌اند؛ برخلاف پژوهش حاضر که تمرکز محدود بر ریسک‌های فناورانه شهری و رتبه‌بندی آن‌ها بر اساس احتمال و اثرگذاری دارد، یافته‌های سانجایا و همکاران نشان می‌دهد که تحلیل جامع ریسک‌ها می‌تواند درک وسیع‌تری از پیامدهای فناوری فراهم کند، اما پژوهش حاضر بیش از عملیاتی و اولویت‌بندی ریسک‌ها برای تصمیم‌گیری مدیریت شهری را ارائه می‌دهد. همچنین، دین و همکاران (۲۰۲۱) بر چالش‌های پذیرش فناوری اینترنت اشیا و مدیریت امنیت سیستم‌های اطلاعاتی متمرکز بوده‌اند؛ پژوهش حاضر با تحلیل میدانی شهرداری تبریز و رتبه‌بندی ریسک‌های فناورانه، امکان‌شناسایی نقاط بحرانی فناوری و مدیریت پیشگیرانه ریسک‌ها را فراهم می‌کند و بیش از عملیاتی جدیدی نسبت به مطالعات مروری ارائه می‌دهد. در مطالعات داخلی، یافته‌های پژوهش حاضر با نتایج جبار زاده و همکاران (۱۳۹۹) و نظم‌فر و همکاران (۱۴۰۳) همسو است؛ با این تفاوت که پژوهش حاضر بر تحلیل بیرونی و رتبه‌بندی ریسک‌ها تمرکز دارد و نشان می‌دهد که حتی در صورت رفع موانع اقتصادی و نهادی، ضعف زیرساخت‌های فناوری و تاب‌آوری سیستم‌ها می‌تواند تحقق شهر هوشمند را محدود کند. این یافته‌ها تأکید می‌کند که مدیریت مؤثر ریسک‌های فناورانه نیازمند ارتقای هم‌زمان زیرساخت‌ها، تاب‌آوری سازمانی و هماهنگی زنجیره‌ای خدمات شهری است. تحلیل ادبیات نشان می‌دهد که اغلب پژوهش‌های مرتبط با ابعاد مدیریتی و سیاست‌گذاری تمرکز داشته‌اند یا بر امنیت سایبری و فناوری. پژوهش حاضر با ترکیب این دو رویکرد و ارائه چارچوب تجربی و کاربردی برای شناسایی و اولویت‌بندی ریسک‌های فناورانه در شهرداری تبریز، جایگاه علمی متمایزی ایجاد می‌کند. سهم علمی این پژوهش را می‌توان در سه سطح خلاصه کرد. ۱) ارائه چارچوب عملیاتی مدیریت ریسک‌های فناورانه: با تمرکز بر داده‌های میدانی و شواهد واقعی، پژوهش ابزار کاربردی برای مدیران شهری فراهم کرده است، ۲) تبیین شکاف میان بلوغ فناوری و بلوغ مدیریتی: نشان می‌دهد توسعه فناوری بدون ارتقای ظرفیت مدیریتی می‌تواند به افزایش آسیب‌پذیری منجر شود، ۳) اولویت‌بندی مؤلفه‌های ریسک برای تصمیم‌گیری: نتایج پژوهش مبنای تخصیص منابع، تقویت امنیت سایبری و برنامه‌ریزی عملیاتی در مدیریت شهری خواهد بود. درنهایت، پژوهش حاضر چارچوبی تحلیلی و راهبردی برای کاهش اثرات منفی

و ارتقای تاب‌آوری شهری ارائه می‌دهد و می‌تواند مدیران شهری را در برنامه‌ریزی، تخصیص منابع و تصمیم‌گیری پیشگیرانه هدایت کند.

۵. نتیجه‌گیری

شهرهای هوشمند از نظر نوع خدمات ارائه‌شده با شهرهای سنتی تفاوت اساسی دارند؛ چراکه خدمات آن‌ها صرفاً محدود به استفاده از اجزای فنی مانند حسگرها، عملگرها و دستگاه‌های هوشمند نیست، بلکه عناصر کلیدی دیگری نظیر داده‌ها، نرم‌افزارها، سیاست‌ها و ذی‌نفعان نیز نقش مهمی در ساختار این شهرها ایفا می‌کنند. با گسترش فناوری‌های نوآورانه، سطح پیچیدگی و عدم قطعیت در محیط شهری افزایش یافته و ضرورت دارد که مدیریت ریسک در این فضا صرفاً به جنبه‌های فنی محدود نشود، بلکه ابعاد مدیریتی، ساختاری و سیاست‌گذاری نیز موردتوجه قرار گیرد. نتایج این پژوهش به‌روشنی نشان داد که وضعیت مدیریت ریسک‌های فناوریانه در شهرداری تبریز، به‌ویژه در حوزه مدیریت شهری هوشمند، در سطحی پایین‌تر از وضعیت مطلوب و نرمال قرار دارد. تحلیل‌های آماری بیانگر آن بود که علی‌رغم گسترش زیرساخت‌های فناوریانه در مدیریت شهری، آمادگی نهادی و ساختار مدیریتی در مواجهه با تهدیدات فناوریانه هم‌تراز با میزان توسعه فناوری پیش نرفته است. بررسی توصیفی متغیرها نشان داد که میانگین مؤلفه‌های مربوط به احتمال وقوع ریسک‌های فناوریانه بالاتر از میانگین مؤلفه‌های تأثیر و اثرگذاری این ریسک‌ها ارزیابی شده است؛ این موضوع حاکی از آن است که کارشناسان شهرداری تبریز وقوع تهدیدات فناوریانه را محتمل می‌دانند، اما ظرفیت مدیریتی و کنترلی لازم برای کاهش اثرات آن را ضعیف ارزیابی می‌کنند. درواقع، ادراک وقوع ریسک در سطح هشداردهنده‌ای قرار دارد، اما ادراک آمادگی سازمانی در سطح پایین‌تری است. بر اساس نتایج آزمون تک نمونه‌ای، تمامی مؤلفه‌های اثرگذاری مدیریت ریسک‌های فناوریانه در سطحی کمتر از نرمال قرار داشتند؛ این امر نشان‌دهنده ضعف سیستماتیک در راهبردهای پیشگیرانه، واکنشی و مقاوم‌سازی فناوری‌های شهری است. در میان مؤلفه‌ها، نرم‌افزارها پایین‌ترین سطح اثرگذاری را داشتند که می‌تواند ناشی از فقدان سیاست‌های به‌روزرسانی منظم نرم‌افزارها، عدم پشتیبانی مناسب، و ضعف در مدیریت آسیب‌پذیری‌های امنیتی باشد. از سوی دیگر، مؤلفه‌هایی نظیر احراز هویت و شبکه‌های هوشمند در بُعد احتمال وقوع، بالاتر از نرمال ارزیابی شدند که نشان‌دهنده افزایش تهدیدات سایبری و حملات احتمالی به زیرساخت‌های داده محور شهری است.

مقایسه نهایی رتبه‌بندی مؤلفه‌ها نشان داد که از نظر احتمال وقوع، اولویت تهدیدها به ترتیب شامل تجهیزات حمل‌ونقل، دوربین‌های هوشمند، شبکه‌های هوشمند و نرم‌افزارهاست، درحالی‌که از نظر میزان اثرگذاری، اولویت‌ها به ترتیب شبکه‌های هوشمند، تجهیزات حمل‌ونقل، نرم‌افزارها و دوربین‌های هوشمند می‌باشند. این همپوشانی نسبی در دو بُعد وقوع و اثرگذاری نشان می‌دهد که ریسک‌های فناوریانه در شهرداری تبریز عمدتاً در حوزه‌هایی متمرکزند که بیشترین وابستگی به فناوری اطلاعات و ارتباطات دارند. در جمع‌بندی نهایی می‌توان گفت که شهرداری تبریز از منظر مدیریت

ریسک‌های فناوریانه، در مرحله شناخت و آگاهی قرار دارد و هنوز به مرحله کنش راهبردی و یکپارچه‌سازی نظام‌مند نرسیده است. شکاف میان احتمال وقوع بالا و اثرگذاری پایین، بیانگر ضعف در زیرساخت‌های مدیریتی، نارسایی در تدوین سیاست‌های امنیت فناوری و کمبود ظرفیت نهادی برای پاسخ به بحران‌های فناوریانه است. از این‌رو، بازنگری در نظام مدیریت ریسک، ایجاد مرکز تخصصی ارزیابی تهدیدات فناوریانه، آموزش کارشناسان فناوری و استقرار سامانه‌های نظارت بلادرنگ می‌تواند گام‌های اساسی برای ارتقای تاب‌آوری دیجیتال و پایداری شهر هوشمند تبریز باشد. با توجه به نتایج پژوهش می‌توان راهکارهای زیر را به‌عنوان پیشنهاد ارائه داد:

۱. تقویت ظرفیت فنی

- برگزاری دوره‌های آموزشی برای کارکنان شهرداری و نیروهای فنی درباره فناوری‌های شهر هوشمند.
- استفاده از فناوری‌های امتحان شده و استاندارد تا احتمال خرابی سیستم‌ها کمتر شود.
- ایجاد گروه پشتیبانی فنی در شهرداری برای رفع سریع مشکلات سیستم‌های هوشمند.

۲. اجتماعی سازی مقررات

- برگزاری جلسات با دانشگاه تبریز، بخش خصوصی و مردم برای هماهنگی در اجرای پروژه‌ها.
- اطلاع‌رسانی شفاف درباره قوانین، مقررات و هزینه‌های پروژه‌های شهر هوشمند.
- جلوگیری از تغییر مکرر قوانین با هماهنگی بین نهادهای مختلف.

۳. مشارکت جامعه

- اطلاع‌رسانی ساده و شفاف به مردم درباره فواید شهر هوشمند از طریق رسانه‌های محلی.
- گرفتن نظر مردم در مورد پروژه‌های جدید (مثلاً از طریق اپلیکیشن شهرداری یا نظرسنجی محله‌ای).
- اجرای چند پروژه کوچک آزمایشی در محله‌های مختلف تبریز تا مردم نتیجه را از نزدیک ببینند.

۴. حفظ محیط‌زیست

- نصب حس گرهای هوشمند برای کنترل آلودگی هوا و آب.
- اجرای طرح‌های هوشمند برای تفکیک زباله و جمع‌آوری پسماند.

فهرست منابع

- برنر، گ.؛ آلیس، گ.، و فرینگا، آ. (۱۳۸۵). مدیریت ریسک در سیستم‌های فناوری اطلاعات. قزوین. انتشارات سایه‌گستر.
- رضایی، ف؛ فیروز علیزاده، ا. پورمحمدی، ا. (۱۳۹۹). رابطه توانایی مدیریت با اجزاء مدیریت ریسک یکپارچه. پژوهش‌های حسابداری مالی و حسابرسی. دوره ۱۲، شماره ۴۸، ۲۳-۴۱.
- روستایی، ش.، پورمحمدی، م.ر.، و قنبری، ح. (۱۳۹۷). تئوری شهر هوشمند و ارزیابی مؤلفه‌های زیرساختی آن در مدیریت شهری مورد شناسی: شهرداری تبریز. جغرافیا و آمایش شهری - منطقه‌ای، ۸(۲۶)، ۱۹۷-۲۱۶.
- ریسک‌های جهان گزارش ۲۰۲۲. معاونت بررسی‌های اقتصادی اتاق بازرگانی، صنایع، معادن و کشاورزی تهران
- زنجانی، م؛ نجفی، ا.، نقی‌لو، ا.، محمدی، ن. (۱۳۹۹). تبیین فرا تحلیل مسائل زنجیره تأمین و مدیریت ریسک. نشریه کاوش‌های مدیریت بازرگانی، ۱۲ (۲۳)، ۲۱۸-۲۵۳.
- زینالی عظیم، ع. (۱۴۰۱). تحلیل دل‌بستگی مکانی در شهر تبریز با به‌کارگیری مقیاس شهرهای هوشمند در دوران بیماری کووید ۱۹. مجله پژوهش‌های جغرافیای برنامه‌ریزی شهری. ۱۰(۳)، ۶۵-۸۰.
- طهماسبی زاده، پ؛ رجب‌پور، م.، فیلی، ر. (۱۳۹۹). مروری بر چالش‌های امنیتی دستگاه‌های موبایل اندروید متصل به اینترنت اشیا. یازدهمین کنفرانس بین‌المللی فناوری اطلاعات، کامپیوتر و مخابرات
- کاظمی مهر، م. (۱۳۹۶). معماری سیستم جامع بانکی و طراحی مدل ایمن موبایل بانک جهت انجام تراکنش‌های آنلاین. گزارش پایان پروژه برای دریافت درجه کارشناسی ارشد در رشته معمار ارشد سرویس در سامانه‌های جامع بانکی. دانشگاه جامع علمی- کاربردی، تهران
- Aithal, P. S. (2022). ICT and digital technology based solutions for smart city challenges and opportunities. *International journal of applied engineering and management letters (ijaeml)*, 6(1), 1-21.
- Button, K. (2002). City management and urban environmental indicators. *Ecological economics*, 40(2), 217-233
- Carraminana, D., Bernardos, A. M., Besada, J. A., & Casar, J. R. (2024). Towards resilient cities: A hybrid simulation framework for risk mitigation through data-driven decision making. *Simulation Modelling Practice and Theory*, 133, 102924.
- Din, Z., Jambari, D. I., Yusof, M. M., & Yahaya, J. (2021). Challenges in iot technology adoption into information system security management of smart cities: a review. *Advances in Science, Technology and Engineering Systems Journal*, 6(2), 99-112.
- Godin, B. (2004). The obsession for competitiveness and its impact on statistics: the construction of high-technology indicators. *Research Policy*, 33(8), 1217-1229

- Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2022). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. *Information Systems Frontiers*, 24(2), 393-414.
- Kitchin, R., & Dodge, M. (2020). The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention. In *Smart cities and innovative Urban technologies* (pp. 47-65). Routledge.
- Kummitha, R. K. R. (2020). Why distance matters: The relatedness between technology development and its appropriation in smart cities. *Technological Forecasting and Social Change*, 157, 120087
- Lacambra, S., Jaimes, I., Sanahuja, H., Torres, A. M., Visconti, E. & Benjamin, L. (2018). Index of governance and public policy in disaster risk management (IGOPP). National Report for The Bahamas,
- Nam, K., Dutt, C. S., Chathoth, P., & Khan, M. S. (2021). Blockchain technology for smart city and smart tourism: latest trends and challenges. *Asia Pacific Journal of Tourism Research*, 26(4), 454-468
- Sanjaya, I. P. A., Sudarsana, D. K., Yana, A. A. G. A., Dewi, A. A. D. P., & Dwijendra, N. K. A. (2025). Risk Management Study in Smart City Development: Challenges and Opportunities in Bali. *ASTONJADRO*, 14(2), 415-421.
- Scuotto, V., Ferraris, A., & Bresciani, S. (2016). Internet of Things: Applications and challenges in smart cities: a case study of IBM smart city projects. *Business process management journal*, 22(2), 357-367.
- Singh, P., & Helfert, M. (2019, September). Smart Cities and Associated Risks: Technical v/s Non-technical Perspective. In *CHIRA* (pp. 221-228).
- Ullah, F., Qayyum, S., Thaheem, M. J., Al-Turjman, E., & Sepasgozar, S. M. (2021). Risk management in sustainable smart cities governance: A TOE framework. *Technological Forecasting and Social Change*, 167, 120743.