مقاله پژوهشی

راهبردهای بکارگیری اینترنت اشیا در مأموریت‌های پلیس آگاهی

بهزاد لک[1]

تاریخ دریافت: ۱۳۹۸/۰۷/۰۱
تاریخ پذیرش: ۱۳۹۸/۱۰/۱۱

چکیده

زمینه و هدف: به‌طور طبیعی، پلیس در آینده باید از تجهیزات هوشمند متصل به دنیای اینترنت اشیا استفاده کند. با عنایت به مهاجرت سیستم‌ها و فرایندهای سنتی پلیس به فرایندهای جدید و امکان وقوع مشکلات خاص در این روند و تهدیدها و آسیب‌هایی که این مهاجرت به‌دنبال خواهد داشت، لازم است راهبردهای بکارگیری اینترنت اشیا در مأموریت‌های پلیس آگاهی بررسی شود.

روش: رویکرد پژوهش ترکیبی و از نوع اکتشافی است و ازنظر هدف کاربری است. در بخش کیفی نقاط قوت، ضعف، فرصت و تهدید بکارگیری اینترنت اشیا و ادوات و تجهیزات هوشمند در مأموریت‌های پلیس آگاهی استخراج شد. جامعه آماری بخش کیفی تمام‌شمار و شامل ۱۸ نفر از کارشناسان بود و اعتبارسنجی از طریق خبرگان انجام شد. جامعه آماری نفر و حجم نمونه ۲۰۰ نفر از کارشناسان مرتبط در پلیس آگاهی، معاونت فناوری اطلاعات و ارتباطات و پلیس فتا است که به روش نمونه‌گیری تصادفی ساده، انتخاب شدند. روش گردآوری داده‌ها، میدانی و ابزار آن مصاحبه و پرسشنامه است. با استفاده از تحلیل عاملی و نکویی برازش، روایی داده‌ها بررسی شد. پایایی و اعتبار پرسشنامه با محاسبه آلفای کرونباخ سنجیده شده است.

یافته‌ها: درخصوص شاخص‌های اس. دبلیو. اُ. تی از تحلیل عاملی تأییدی در قالب چهار فرضیه فرعی استفاده شد. امتیاز نهایی ماتریس ارزیابی داخلی ۲/۲۹ و خارجی ۲/۸۵ به‌دست آمده است؛ با توجه به اینکه نقطه (۲/۸۵، ۲/۲۹) در خانه (ضعف – فرصت) قرار دارد، راهبرد مناسب بکارگیری اینترنت اشیا در پلیس آگاهی راهبرد محافظه‌کارانه است.

نتایج: راهبرد محافظه‌کارانه هشدار می‌دهد که حرکت بی‌مهابا به‌سمت سامانه‌های اینترنتی و تجهیزات هوشمند متصل به دنیای شبکه، ممکن است آسیب‌ها و یا شکست را به‌دنبال داشته باشد و لازم است با احتیاط بیشتری بکارگیری شوند و الزامات سخت‌افزاری و نرم‌افزاری اینترنت اشیا در حوزه ارتباطات رادیویی، ارتباطات زیرساخت، فناوری اطلاعات، مراقبت الکترونیک و اینترنت و شبکه در پلیس آگاهی فراهم شوند.

کلیدواژه‌ها: تجهیزات هوشمند، اینترنت اشیا، پلیس آگاهی، زیرساخت فناوری اطلاعات، راهبردسنجی

❑ **استناد:** لک، بهزاد. (۱۳۹۹). راهبردهای بکارگیری اینترنت اشیا در مأموریت‌های پلیس آگاهی. *فصلنامهٔ پژوهش‌های مدیریت انتظامی*، ۱۵(۱)، صص ۷۵-۱۰۰.

۱. استادیار گروه فاوا، دانشکده علوم و فنون منابع سازمانی، دانشگاه علوم انتظامی امین. تهران. ایران. رایانامه: behzad1726@chmail.ir

مقدمه

اینترنت اشیا[1] ظرفیت بالقوه‌ای برای تبدیل شدن به مهمترین فناوری دنیا را دارد که در طی دهه‌های اخیر، انقلاب عظیمی در عرصه فناوری اطلاعات و ارتباطات ایجاد کرده است. این مفهوم جدید هم کاربردهای غیرنظامی (شهری) و هم کاربردهای نظامی را تحت تأثیر قرارداده است. در این میان کاربردهای نظامی و پلیسی اینترنت اشیا حائز اهمیت است، زیرا می‌تواند تأثیر مستقیم مثبت یا مخربی را در صحنه‌های نبرد به‌دنبال داشته باشد. از این رو مسائل امنیتی مرتبط با بخش‌های مختلف اینترنت اشیا نظامی بسیار حیاتی است. اینترنت اشیا کاربردهای متعددی در بخش‌های مختلف دیگر از قبیل شهرهای هوشمند، کشاورزی، بهداشت و پزشکی، صنعت، مدیریت بحران و بسیاری از بخش‌های دیگر دارد. با توجه به امکان جمع‌آوری داده ازطریق انواع برچسب[2]، فرستنده‌های رادیویی دارای کد شناسایی[3] و حسگرهای[4] مختلف در فناوری اینترنت اشیا، از این فناوری می‌توان در کاربردهای مختلف پلیس برای اعمال کنترل، پایش و نظارت دقیق و انجام بهتر مأموریت‌های پلیس استفاده کرد (براری و همکاران، ۱۳۹۵، ص۴۳-۴۴). در حال حاضر پلیس در مأموریت‌های خود از فرایندهای سنتی با ساختار تجهیزاتی فناوری متوسط و غیرهوشمند بهره می‌برد. مؤسسه آینده‌پژوهی گارتنر، ۱۰ پیش‌بینی خود از نوآوری در دنیای فناوری طی سال‌های آینده تا ۲۰۲۲ را اعلام کرده که در این میان اینترنت اشیا در دگرگون کردن دنیای فناوری نقش بسزایی ایفا خواهد کرد. به‌طور طبیعی پلیس در آینده باید از تجهیزات هوشمند متصل به دنیای اینترنت اشیا استفاده کند، اهم چالش‌های اینترنت اشیا با توجه به گزارش مؤسسات آینده پژوهی یادشده به‌شرح زیر است:

- هکرها تا سال ۲۰۲۱، از روش‌های جدیدی برای حملات علیه پروتکل‌ها و دستگاه‌های اینترنت اشیا استفاده خواهند کرد. به موازات افزایش حجم داده‌ها تا سال ۲۰۲۱، اینترنت اشیا باعث فاصله گرفتن از روش‌های تجزیه و تحلیل سنتی خواهد شد. پردازنده‌ها و معماری استفاده شده در دستگاه‌های اینترنت اشیا بیانگر بسیاری از قابلیت‌های آنها است. سکوهای[5] اینترنت اشیا تعداد زیادی از اجزاء زیرساختی یک سیستم اینترنت اشیا را درون یک محصول بسته‌بندی می‌کنند. سرویس‌های ارایه

1. Internet of things
2. Tag
3. Radio frequency identification (RFID)
4. Sensor
5. Platform

شده توسط این چنین زیرساخت‌هایی را می‌توان به سه گروه عمده تقسیم کرد:

الف - کنترل سطح پایین دستگاه‌ها برای انجام عملیاتی نظیر ارتباطات، پایش دستگاه‌ها و مدیریت امنیت؛

ب – جمع‌آوری، تبدیل و مدیریت داده‌های اینترنت اشیا؛

ج – پیاده‌سازی برنامه‌های اینترنت اشیا شامل منطق مبتنی بر رویداد، برنامه‌نویسی، بصری‌سازی، تجزیه و تحلیل و وفق دهنده‌هایی[1] برای اتصال به سیستم‌های سازمان (سخایی، ۱۳۹۴).

در حوزه ارتباطات و مخابرات، بسیاری از موضوعات اینترنت اشیا می‌تواند باعث شود تا پلیس در این حوزه که دنیای مجازی را به دنیای واقعی تبدیل و جرایم و وقایع اجتماعی را در آن رقم خواهد زد، وارد سازد. با گسترش روزافزون فناوری اطلاعات، به‌منظور برقراری نظم و امنیت و پیشی گرفتن از مجرمان، پلیس باید از فناوری روز دنیا استفاده کند. پلیس باید فرایندهای مأموریتی اعم از پایش، پیشگیری و کشف جرایم را مبتنی بر تجهیزات و ادوات فناورمحور جدید انجام دهد. با طرح اینترنت اشیا در مأموریت‌های پلیس، این فناوری می‌تواند در راستای بهبود کیفیت مأموریت‌های پلیس نقش مؤثری را ایفا کند. به‌طور مثال ادوات و تجهیزاتی همچون سلاح کلت کمری که در حوزه اینترنت اشیا امکان ارایه گزارش لحظه‌ای از زمان و مکان شلیک و یا حالات روحی مأموران در حین بکارگیری و استفاده از سلاح را گزارش می‌کند، باعث می‌شود تا مأموران پلیس در مأموریت‌های خود، دقت و مسئولیت‌پذیری بیشتری داشته باشند. اطلاع ناکافی بهره‌برداران و کارآگاهان پلیس در حوزه کشف جرائم، از فناوری جدید در حوزه اینترنت اشیا و آشنایی ناکافی با توجیه اقتصادی و امنیتی بکارگیری آن، موجب شده است که در استفاده از تجهیزات و اشیا اینترنتی جدید تردید و در بعضی مواقع واکنش منفی وجود داشته باشد. باوجود این موضوع، مهاجرت اشیا به سمت تجهیزات متصل به شبکه جهانی اینترنت روز به روز کاربرد بیشتری پیدا کرده و روند رشد آن چشمگیر بوده است. حال این پرسش پیش می‌آید که چرا باید تجهیزات و ادوات جدید اینترنتی در مأموریت‌های حساس پلیس بکارگیری شود؟

امروزه دو مقوله اطلاعاتی زمان و مکان افراد و اشیا از ارزش بسیار زیادی برای انسان‌ها برخوردار است. داشتن اطلاعات مکانی اشیا و افراد و یا زمان رویدادهایی که پیرامون او در حال اتفاق است، اشرافیت نسبت به شرایط پیرامونی را بیشتر خواهد کرد. اشرافیت پیرامونی از الزامات پلیس موفق است. از طرفی

1. Adapter

دسترسی‌های راه دور و حسگرهای متصل به اشیایی که فاصله‌های زیادی دارند، به پلیس درخصوص بسیاری از ناتوانی‌هایی که در گذشته به‌واسطه فاصله با اشیا داشته است، توانایی‌های ویژه‌ای داده است. در این میان شاید بتوان اینترنت را به‌عنوان یک حس جدید اضافه بر حواس پنج‌گانه انسان فرض کرد؛ بنابراین دور از انتظار نیست که پلیس به‌عنوان عامل هوشیار در حوزه برقراری نظم و امنیت از این حس جدید، جلوتر از سایر افراد استفاده کند. استفاده از تجهیزات جدید اینترنتی و اشیا و ادوات نظامی متصل به شبکه اینترنت که علاوه بر کنترل محلی، امکان دسترسی، گزارش و کنترل از فواصل دور را نیز دارد، از ضروریات کنونی پلیس است. بنابراین لازم است تجهیزات جدید با دیدگاه اینترنت اشیا خریداری و در اختیار پلیس قرار داده شود تا در آینده‌ای نزدیک از فضای جدید اینترنت اشیا جهانی و تجاری نیز بی‌بهره نماند. البته در این راه نقاط ضعف و حفره‌های امنیتی وجود خواهد داشت که باید شناسایی شود تا فرصت بکارگیری تجهیزات پلیسی جدید دارای ارزش افزوده بیشتری نسبت به چالش‌ها و حفره‌های امنیتی احتمالی پیش رو داشته باشد. با توجه به بانک‌های اطلاعاتی وسیع در حوزه پلیس که حاوی اطلاعات شخصی افراد، خودروها و وسایل نقلیه، منازل و اماکن و بسیاری از پرونده‌های موجود است، اینترنت اشیا، ضمن بالا بردن حجم اطلاعات، تجزیه و تحلیل این داده‌ها را امری اجتناب‌ناپذیر می‌کند. بنابراین پژوهش حاضر به‌دنبال پاسخ دادن به این پرسش است که «برای بکارگیری اینترنت اشیا در مأموریت‌های پلیس چه ملاحظاتی را باید درنظر گرفت و بهترین راهبرد کدام است؟»

پیشینه: طباطبایی، منطقی، حنفی‌زاده، نقی‌زاده و نیرومند (۱۳۹۱) پژوهشی با عنوان «الگوی بهبود توانمندی فناورانه در بنگاه‌های دانش‌بنیان تأمین‌کننده تجهیزات الکترونیک پلیس بر پایه الگوی توانمندی پویا»، را انجام داده‌اند. نتایج این پژوهش نشان می‌دهد، بنگاه‌هایی با توانمندی پویای بالاتر که داری توانایی درک محیطی، توانایی و انعطاف‌پذیری بالاتری باشند، از سطح توانمندی فناوری بالاتری نیز برخوردار هستند. دستیابی به سطوح بالای توانمندی فناوری - که در برگیرنده مجموعه‌ای جامع از توانایی‌ها است - نیازمند چیزی بیش از توانایی معمول فنی، مهندسی و تحقیقاتی است و به‌ویژه درشرکت‌های فعال در بخش‌های با فناوری برتر همچون تجهیزات الکترونیکی پلیس، نیازمند توانمندی پویایی است که به‌طور مستمر و پیوسته خود را اصلاح و بازآرایی کرده و شایستگی‌های محوری سازمان را اصلاح و بازتولید کند. شفیعی (۱۳۹۴)، در پژوهشی چالش‌های فراروی توسعه فناوری اینترنت اشیا

را بررسی کرده است. وی در پژوهش خود به بررسی تهدیدات امنیتی و ایجاد شکاف دیجیتالی ناشی از استفاده از اینترنت اشیا پرداخته است. وی معتقد است پیچیدگی جهان مبتنی بر اینترنت اشیا و پیامدهای امنیتی آن ممکن است بسیاری از افراد یا کشورها را به استفاده نکردن از دستاوردهای این پدیده ترغیب کند. کاربرد فناوری‌های یادشده به نفع بسیاری از کشورهای در حال توسعه است، اما ممکن است این کشورها به دلایل دیگری از جمله هزینه‌های سنگین قادر به استفاده از آن نباشند و تمام این موضوعات باعث تعمیق شکاف دیجیتال می‌شود. از طرفی دغدغه‌های امنیتی پیش روی این فناوری باید به دقت مورد بررسی قرار گیرند و سیاست‌های مناسب برای مقابله با این تهدیدات و ترغیب افراد، دولت‌ها و کشورها برای تمایل به استفاده از این فناوری، بکارگیری شوند. تردیدی وجود ندارد که اینترنت اشیا در کنار مزایایش، مشکلاتی هم دارد و صاحب‌نظران و سیاست گذاران باید از هم اکنون در اندیشه مقابله با چالش‌های آن باشند. امیری (۱۳۸۸) در پژوهشی با عنوان «مطالعه فرصت‌ها و تهدیدات ناشی از ظهور فناوری‌های نوین اطلاعاتی: گامی به سوی تدوین راهبرد در ناجا»، به این نتایج رسیده است که با ظهور فناوری‌های نوین اطلاعاتی، فرصت‌ها و تهدیدهای جدیدی در محیط راهبردی ناجا به‌وجود می‌آید که لزوم استفاده از راهبردهای نوین را مطرح می‌کند و به‌ترتیب راهبردهای ترکیبی، پیشگیرانه، همکاری‌های بین‌المللی، جرم‌انگاری و مداخله گرایانه، مناسب‌ترین راهبردها هستند. اسفار، ناتالیزیو، چلال و چوتورو[1] (۲۰۱۸) در پژوهش خود یک نقشه راه برای بررسی چالش‌هایی نظیر حریم خصوصی، اعتماد، شناسایی اشیا و کنترل دسترسی و بررسی تاثیر و جایگاه هر مولفه در بحث امنیت کل سیستم را ارائه کردند. کانتی، دهقان تنها، فرانک و واتسون[2] (۲۰۱۸) در پژوهش خود به بررسی سرعت رشد و توسعه اینترنت اشیا و کاربردهای آن و اشاره به چالش‌های امنیتی و فارنزیک پرداختند. لوترا، گارگ، منگل و بروال[3] (۲۰۱۸) در پژوهش خود به بررسی و رتبه‌بندی چالش‌های اینترنت اشیا با استفاده از تکنیک تحلیل سلسله مراتبی و تحلیل رابطه خاکستری پرداختند. همانطور که مشخص است، در بیشتر پژوهش‌ها، چالش‌های مطرح به‌صورت جامع در نظر گرفته نشده و تمرکز اصلی کارهای پیشین بر روی چالش‌های محیط خارج سازمان است، در صورتی که پیاده‌سازی اینترنت اشیا چالش‌های درون سازمانی نیز به همراه

1. Sfar, Natalizio, Challal & Chtourou
2. Conti, Dehghantanha, Franke & Watson
3. Luthra, Garg, Mangla & Berwal

دارد که اگر به آن توجه نشود، هزینه زیادی برای جبران آن صرف خواهد شد.

مبانی نظری: اینترنت اشیا به‌طور اساسی هر وسیله‌ای را با کلید روشن و خاموش به اینترنت و یا به یکدیگر متصل می کند و می تواند شامل تلفن‌های همراه، ماشین لباسشویی، هدفون، لامپ، دستگاه‌های پوشیدنی، وسایل حمل‌ونقل، تجهیزات سازمانی و مانند آنها باشد. گارتنر[1] معتقد است تا سال ۲۰۲۰ بیش از ۲۶ میلیارد دستگاه به دنیای اینترنت اشیا متصل خواهد شد. برخی حتی ارزش این تعداد اشیا را بیش از ۱۰۰ میلیارد دلار تخمین زده‌اند. اینترنت اشیا یک شبکه غول پیکر از اشیا متصل است که شامل افراد نیز می‌شود. اینترنت اشیا رابطه بین مردم – مردم، مردم – اشیا و اشیا با اشیا خواهد بود (مورگان[2]، ۲۰۱۴، ص ۶۶). شرکت اسکا تلکام کره جنوبی اخیراً فناوری «آی. اُ. اس. تی»[3] را برای مدل تجارت خود معرفی کرده است. این شرکت از فناوری یادشده، که به‌طور مدام داده‌ها را از طریق پلت فرم بی‌سیم لورا تولید می کند، استفاده کرد. نرخ داده‌های تولید شده توسط فناوری یادشده در حال افزایش است (گوهر، احمد، خان،گویزانی، احمد و راهمن[4]، ۲۰۱۸، ص ۱۳۰). اینترنت اشیا صنعتی است که ایجاد آن، گسترش شبکه‌های حسگر، پروتکل‌ها و برنامه‌های کاربردی را به‌دنبال خواهد داشت که در آن شاخص فرکانس رادیویی یکی از ارکان اصلی خواهد بود. تاریخچه اینترنت اشیا، به اشیای برچسب گذاری شده‌ای اشاره دارد که شاخص فرکانس رادیویی آن را شناسایی کرده و در ارتباطات اینترنت استفاده شده است (خدمتگزار[5]، ۲۰۱۵، ص ۵۶۰). اینترنت اشیا در حوزه‌های امنیت و سلامت عمومی و حوزه‌های نظامی و دفاعی، ایده‌های کلیدی بسیاری را به ارمغان آورده که در آن‌ها چابکی و امنیت لجستیک نظامی تا حد زیادی بهبود یافته است. با توسعه فناوری اینترنت اشیا، کاربردهای نظامی آن تنها به حوزه لجستیک محدود نشده و اینترنت اشیا ارزش ویژه‌ای برای شناسایی نظامی، نظارت و کنترل محیطی و پیرامونی، جنگ‌افزارهای بدون سرنشین و مانند آن به ارمغان می آورد (وبسکال[6]، ۲۰۰۸، ص ۱۹). در حقیقت اینترنت اشیا فرصت‌های بالقوه عظیمی در بسیاری از دامنه‌های کاربردی شامل توزیع توان الکتریکی، حمل‌ونقل هوشمند، کنترل صنعتی، کشاورزی صنعتی، پایش محیطی و پیرامونی، خرده‌فروشی کالا و مانند آن ارائه می‌دهد (آت

1. Gartner
2. Morgan
3. Internet of services token (IOST)
4. Gohar, Ahmed, Khan, Guizani, Ahmed & Rahman
5. Gohar, Ahmed, Khan, Guizani, Ahmed & Rahman
6. Khedmatgozar
7. Wobschall

زوری، لرا و مرابیتو[1]، ۲۰۱۰، ص ۲۸۰۱). اینترنت اشیا می‌تواند انقلاب اطلاعاتی - نظامی جدیدی را در امور نظامی نوین ایجاد کرده و به روند پیشرفت آن شتاب دهد. اینترنت اشیا آن‌طوری که اینترنت عمومی امروزه کامل است، مطلوب نیست و مسائل و مشکلات بسیاری در مورد کاربردهای آن باقیمانده است که باید حل شود (دنیس و دومینیک[2]، ۲۰۱۰، ص ۱۷؛ وبسکال، ۲۰۰۸، ص ۲۰).

اینترنت اشیا در حوزه نظامی در حال گسترش روزافزون است، اما تاحدودی همه پژوهش‌های حاضر در مثال‌ها و ایده‌های ساده نظامی باقیمانده است. پژوهش‌های اصولی در حوزه کاربردی اینترنت اشیا باید برای کاربردهای نظامی صورت گیرد. با ایجاد اینترنت اشیا زنجیره تکاملی از اتصال اشیا با یکدیگر به‌وجود خواهد آمد. این زنجیره تکامل با یکپارچه‌سازی حوزه‌های عمودی مانند امنیت، انرژی، زباله‌ها، مدیریت شهری، پلیس، حمل‌ونقل عمومی، حوزه‌های نظامی، پاسگاه‌های مرزی، پزشکی و مانند آن به‌وجود خواهد آمد (شاه و یعقوب[3]، ۲۰۱۶، ص ۱۱). در اینترنت اشیا از شاخص‌های فرکانسی برای کاربرد در ارتباطات نزدیک، و متحرک دستگاه‌ها استفاده خواهد شد، که می‌تواند برای پیاده‌سازی ایده نوین اینترنت اشیا استفاده شود (شاه و یعقوب، ۲۰۱۶، ص ۱۳).

اینترنت اشیا در حوزه پزشکی نظامی، نجات افراد و درمان پزشکی سربازان، دستگاه‌های مراقبت پزشکی هوشمند و دستگاه‌های پایش سلامت، با تجهیزات بی‌سیم و با قابلیت برقراری ارتباط میان دستگاه‌ها و دستگاه‌های پزشکی مستقر تجهیز می‌شوند. این تجهیزات و دستگاه‌های پوشیدنی کاربردی، آسیب‌پذیری‌های امنیتی خاصی دارند (هالپرین، هیت بنجامین، رنسفورد، دیفند، مورگان و مایسل[4]، ۲۰۰۸، ص ۲۵ و مایسل[5]، ۲۰۱۰، ص ۱۱۶۵). در بررسی کاربرد اینترنت اشیا در حوزه نظامی چندین حالت استفاده با تأثیر بالا به‌منظور پیاده‌سازی در محیط‌های نظامی وجود دارد. برخی از این کاربردها عبارت‌اند از: ۱- تجهیزات هوشمند، ۲- آگاهی موقعیتی، ۳- لجستیک و ۴- مراقبت پزشکی نظامی. مباحث کاربردی جدی‌تر اینترنت اشیا در عملیات نظامی در مراجع خاصی قابل مطالعه است (هالپرین و همکاران، ۲۰۰۸، ص ۲۷). اینترنت اشیا برای تجهیزات گوناگون و گسترده نظامی همانند وسایل

1. Atzori, Iera & Morabito
2. Dennis & Dominik
3. Shah & Yaqoob
4. Halperin, Heydt-Benjamin, Ransford, Clark, Defend, Morgan & Maisel
5. Maisel

نقلیه، سیستم‌های پشتیبانی و حتی سلاح‌های مختلف قابل استفاده است. بسیاری از اشیا فعال در شبکه، رخنه‌های معنی‌دار و آسیب‌پذیری دارند. به‌ویژه، چندین آسیب جدی در وسایل نقلیه شناسایی شده است که منجر به فراخوانی‌های گسترده این خودروها شده است (ایشتیاق روفا، مصطفی، تراویس تیلور، زوا، گروتسرب، تراپب و سسکارب[1]، ۲۰۱۰، ص ۱۷). یکی از مهم‌ترین رویکردهای هر عملیات نظامی، آگاهی درست و مناسب از موقعیت است که باعنوان آگاهی موقعیتی از آن یاد می‌شود. در حال حاضر بیشتر نیروهای نظامی از یک محدوده گسترده و بزرگ از حسگرها و وسایل نقلیه بدون سرنشین به‌منظور جمع‌آوری اطلاعات استفاده می‌کنند. ترکیب راه‌حل‌های اینترنت اشیا شهری (غیرنظامی) در دستگاه‌های فناوری اطلاعاتِ نظامی می‌تواند تصویر عملیاتی موجود را برای یک فرمانده بهبود بخشد و آگاهی‌های موقعیتی او را تقویت کند. استفاده از اینترنت اشیا شامل حسگرها و شاخص فرکانسی، پایه‌ای‌ترین الزام برای بهبود کارآیی و اثربخشی عملیات لجستیکی به‌شمار می‌رود که شامل قابلیت همکاری با سایر دستگاه‌های لجستیک است، زیرا تجهیزات پشتیبانی موردنیاز در خلال عملیات نظامی تنها شامل تجهیزات نظامی نمی‌شود، بلکه مواد غذایی، پزشکی و پشتیبانی برای نیروها را نیز دربر می‌گیرد. استفاده از دستگاه‌های فناوری اینترنت اشیا در لجستیک همچنین می‌تواند به ایمنی بیشتر عملیات لجستیکی منجر شود. برای مثال به‌وسیله جلوگیری از حمل‌ونقل مشترک برخی کالاها و محصولات همچون اجزای شیمیایی که می‌تواند منجر به واکنش‌های شیمیایی خطرناک شوند، یا بخش‌های تجهیزات رمزنگاشتی که نباید به‌هیچ‌وجه توسط یک دشمن شنود شوند (سورنیوتی، گومز، رونا و اودوریکو[2]، ۲۰۰۷، ص ۱۹۲).

کاربرد اینترنت اشیا در حوزه‌های نظامی جزء جدانشدنی و اضطراری توسعه اطلاعاتی نظامی است. اینترنت اشیا توسعه حوزه نظامی و پلیس را به‌طور عمده‌ای پیش خواهد برد و به‌نظر می‌رسد که به‌زودی دنیا شاهد شبکه‌های اینترنت اشیا نظامی که در آن نقش انسان کمرنگ‌تر است خواهد بود. با توجه به دامنه کاربردهای اینترنت اشیا نظامی و اهمیت خروجی آن‌ها، شاید بتوان گفت که بحث امنیت، اصلی‌ترین چالش اینترنت اشیا نظامی محسوب می‌شود. وجود یک آسیب‌پذیری در هریک از بخش‌ها و اجزای اینترنت اشیا نظامی می‌تواند به بروز خسارت‌های جبران‌ناپذیری منجر شود (براری و همکاران، ۱۳۹۵، ص ۴۵).

1. Ishtiaq Roufa, Mustafaa, Travis Taylora, Xua, Gruteserb, Trappeb & Seskarb,
2. Sorniotti, Gomez, Wrona & Odorico

امنیت اینترنت اشیا: اگر دسترسی موردنیاز به اطلاعات ارسالی از حسگرها و دستگاه‌ها وجود نداشته باشد، استفاده از ظرفیت کامل اینترنت اشیا در محیط‌های نظامی قابل دستیابی نخواهد بود. به‌طور مشابه، اطلاعات فرمان و کنترل باید در مواقع لزوم برای عملگرها و دستگاه‌های هوشمند قابل دسترسی باشد. یک مفهوم مشخص از دسترسی مرتبط با اینترنت اشیا به حمله خواب – محرومیت معروف است. این نوع حمله به‌طور مشخص دستگاه‌های دارای باطری را هدف قرار می‌دهد که در میان دستگاه‌ها و اشیای هوشمند متداول است. این حمله از ورود این دستگاه‌ها به حالت صرفه‌جویی در مصرف انرژی جلوگیری می‌کنند. این عمل به تخلیه باطری دستگاه منجر می‌شود. این در حالی است که شارژ مجدد باطری دستگاه ممکن است در شرایط نبرد و حمله بسیار سخت و حتی ناشدنی باشد. بنابراین فناوری توان – صفر و صرفه‌جویی در مصرف انرژی ممکن است برای بقای حیات دستگاه‌های اینترنت اشیا مهم باشد. این موضوعات بخش عظیمی از برنامه‌های پژوهشی اخیر در اینترنت اشیا برای حوزه‌های امنیتی و نظامی را دربر می‌گیرد (هالپرین و همکاران، ۲۰۰۸، ص ۲۳). در اینترنت اشیا مقیاس گسترده‌ای از داده‌ها، مربوط به شاخص‌های فرکانسی خواهد بود. اشتراک‌گذاری اطلاعات متقابل سازمانی، مشکلات امنیت داده‌ها را به‌وجود خواهد آورد. توزیع کلیدهای مدیریت برای برچسب‌ها به‌عنوان یکی از این مشکلات بالقوه است. چالش‌های دیگری که در بحث تگ شاخص‌های فرکانسی به‌وجود آمده است، ایجاد تغییرات در نام‌گذاری دامنه‌ها است که می‌تواند کاربران را درگیر کند (جولس[1]، ۲۰۰۶، ص ۳۹۰). در بحث امنیت اینترنت اشیا، حضور تگ‌های مسدودکننده شاخص فرکانسی دستگاه‌های الکترونیکی است، که به لحاظ نظری باید انتقال همه یا اطلاعات موجود در برچسب‌های شاخص فرکانسی را مختل کند. برچسبِ مسدودکننده ممکن است در یک کیسه خرید، کیف پول یا هر شیء دیگری دیده شود که حملات آن در تبلت‌ها قرار می‌گیرد، تا اطلاعاتی را که مصرف‌کنندگان می‌خواهند، مسدود کنند (کلیرینگ هوس[2]، ۲۰۰۳، ص ۵۶). درخصوص میزان آسیب‌پذیری و تهدیداتی که در حوزه مهاجرت اشیا چه در بخش‌های تجاری و چه در حوزه پلیس و سازمان‌های امنیتی وجود دارد، پیشرفت‌های اخیر نشان داده است که در آینده باید انتظار حملات گسترده‌تری را از طریق بات نت‌های[3] اینترنت اشیا داشت. جان هایمرل[4]، مدیر گروه هوشمندی

1. Juels
2. Clearinghouse
3. Botnet
4. John Heimerl

مقابله با تهدیدات در شرکت ان تی تی سکوریتی عنوان کرد: دستگاه‌های بسیار زیادی وجود دارند که از سرویس‌ها و گذرواژه‌های ناامن بهره می‌برند. امن‌سازی این دستگاه‌ها در وضعیت فعلی‌شان درعمل امکان‌پذیر نیست. بسیاری از این دستگاه‌ها قابلیت رفع عیب ندارند، زیرا گذرواژه‌هایشان غیرقابل تغییر است و پیکربندی ثابتی دارند. حتی اگر سازندگان تکامل یابند و دستگاه‌های امن‌تری بسازند، هزینه‌هایشان بیشتر می‌شود و ممکن است بازار از افزایش قیمت و پیچیدگی این دستگاه‌ها استقبال نکند. درنتیجه، همچنان که سازندگان برای ساخت دستگاه‌های جدید تلاش می‌کنند، دستگاه‌های موجود به شکلی ناامن به شبکه متصل می‌مانند. در خبرنامه افتا گفته شده، اگرچه ممکن است دستگاه‌های آینده بهبود یابد و از برخی از دستگاه‌های فعلی به شکلی هوشمندانه‌تر استفاده شود، اما بیشتر دستگاه‌های اینترنت اشیا همچنان تا سال‌ها آسیب‌پذیر خواهند بود (بی‌نام، ۱۳۹۶، ص ۲۶).

همانطور که در بخش مقدمه اشاره شد، پیاده‌سازی اینترنت اشیا دارای چالش‌های متعددی بوده که در هر کدام از پژوهش‌های پیشین به جنبه‌های خاصی از این چالش‌ها توجه شده است. با توجه به مرور کارهای پیشین، برخی از دسته‌بندی‌های کلی از چالش‌های مطرح در پیاده‌سازی اینترنت اشیا را می‌توان به شرح زیر بیان کرد:

امنیت و حریم خصوصی، این چالش در قالب مفاهیمی مانند احراز هویت، کنترل دسترسی، حریم خصوصی، معماری و ساختار امن تقسیم بندی می‌شود (کانتی و همکاران، ۲۰۱۸، ص ۵۴۵).

قوانین، با ورود اینترنت اشیا به بازار و صنعت، چالش‌هایی در زمینه تنظیم مقررات و قوانین مناسب باعنوان استانداردها برای رسیدن به هماهنگی به‌عنوان یک چالش مطرح شده است. با توجه به این مسئله که هر روز مؤلفه جدیدی به بستر اینترنت اشیا اضافه می‌شود، تقسیم‌بندی و تعریف استانداردها برای سازمان‌ها و استفاده از مزایا و امکانات اینترنت اشیا دشوار خواهد بود (چن، اکسو، لیو هو و ونگ[1]، ۲۰۱۴، ص ۳۵۱).

فنآوری، اینترنت اشیا شامل طیف گسترده‌ای از فناوری‌ها است، بنابراین، مشکلات و چالش‌های موجود در هر کدام از این فناوری‌ها می‌تواند در بدنه اینترنت اشیا نفوذ کند (محمدزاده، غفوری، محمدیان، محمدکاظمی، مهبانویی و قاسمی[2]، ۲۰۱۸، ص ۱۲۸).

1. Chen, Xu, Liu, Hu & Wang
2. Mohammadzadeh, Ghafoori, Mohammadian, Mohammadkazemi, Mahbanooei & Ghasemi

فرهنگ، در فرهنگ کشورها، اعتماد به اینترنت اشیا، تاثیر قابل توجهی در استفاده و برقراری ارتباط کاربران با آن دارد. اگر تلاش برای اعتمادسازی و فرهنگ‌سازی در اینترنت اشیا ناموفق باشد، رسیدن به توسعه سریع و پایدار مقدور نخواهد بود (ویتمور، آگاروال وایکسیو[1]، ۲۰۱۵، ص ۲۶۳).

مدل کسب و کار، وقتی سازمانی تصمیم به پیاده‌سازی اینترنت اشیا دارد، لازم است یکسری تغییرات را در مدل کسب و کار خود انجام دهد و مدل کسب و کار خود را به روزرسانی کند (میورندی، سیاری، پلگرینی و چامتک[2]، ۲۰۱۲، ص ۱۴۹۹).

فرایندهای مأموریتی پلیس آگاهی: در شرایط فعلی پلیس آگاهی کشور مجموعه‌ای از فرایندهای دستی را به‌صورت زیر انجام می‌دهد که عبارت‌اند از: فرایند بررسی صحنه سرقت، فرایند تعقیب و مراقبت، فرایند چهره‌نگاری و فرایند گشت‌زنی. این فرایندها مجموعه مأموریت‌های پلیس آگاهی را تشکیل می‌دهند که در حال حاضر به‌صورت عملی و به‌شرح جدول ۱ تحلیل شده است.

جدول ۱. فرایندهای مأموریتی پلیس آگاهی

فرایند	ورودی	تعداد فعالیت در فرایند
بررسی صحنه سرقت	اعلام پلیس ۱۱۰ یا مقامات قضایی	۱۱
تعقیب و مراقبت	ارجاع پرونده از واحد ارجاع و دستور مقام قضایی	۱۵
چهره‌نگاری	کلیه پرونده‌های ارجاع شده از طریق مقام قضایی، کلانتری‌ها، پاسگاه‌ها، پایگاه‌های پلیس آگاهی و مراکز تشخیص هویت و دستگاه‌ها اطلاعاتی و امنیتی کشور	۱۰
گشت زنی	ارجاع پرونده از واحد ارجاع و دستور مقام قضایی	۱۶

راهبردهای بکارگیری ابزارها و اشیا هوشمند اینترنتی که بسیاری از بخش‌های این فرایندها را به سرعت و دقت بالا و در فضای مجازی انجام نماید از اهداف این پژوهش است. در بررسی کل فرایندهای پلیس آگاهی درمجموع ۵۲ فعالیت احصاء شد که از این تعداد فعالیت، امکان خودکارسازی و هوشمندسازی بسیاری از این فعالیت‌ها ازطریق بکارگیری تجهیزات مرتبط با اینترنت اشیا وجود دارد و حدود ۳۸ فعالیت در مأموریت‌های مختلف می‌تواند بوسیله تجهیزات جدید و بروز در فضای اینترنت اشیا صورت پذیرد.

1. Whitmore, Agarwal & Da Xu
2. Miorandi, Sicari, De Pellegrini & Chlamtac

روش

رویکرد پژوهش ترکیبی (کیفی و کمی) و از نوع اکتشافی است و از نظر هدف کاربری است. در بخش کیفی نقاط قوت، ضعف، فرصت و تهدید (روش تحلیل اس دبلیو اُتی) بکارگیری اینترنت اشیا و ادوات و تجهیزات هوشمند در مأموریت‌های پلیس آگاهی استخراج شد. جامعه آماری در این بخش تمام‌شمار و شامل ۱۸ نفر از کارشناسان بود. در بخش کمی با استفاده از تحلیل عاملی نکویی برازش آنها گزارش شد. در این پژوهش با رویکرد کتابخانه‌ای و میدانی و استفاده از اطلاعات وضعیتی فرایندهای موجود در پلیس به منظور بررسی شرایط فعلی و همچنین با استفاده از روش اس دبلیو اُتی، نقاط قوت و ضعف، فرصت‌ها و تهدیدها در بکارگیری اینترنت اشیا در مأموریت‌های پلیس آگاهی، تحلیل شدند. در پایان این سنجش راهبرد مناسب برای مهاجرت به سمت تجهیزات و ادوات هوشمند مبتنی بر اینترنت اشیا در پلیس آگاهی مشخص شد. جامعه آماری پژوهش حاضر ۴۲۰ نفر برآورد شد که شامل تعداد نفرات بهره‌بردار از تجهیزات تخصصی حوزه مأموریت‌های پلیس آگاهی بود. روش نمونه‌گیری در بخش کمی پژوهش تصادفی ساده است. برای تعیین حجم نمونه نیز از رابطه کوکران با اطمینان ۹۵ و دقت آزمون ۰/۰۵ استفاده شد. به‌منظور بیشینه‌شدن حجم نمونه، مقدار p، ۰/۵ در نظر گرفته شد. بنابراین با توجه به حجم جامعه، اندازه نمونه ۲۰۰ نفر به‌دست آمد. در این پژوهش با توجه به چهار فرضیه متصور، نقاط قوت، ضعف، فرصت و تهدید بکارگیری اینترنت اشیا به‌عنوان متغیرهای مستقل و راهبرد برتر بکارگیری اینترنت اشیا و تجهیزات هوشمند جدید در پلیس آگاهی به‌عنوان متغیر وابسته در نظر گرفته شد. در تدوین ادبیات پژوهش، جمع آوری اطلاعات به‌صورت کتابخانه‌ای انجام شد و برای نظرسنجی از جامعه آماری در راستای سنجش متغیرهای پژوهش، به‌منظور بررسی تأثیر متغیرهای مستقل بر متغیر وابسته از پرسشنامه محقق‌ساخته استفاده شد. در این پژوهش پس از دریافت نظر صاحب‌نظران، نسبت به تهیه پرسشنامه اولیه شامل ۸۰ پرسش براساس اهداف پژوهش و رابطه مؤلفه‌ها و شاخص‌های هریک از متغیرها، از مقیاس طیف لیکرت[1] استفاده شد و پس از اعمال نظر خبرگان، به ۶۵ پرسش کاهش یافت. پس از آن به صورتی که در بخش بعدی نشان داده می‌شود، تحلیل عاملی تأییدی برای هریک از ابعاد چهارگانه اجرا شد و شاخص‌ها دوباره کاهش یافت. پایایی و اعتبار پرسشنامه پژوهش با محاسبه ضریب

1. LIKERT scale

آلفای کرونباخ[1]، سنجیده شد. پایایی اولیه براساس نمونه‌ای ۲۵ تایی، ۰/۸۲۱ به‌دست آمد که با توجه به مناسب بودن آن، پرسشنامه بین سایر اعضای نمونه نیز توزیع شد. جدول ۲ پایایی‌های جزئی محاسبه شده را نشان می‌دهد.

جدول ۲. پایایی پرسشنامه

شاخص	ضریب آلفای کرونباخ
فرصت	۰/۸۱۱
تهدید	۰/۷۷۵
قوت	۰/۸۰۵
ضعف	۰/۷۹۳

یافته‌ها

در این پژوهش برای پاسخ به پرسش اصلی و تعیین راهبرد مناسب از روش تحلیل «اس. دبلیو. اُ. تی» استفاده شد. برای بررسی نظر اعضای جامعه آماری درخصوص قوت‌ها، ضعف‌ها، فرصت‌ها و تهدیدها از تحلیل عاملی تأییدی در قالب چهار فرضیه فرعی استفاده شد. آزمون برازندگی در تحلیل تأییدی، شاخص جذر برآورد واریانس خطای تقریب[2] کمتر از ۰/۱ درصد شاخص و کمتر از سه است. اگر مقدار (T-Value) ضرایب معنی‌داری هر متغیر نیز بزرگ‌تر از ۱/۹۶ و کوچک‌تر از ۱/۹۶- باشد، مدل از برازش خوبی برخوردار است. از آنجا که در این بخش، خروجی نرم‌افزار (شکل‌های ۱ تا ۸) بدون تغییر آورده شد، قبل از مشاهده خروجی نرم‌افزار، برای شناسایی علائم اختصاری متغیرهای مکنون و مشاهده‌ای، جدول ۳ ارائه شد.

جدول ۳. راهنمای شناسایی علائم اختصاری متغیرهای مدل

شاخص	علامت اختصاری
قوت	STRENGH
ضعف	WEAKNESS
فرصت	OPPORTUNITY
تهدید	THREAT

ویژگی‌های جمعیت‌شناختی: یافته‌های توصیفی جامعه پژوهش در جدول ۴ نمایش داده شده است.

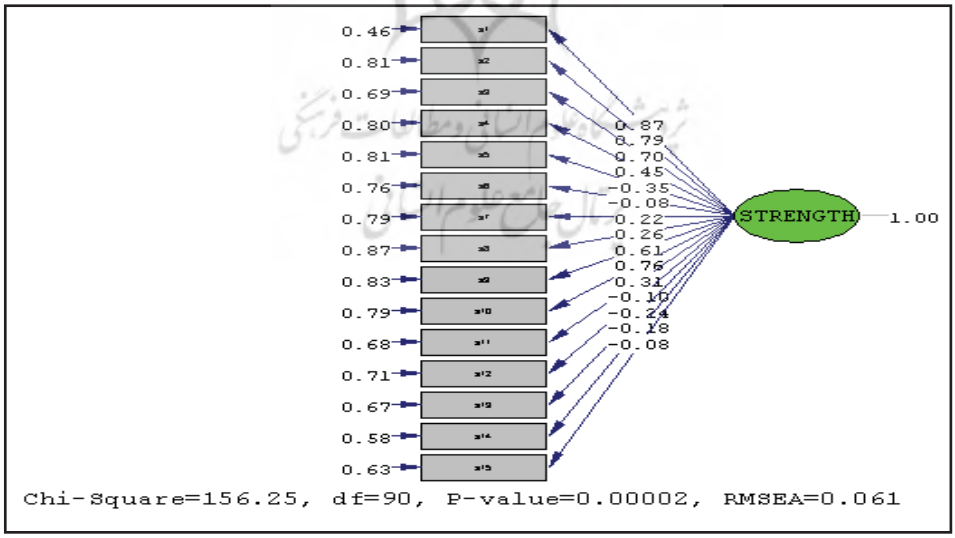
1. CRONBACH's alpha
2. RMSEA: Root mean square error of approximation

جدول ۴. ویژگی‌های جمعیت شناختی

بخش	سن					جنسیت		تحصیلات			سابقه خدمت (سال)				جمع
	۲۷ تا ۳۵	۳۶ تا ۴۴	۴۵ تا ۵۳	مرد	زن	دیپلم و کاردانی	کارشناسی	کارشناسی ارشد	دکترا	۱۱ تا ۲۰	۲۱ تا ۳۰	۳۰+		
کیفی	۴	۱۰	۴	۱۸	۰	۱	۲	۱۲	۳	۱۰	۶	۲		۱۸
کمی	۵۹	۱۱۰	۳۱	۱۹۷	۳	۲۹	۱۳۲	۳۸	۱	۷۹	۱۱۹	۲		۲۰۰

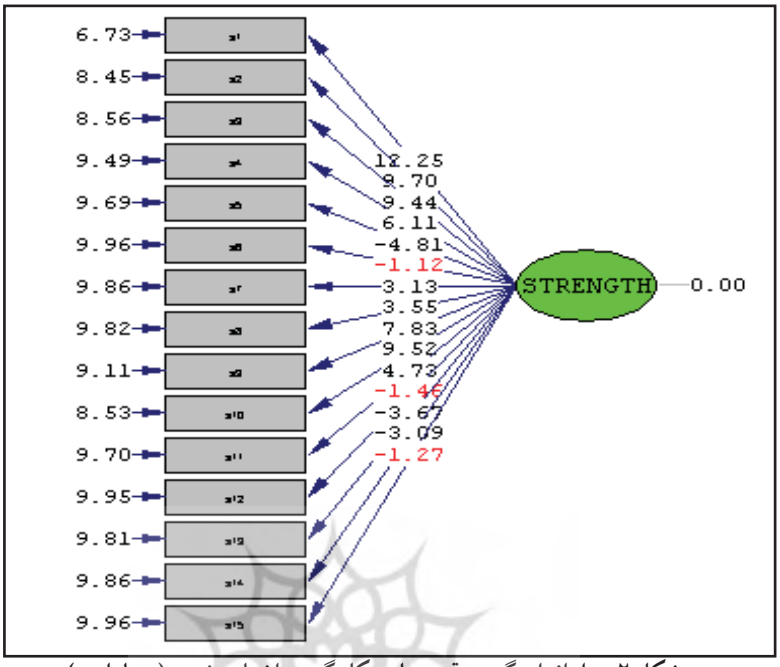
تجزیه و تحلیل داده‌های پرسشنامه: در پژوهش حاضر از تحلیل عاملی با بهره‌گیری از نرم‌افزار لیزرل[1] برای پاسخ به پرسش‌های پژوهش استفاده شد. به ترتیب تحلیل پرسشنامه در هر بخش از نقاط قوت و ضعف و تهدیدها و فرصت‌ها به‌صورت زیر ارائه می‌شود:

نقاط قوت بکارگیری اینترنت اشیا در مأموریت‌های پلیس آگاهی: برای تعیین نقاط قوت بکارگیری اینترنت اشیا در مأموریت‌های پلیس آگاهی، از تحلیل عاملی تأییدی استفاده شد. شکل‌های ۱ و ۲ مدل نقاط قوت را در حالت استاندارد و معناداری نشان می‌دهد.



شکل ۱. مدل اندازه‌گیری قوت‌های بکارگیری اشیا هوشمند در فرآیند ورودی (استاندارد)

1. LISREL



شکل ۲. مدل اندازه‌گیری قوت‌های بکارگیری اشیا هوشمند (معناداری)

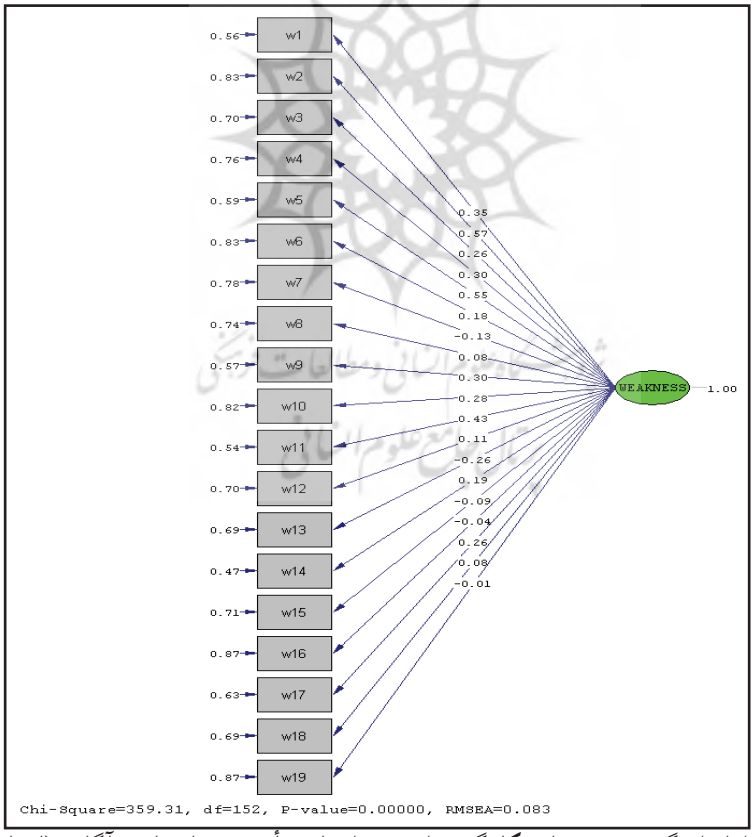
نقاط قوتی که مقدار قدر مطلق تی آن‌ها کوچکتر از ۱/۹۶ است معنادار نبوده و حذف شدند. بنابراین در پاسخ به پرسش فرعی نخست، با حذف شاخص‌های ششم، دوازدهم و پانزدهم، نقاط قوت براساس جدول ۵ مشخص شد.

جدول ۵. نقاط قوت پلیس آگاهی در بکارگیری اینترنت اشیا

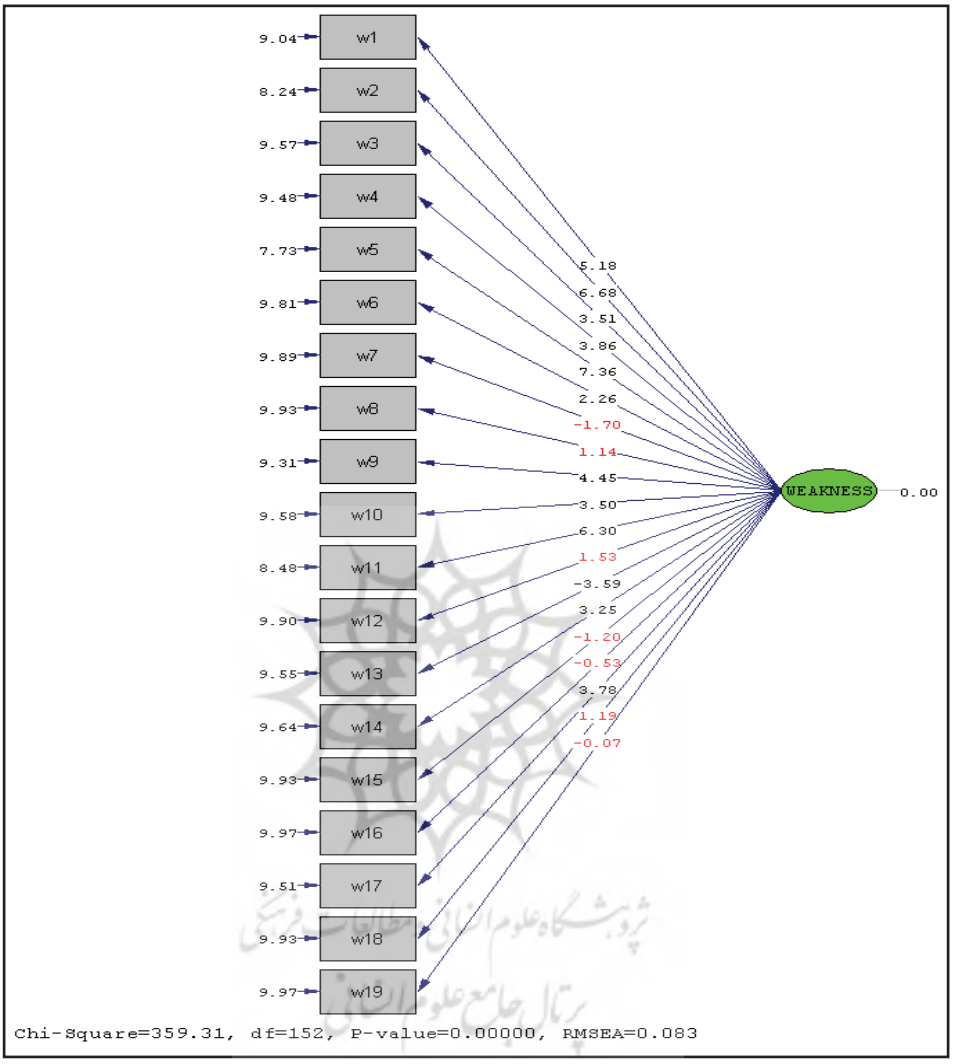
نماد	قوت‌ها
S1	در پلیس آگاهی بکارگیری سامانه نمایش موقعیت گشتی‌ها (مبتنی بر اینترنت اشیا) باعث اقتدار در پاسخگویی سریع به مأموریت‌ها خواهد شد.
S2	امکان بهره‌برداری از تجهیزات هوشمند (مبتنی بر اینترنت اشیا) باعث سرعت در پاسخگویی و واکنش سریع در مأموریت‌ها خواهد شد.
S3	توجه به بروز شدن تجهیزات (مبتنی بر اینترنت اشیا) در راستای بهبود مأموریت‌های محول
S4	بکارگیری اسلحه و سلاح‌های هوشمند جدید(مبتنی بر اینترنت اشیا) به‌منظور ثبت وقایع و مأموریت‌ها
S5	آموزش مستمر کارکنان درخصوص فنّاوری‌های جدید (مبتنی بر اینترنت اشیا)
S6	علاقمند برای مهاجرت به سامانه‌های هوشمند (مبتنی بر اینترنت اشیا)
S7	تأکید در بکارگیری افسران و نفرات باهوش‌تر نسبت به سایر پلیس‌های تخصصی برای تفهیم سریع‌تر فنّاوری‌های جدید(مبتنی بر اینترنت اشیا)

S8	مأموریت‌های پلیس آگاهی فرایندمحور بوده و به سامانه‌ها و تجهیزات ارتباطی نسل جدید (مبتنی بر اینترنت اشیا) نزدیک‌تر است.
S9	بکارگیری سامانه‌های تعیین موقعیت و زمان (مبتنی بر اینترنت اشیا) به‌منظور کشف جرائم در پلیس آگاهی.
S10	در پلیس آگاهی به شکوفایی و گسترش فنّاوری جدید(مبتنی بر اینترنت اشیا) ارج گذاشته و اهمیت داده می‌شود
S11	توجه خاص به حرفه‌ای گرایی
S12	نگرش مثبت مسئولان به اینترنت اشیا و قدرتی که این فنّاوری در بالابردن سرعت پاسخگویی به مأموریت‌ها دارد
S13	برخورداری از امکان ایجاد فضای آزمودن تجهیزات جدید اینترنتی(مبتنی بر اینترنت اشیا)
S14	وجود آمادگی ذهنی به‌منظور تغییرات در تجهیزات پلیس آگاهی

نقاط ضعف بکارگیری اینترنت اشیا در مأموریت‌های پلیس آگاهی: برای تعیین نقاط ضعف بکارگیری اینترنت اشیا در مأموریت‌های پلیس آگاهی نیز از تحلیل عاملی تأییدی استفاده شد. شکل‌های ۳ و ۴ مدل نقاط ضعف را در حالت استاندارد و معناداری نشان می‌دهد.



شکل ۳. مدل اندازه‌گیری ضعف‌های بکارگیری اینترنت اشیا در مأموریت‌های پلیس آگاهی (استاندارد)



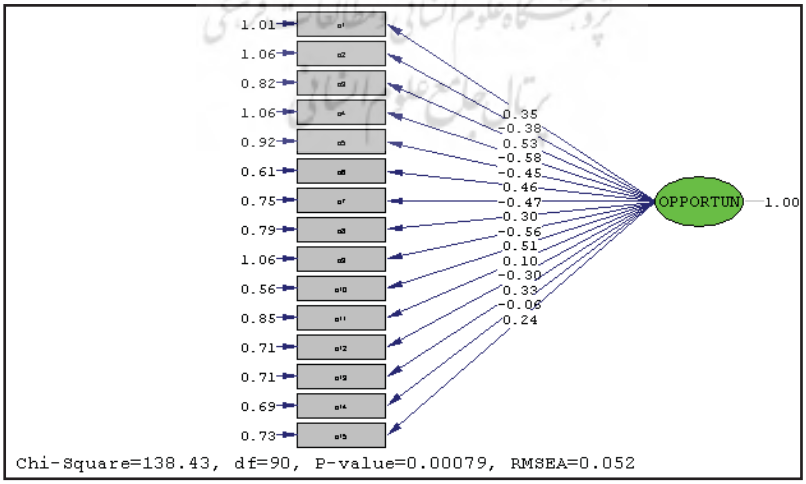
شکل ۴. مدل اندازه‌گیری ضعف‌های بکارگیری اینترنت اشیا در مأموریت‌های پلیس آگاهی (معناداری)

ضعف‌هایی که قدر مطلق تی کوچکتر از ۱/۹۶ داشتند، معنادار نبوده و حذف شدند. بنابراین در پاسخ به پرسش فرعی دوم، با حذف شاخص‌های هفتم، هشتم، دوازدهم، پانزدهم، شانزدهم و نوزدهم، نقاط ضعف براساس جدول ۶ مشخص شد.

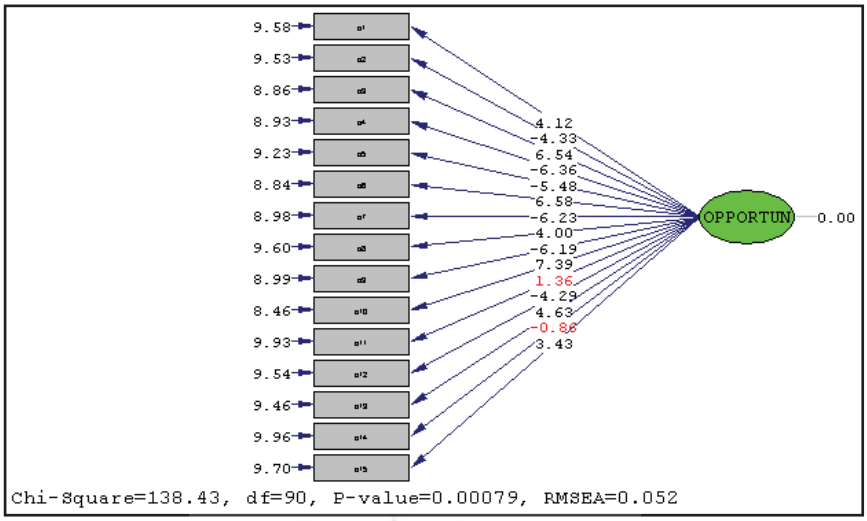
جدول ۶. نقاط ضعف پلیس آگاهی در بکارگیری اینترنت اشیا

نماد	ضعف‌ها
W1	توجه ناکافی به نوسازی و هوشمند کردن تجهیزات در پلیس آگاهی
W2	پلیس آگاهی فاقد اهداف مشخص در حوزه اینترنت اشیا است
W3	تناسب ناکافی بین تجهیزات جدید با مأموریت‌ها و نیازهای شغلی کارکنان پلیس آگاهی
W4	مشخص نشدن دقیق زمینه‌ها و نیازمندی‌های تجهیزات هوشمند در رده‌های مختلف پلیس آگاهی
W5	ضعف برنامه بروزرسانی تجهیزات موجود در سطح پلیس آگاهی
W6	پلیس آگاهی فاقد خط‌مشی‌های مناسب و هدف‌گذاری صحیح در امر مهاجرت تجهیزات خود به سمت اینترنت اشیا است
W9	راهبردهای تجهیزاتی مناسبی در پلیس آگاهی وجود ندارد
W10	آشنایی ناکافی مدیران دوایر پلیس آگاهی با مباحث برنامه‌ریزی راهبردی
W11	بین برخی از تجهیزات جدید فعلی با شرح وظایف کارکنان تناسبی وجود ندارد
W13	برخی از کارکنان پلیس آگاهی به دلیل کنترل موقعیت و زمان خود توسط سیستم، انگیزه لازم برای بکارگیری و استفاده صحیح از تجهیزات اینترنتی را ندارند
W14	تناسب ناکافی بین امکانات پلیس آگاهی با نیازهای مأموریتی
W17	ضعف استفاده کارکنان پلیس آگاهی در استفاده از سامانه‌های جدید

فرصت‌های بکارگیری اینترنت اشیا در پلیس آگاهی: برای تعیین فرصت‌های بکارگیری اینترنت اشیا در پلیس آگاهی نیز از تحلیل عاملی تأییدی استفاده شد. شکل‌های ۵ و ۶ مدل فرصت‌ها را در حالت استاندارد و معناداری نشان می‌دهد.



شکل ۵. مدل اندازه‌گیری فرصت‌های بکارگیری اینترنت اشیا در پلیس آگاهی (استاندارد)



شکل ۶. مدل اندازه‌گیری فرصت‌های بکارگیری اینترنت اشیا در پلیس آگاهی (معناداری)

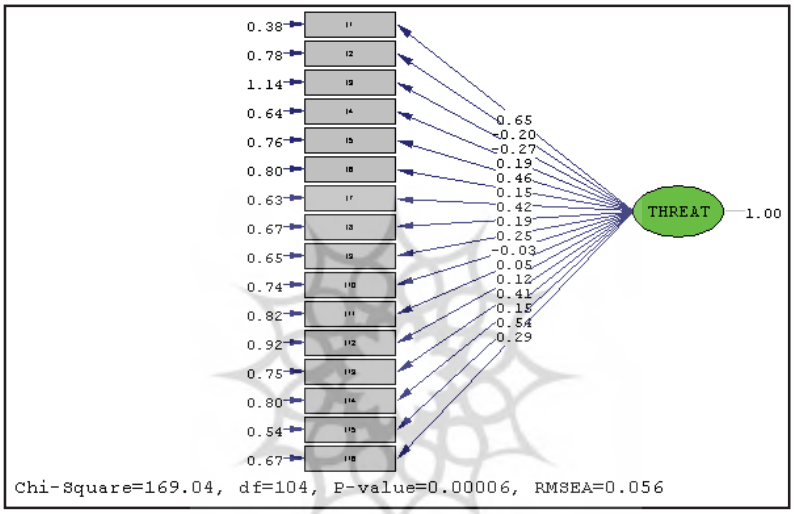
فرصت‌هایی که قدر مطلق تی کوچکتر از ۱/۹۶ داشتند، معنادار نبوده و حذف شدند. بنابراین در پاسخ به پرسش فرعی سوم، با حذف شاخص‌های هفتم، هشتم، دوازدهم، پانزدهم، شانزدهم و نوزدهم، فرصت‌های بکارگیری اینترنت اشیا در پلیس آگاهی براساس جدول ۷ مشخص شد.

جدول ۷. فرصت‌های بکارگیری اینترنت اشیا در پلیس آگاهی

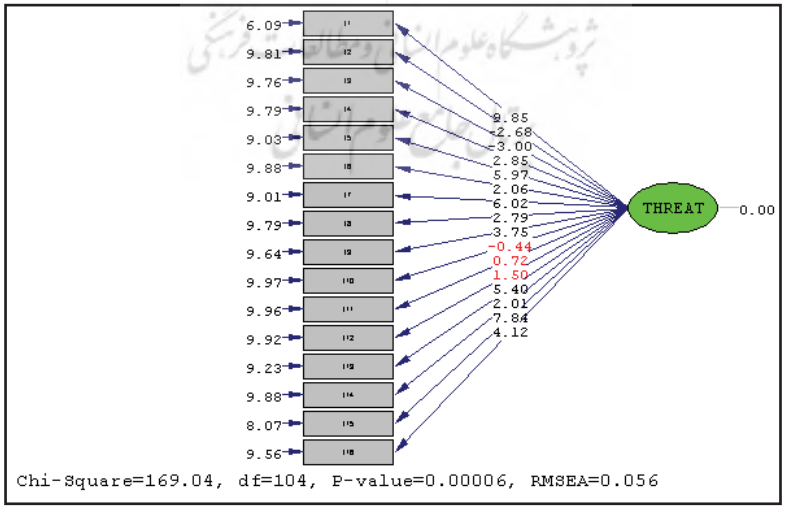
نماد	فرصت‌ها
O1	برخورداری از کمیته تصمیم‌گیری درخصوص بکارگیری تجهیزات هوشمند
O2	تغییر نگرش مدیران و فرماندهان از بکارگیری تجهیزات سنتی به تجهیزات هوشمند
O3	برخورداری از دانش فنی و تخصصی بالا در برخی از مدیران و فرماندهان
O4	پیشرفت سریع تجهیزات
O5	وجود امکان استفاده از ظرفیت‌ها و اطلاعات سایر سازمان‌های مشابه که به‌سمت هوشمندسازی حرکت کرده‌اند، در صورت اختصاص اعتبار
O6	طراحی برنامه مهاجرت پلیس به سمت اینترنت اشیا از سوی معاونت فناوری اطلاعات و ارتباطات نیروی انتظامی
O7	وجود حس هماهنگی در نحوه انجام فعالیت‌های فنی در حوزه بکارگیری تجهیزات هوشمند و اینترنت اشیا
O8	برگزاری مستمر کمیسیون اثربخشی هوشمندسازی پلیس و بکارگیری اینترنت اشیا در مأموریت‌های پلیس در شرکت صنایع مخابرات با حضور معاونت فناوری اطلاعات و ارتباطات و گروه بنیان و دیگر پلیس‌های تخصصی
O9	برخورداری از مدیران فعال برای یافتن پاسخ مشکلات تجهیزاتی
O10	لحاظ شدن آموزش تخصصی کارکنان در قانون استخدامی نیروی انتظامی برای آشنایی کارکنان جدید با ادوات و تجهیزات هوشمند جدید

O12	برخورداری از شرح فرایندهای مأموریتی در طرح مکنا
O13	برخورداری از حمایت فرمانده و مسئولان نیروی انتظامی
O15	حضور نیروهای جوان، بااستعداد، باهوش و با قدرت فراگیری بالا

تهدیدهای بکارگیری اینترنت اشیا در پلیس آگاهی: برای تعیین تهدیدهای بکارگیری اینترنت اشیا در پلیس آگاهی نیز از تحلیل عاملی تأییدی استفاده شد. شکل‌های ۷ و ۸ مدل تهدیدها را در حالت استاندارد و معناداری نشان می‌دهد.



شکل ۷. مدل اندازه‌گیری تهدیدهای بکارگیری اینترنت اشیا در پلیس آگاهی (استاندارد)



شکل ۸. مدل اندازه‌گیری تهدیدهای بکارگیری اینترنت اشیا در پلیس آگاهی (معناداری)

تهدیدهایی که قدر مطلق تی کوچکتر از ۱/۹۶ داشتند، معنادار نبوده و حذف شدند. بنابراین در پاسخ به پرسش فرعی چهارم، با حذف شاخص‌های دهم، یازدهم و دوازدهم، تهدیدهای بکارگیری اینترنت اشیا در پلیس آگاهی براساس جدول ۸ مشخص شد.

جدول ۸. تهدیدهای بکارگیری اینترنت اشیا در پلیس آگاهی

نماد	تهدیدها
t۱	نبود ممیزی مناسب برای انتخاب تجهیزات هوشمند
t۲	تنوع و پیچیدگی زیاد مأموریت‌ها و عملیات در فرایندها
t۳	تنوع زیاد ابزار و فناوری‌های نوین و پیشرفته و شگردهای مورد استفاده مجرمان
t۴	پیچیدگی دانش پلیسی
t۵	ترک خدمت برخی از مدیران متخصص و باتجربه
t۶	تأخیر در واگذاری اعتبارات لازم برای اجرای برنامه‌های تجهیز پلیس
t۷	توجه ناکافی به آموزش کارکنان در برنامه‌های جانشین‌پروری
t۸	ضعف نگرش برخی از مدیران به تجهیزات پیشرفته به‌عنوان یک سرمایه راهبردی
t۹	ضعف نگرش راهبردی نسبت به هوشمندسازی پلیس
t۱۳	وجود برخی از مدیران محتاط و گریزان از خطر
t۱۴	فقدان برنامه عملیاتی در بکارگیری تجهیزات هوشمند و اینترنت اشیا در فرایندها و مأموریت‌ها
t۱۵	اراده ناکافی مدیران برای تغییر تجهیزات سنتی فعلی متناسب با شرح وظایف و مأموریت‌ها
t۱۶	توجه بیش از حد مسئولان در امر فناوری و اینترنت اشیا به کمیت به‌جای کیفیت

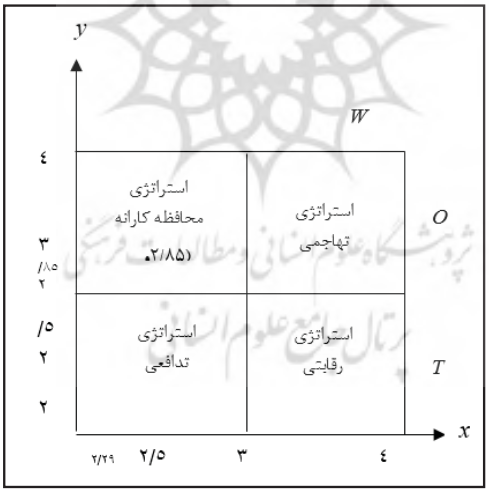
ماتریس تحلیل «اس. دبلیو. اُ. تی» بکارگیری اینترنت اشیا در پلیس آگاهی: پس از شناسایی نقاط ضعف و قوت محیط داخلی اینترنت اشیا در آگاهی و فرصت‌ها و تهدیدات محیط خارجی، امتیازات هریک از شاخص‌ها در قالب ماتریس‌های ارزیابی داخلی و خارجی محاسبه شد. از اعضای نمونه خواسته شد که به نقاط ضعف و تهدید رتبه‌های ۱ و ۲ و به نقاط قوت و فرصت رتبه‌های ۳ و ۴ داده شود. همچنین برای محاسبه ضریب اهمیت هر شاخص، از روش آنتروپی شانون[1] که یکی از روش‌های وزن‌دهی در تصمیم‌گیری چند شاخصه است استفاده شد.

پس از ترسیم ماتریس نقاط قوت و ضعف بکارگیری اینترنت اشیا در پلیس آگاهی امتیاز نهایی ماتریس ارزیابی داخلی ۲/۲۹ به‌دست آمد که با توجه به کمتر بودن آن از ۲/۵، می‌توان چنین تحلیل

1. Shannon's entropy

کرد که بکارگیری اینترنت اشیا در پلیس آگاهی با ضعف داخلی مواجه است. همچنین پس از ترسیم ماتریس نقاط فرصت و تهدید بکارگیری اینترنت اشیا در پلیس آگاهی، ارزیابی خارجی ۲/۸۵ به‌دست آمد که با توجه به بیشتر بودن آن از ۲/۵، می‌توان چنین تحلیل کرد که بکارگیری اینترنت اشیا با فرصت خارجی مواجه است.

در مرحله بعد پس از کدگذاری هر یک از عوامل مندرج در ماتریس‌های داخلی و خارجی با نگرش سیستمی به این عوامل براساس امتیاز نهایی، راهبردهای تعیین شده در خانه مربوطه، جایگاه آن در جدول چهار خانه‌ای، به‌لحاظ تعیین خط مشی کلی در بکارگیری راهبرد مناسب توسعه مشخص شد. در ماتریس داخلی و خارجی چهار خانه‌ای، جمع نمره‌های نهایی بر روی محور xها از ۱ تا ۲/۵ نشان دهنده ضعف داخلی و نمره ۲/۵ تا ۴ بیانگر میزان قوت است. به همین شیوه، جمع نمره‌های نهایی ماتریس ارزیابی خارجی از ۱ تا ۲/۵ بیانگر میزان تهدید و نمره ۲/۵ تا ۴ بیانگر میزان فرصت است. قرار گرفتن در هر یک از خانه‌های ماتریس داخلی و خارجی مفاهیم راهبردی خاصی دارد.



شکل ۹. ماتریس «اس. دبلیو. اُ. تی»

امتیاز نهایی ماتریس ارزیابی داخلی ۲/۲۹ و خارجی ۲/۸۵ بدست آمده است. با توجه به اینکه نقطه (۲/۸۵، ۲/۲۹) در خانه WO قرار دارد، بنابراین، راهبرد مناسب بکارگیری اینترنت اشیا در پلیس آگاهی باید یک راهبرد محافظه کارانه باشد.

بحث و نتیجه‌گیری

اینترنت اشیا، توسط تجهیزات سنجشی، میان اشیا و اینترنت ارتباط برقرار می‌کند به‌گونه‌ای که امکان شناسایی و مدیریت هوشمند را فراهم می‌سازد. تمام این تجهیزات برای کنترل و مدیریت از راه دور به اینترنت متصل هستند. یکی از اصلی‌ترین مواردی که همواره در مورد اینترنت اشیا مطرح می‌شود، بحث امنیت آن است. از آنجایی که در این فناوری، دستگاه‌های زیادی از طریق اینترنت به‌هم متصل می‌شوند، هک‌شدن آن‌ها می‌تواند ضررهای جبران‌ناپذیری را نظیر لو رفتن اطلاعات حساس، به‌همراه داشته باشد. اگرچه استفاده گسترده‌تر از این فناوری در سطوح مختلف نیروهای نظامی زمان‌بر خواهد بود، اما هم‌اکنون نیز می‌توان با کاربری‌های در دسترس‌تر و دقیق، منجر به کاهش هزینه‌ها و افزایش بهره‌وری شد. در بیشتر پژوهش‌های قبلی، تمرکز اصلی بر روی چالش‌های پیاده‌سازی اینترنت اشیا از بعد محیط خارجی بوده است (میورندی و همکاران، ۲۰۱۲؛ اسفار و همکاران، ۲۰۱۸؛ کانتی و همکاران، ۲۰۱۸). عرصه نظامی، یکی دیگر از عرصه‌هایی است که اینترنت اشیا بر آن تأثیر فراوانی خواهد داشت. برخی از منابع مانند محمدزاده و همکاران (۲۰۱۸) با توجه به اهمیت چالش‌های داخلی از طریق روش‌های تصمیم‌گیری چندمعیاره گزارشی از رتبه‌بندی این چالش‌ها ارائه کرده‌اند. همان‌طور که مشخص است بکارگیری فناوری اینترنت اشیا از ملاحظات هوشمندسازی سازمان است. نگاه به هوشمندسازی، نگاه راهبردی است، بنابراین تنها شناسایی عوامل و چالش‌های داخلی، کمک شایانی برای استقرار این فناوری نخواهد داشت و شناسایی عوامل درونی (نقاط ضعف و قوت) و عوامل بیرونی (تهدیدها و فرصت‌ها) برای انتخاب راهبرد مناسب امری ضروری است. از طرفی دیگر با وجود آن‌که این فناوری در حال حاضر به‌صورت کامل محقق نشده و در آستانه ظهور قرار دارد، پژوهش‌های گسترده‌ای در زمینه کاربردهای نظامی آن صورت گرفته است. نتیجه پژوهش نشان از آن دارد که امکان بکارگیری اینترنت اشیا با حفظ ملاحظات و به‌صورت محافظه‌کارانه وجود دارد اما با عنایت به نظر خبرگان، نحوه مهاجرت به این فناوری باید محتاطانه و با نگرش به تمام جوانب با حفظ نقاط قوت کلیدی صورت پذیرد و از مزیت‌های موجود در نقاط قوت برای پوشاندن نقاط ضعف استفاده شود. پلیس برای رسیدن به شرایط روزآمد و جلوگیری از عقب‌ماندگی از تبهکاران، باید به‌سمت هوشمندسازی ادوات و تجهیزات و سامانه‌های خود حرکت کند و برای این موضوع گریزی وجود ندارد و تنها گذشت زمان پلیس را از برنامه‌های آینده فاصله‌دارتر

خواهد کرد. با توجه یافته‌های پژوهش برای برطرف کردن آسیب‌های بکارگیری اینترنت اشیا در پلیس آگاهی، بهتر است با استفاده از فرصت خارجی به صورت مهاجرت نرم و کاملاً با احتیاط و بدون هرگونه شتابزدگی به این سمت حرکت کرد.

پیشنهادها

۱- قبل از بکارگیری فناوری اینترنت اشیا، الگوی راهبردی هوشمندسازی به‌منظور مدیریت خطر نقاط ضعف تدوین شود.

۲- قبل از بکارگیری فناوری اینترنت اشیا، الگوی راهبردی هوشمندسازی به‌منظور مدیریت خطر نقاط قوت تدوین شود.

۳- قبل از بکارگیری فناوری اینترنت اشیا، الگوی راهبردی هوشمندسازی به‌منظور مدیریت خطر فرصت‌ها تدوین شود.

۴- قبل از بکارگیری فناوری اینترنت اشیا، الگوی راهبردی هوشمندسازی به‌منظور مدیریت خطر تهدیدها تدوین شود.

۵- با نگاه به راهبرد محافظه‌کارانه، نقشه راه هوشمندسازی پلیس‌های تخصصی تدوین و براساس عوامل اساسی موفقیت هوشمندسازی، استقرار یابد.

سپاسگزاری

از همه کارشناسان، صاحب نظران و همکاران پلیس که در انجام این پژوهش محقق را یاری کردند، سپاسگزاری دارم زیرا بدون همکاری و همراهی آنها انجام این پژوهش مقدور نبود.

فهرست منابع

امیری، عبدالرضا. (۱۳۸۸). مطالعه فرصت‌ها و تهدیدات ناشی از ظهور فناوری‌های نوین اطلاعاتی: گامی به‌سوی تدوین راهبرد در ناجا. فصلنامه پژوهش‌های مدیریت انتظامی، ۴(۴)، صص ۶۰۱-۶۱۸. قابل بازیابی از:
http://pmsq.jrl.police.ir/article_92000.html.

براری، مرتضی؛ عارف، محمدرضا؛ بهشتی آتشگاه، محمد (۱۳۹۵). اینترنت اشیای نظامی: مفهوم و چالش‌های امنیتی. نهمین کنفرانس ملی فرماندهی و کنترل ایران، تهران، دانشگاه خوارزمی -انجمن علمی فرماندهی و کنترل ایران.

بی‌نام. (۱۳۹۶). مهمترین تهدیدات سایبری سال ۲۰۱۷. خبرنامه افتا، شماره ۲۲. قابل بازیابی از:
http://www.afta.gov.ir/portal/file/?237026/boultan-22.pdf

سخایی، محمدجواد. (۱۳۹۴). فناوری‌های اینترنت اشیا برای سال‌های ۲۰۱۷ و ۲۰۱۸ از نگاه گارتنر- فابک. قابل بازیابی از:

http://www.fabak.ir/ShowResourceDetailsForPublic.aspx?Side=XQDN1E96Ddw=
شفیعی، ساناز. (۱۳۹۴). تحلیل چالش‌های فراروی توسعه فناوری اینترنت اشیا. تهدیدات امنیتی و شکاف دیجیتالی. ماهنامه نوشتار کوتاه، ۱(۷)، صص ۱-۸. قابل بازیابی از:https://iotone.ir/shop/public/upload/article/5b9cb0f7cb738.pdf
طباطبایی، حبیب الله؛ منطقی، منوچهر؛ حنفی‌زاده، پیام؛ نقی‌زاده، محمد و نیرومند، پوراندخت. (۱۳۹۱). الگوی بهبود توانمندی فناورانه در بنگاه‌های دانش‌بنیان تأمین کننده تجهیزات الکترونیک پلیس بر پایه الگوی توانمندی پویا. فصلنامه پژوهش‌های مدیریت انتظامی، ۷(۲)، صص ۱۷۷-۱۵۹. قابل بازیابی از:.http://pmsq.jrl.police.ir/article_92064.html

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer networks, 54(15), pp 2787-2805. Retrieved from: https://doi.org/10.1016/j.comnet.2010.05.010.

Chen, S., Xu, H., Liu, D., Hu, B., & Wang, H. (2014). A vision of IoT: Applications, challenges, and opportunities with china perspective. IEEE Internet of Things journal, 1(4), pp 349-359. Retrieved from: https://ieeexplore.ieee.org/iel7/6488907/6702522/06851114.pdf.

Clearinghouse, P. R. (2003). RFID position statement of consumer privacy and civil liberties organizations. Privacy Rights Clearinghouse.

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems, 78(3), pp 544–546. Retrieved from: https://arxiv.org/pdf/1807.10438.

Dennis, M., & Dominik, H. P. (2010). Key problems and instantiations of the internet of things (IoT). In Proceedings of the TKK T-110.5190 Seminar on Internetworking.

Gohar, M., Ahmed, S. H., Khan, M., Guizani, N., Ahmed, A., & Rahman, A. U. (2018). A big data analytics architecture for the internet of small things. IEEE Communications Magazine, 56(2), pp 128-133. Retrieved from: https://ieeexplore.ieee.org/abstract/document/8291127/.

Halperin, D., Heydt-Benjamin, T. S., Fu, K., Kohno, T., & Maisel, W. H. (2008). Security and privacy for implantable medical devices. IEEE pervasive computing, 7(1), pp 20-39. Retrieved from: https://doi.org/10.1109/MPRV.2008.16 .

Ishtiaq Roufa, R. M., Mustafaa, H., Travis Taylora, S. O., Xua, W., Gruteserb, M., Trappeb, W., & Seskarb, I. (2010). Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study. In 19th USENIX Security Symposium, Washington DC.

Juels, A. (2006). RFID security and privacy: A research survey. IEEE journal on selected areas in communications, 24(2), pp 381-394. Retrieved from: https://www.researchgate.net/profile/Ari_Juels/publication/3236246_RFID_security_and_privacy_A_research_survey/links/00b4953bbe80a8c975000000/RFID-security-and-privacy-A-research-survey.pdf

Khedmatgozar, H. R. (2015). The role of internet of things (IOT) in knowledge management systems (Case study: Performance management of Yazd municipality staff). Journal of Information Technology Management, 7(3), pp 553-572. Retrieved from: https://doi.org/ 10.22059/JITM.2015.53916.

Luthra, S., Garg, D., Mangla, S. K., & Berwal, Y. P. S. (2018). Analyzing challenges to Internet of Things (IoT) adoption and diffusion: An Indian context. Procedia Computer Science, 125, 733-739. Retrieved from: https://www.sciencedirect.com/science/article/pii/S1877050917328624.pdf.

Maisel, W. H. (2010). Improving the security and privacy of implantable medical devices. The New

England journal of medicine, 362(13), p 1164. Retrieved from: https://pdfs.semanticscholar.org/d98f/2a7857ffbd0c883a8884531a254febea7684.pdf.

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. Ad hoc networks, 10(7), pp 1497-1516. Retrieved from: https://fardapaper.ir/mohavaha/uploads/2018/10/Fardapaper-Internet-of-things-Vision-applications-and-research-challenges.pdf.

Mohammadzadeh, A. K., Ghafoori, S., Mohammadian, A., Mohammadkazemi, R., Mahbanooei, B., & Ghasemi, R. (2018). A Fuzzy Analytic Network Process (FANP) approach for prioritizing internet of things challenges in Iran. Technology in Society, (53), pp 124-134. Retrieved from: https://fardapaper.ir/mohavaha/uploads/2019/04/Fardapaper-A-Fuzzy-Analytic-Network-Process-FANP-approach-for-prioritizing-internet-of-things-challenges-in-Iran.pdf.

Morgan, J. (2014). A simple explanation of' the internet of things. Forbes Leadership. Retrieved from: http://dublinohiousa.gov/dev/dev/wp-content/uploads/2016/02/A-Simple-Explanation-of-The-IoT.docx.

Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. Digital Communications and Networks, 4(2), pp 118-137. Retrieved from: https://doi.org/10.1016/j.dcan.2017.04.003.

Shah, S. H., & Yaqoob, I. (2016). A survey: Internet of Things (IOT) technologies, applications and challenges. In 2016 IEEE Smart Energy Grid Engineering (SEGE). IEEE.

Sorniotti, A., Gomez, L., Wrona, K., & Odorico, L. (2007). Secure and trusted in-network data processing in wireless sensor networks: a survey. Journal of Information Assurance and Security, 2(3), pp 189-199. Retrieved from: https://pdfs.semanticscholar.org/46ee/194f7a0b07869ecab6b210a6a857f3642437.pdf.

Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The Internet of Things—A survey of topics and trends. Information Systems Frontiers, 17(2), pp 261-274. Retrieved from: https://pdfs.semanticscholar.org/705f/e9247176e3f891b249c49b08492c295e507d.pdf.

Wobschall, D. (2008). Networked sensor monitoring using the universal IEEE 1451 standard. IEEE instrumentation & measurement magazine, 11(2), pp 18-22. Retrieved from: https://doi.org/10.1109/MIM.2008.4483729.