فصلنامهٔ امنیت پژوهی (علمی-پژوهشی)
سال پانزدهم: شماره ۵۴ – تابستان ۱۳۹۵

Amniat Pajouhi: A Security Studies Quarterly Research Journal
Vol 15, No 54, 2016 Summer

تاریخ دریافت: ۹۵/۰۲/۱۵ **تاریخ تأیید: ۹۵/۰۴/۲۵**

بررسی الزامات اجرایی معماری امنیت اطلاعات سازمانی در سازمان‌های دفاعی

محمود دی‌پیر[۱]
خداداد هلیلی[۲]
داود عبیری[۳]

چکیده

معماری امنیت اطلاعات سازمانی، یک راه‌حل جامع امنیتی است که برای جهت‌دهی و هم‌راستایی فرایندها، ساختارها و سازوکارهای امنیتی سازمان و پشتیبانی از اهداف حرفه به‌عنوان مکمل معماری سازمانی، استفاده می‌شود. با توجه به حساسیت مباحث امنیتی در این سازمان‌های دفاعی، سازوکارهای رایج معماری امنیت اطلاعات سازمانی، لزوماً برطرف‌کننده نیازهای این سازمان‌ها نیستند. هدف از انجام این پژوهش بررسی الزامات اجرایی معماری امنیت اطلاعات سازمانی در سازمان‌های دفاعی کشور است. در این پژوهش با ارائه الگویی مفهومی الزامات اجرایی معماری امنیت در سازمان‌های دفاعی بررسی شده و برای ارزیابی این الگو و اولویت‌بندی مؤلفه‌ها و شاخص‌ها، از روش الگوسازی معادلات ساختاری استفاده شده است. پژوهش حاضر ازنظر هدف، کاربردی و ازنظر روش، نوع توصیفی-پیمایشی است. پس از تحلیل نتایج، اولویت‌های اجرایی معماری امنیت اطلاعات سازمانی در سازمان‌های دفاعی استخراج گردید. ضرورت بومی‌سازی چارچوب‌های موجود، ضرورت توجه به اهداف، سیاست‌ها، چشم‌اندازها و برنامه‌های کلان به هنگام تدوین چارچوب امنیتی، بازخوردگیری در زمان اجرای چارچوب‌های امنیتی و دست‌یابی به زبان مشترک بین کارشناسان مجری، سیاست‌مداران و مدیران سطح عالی سازمان‌ها از نتایج ارائه شده در این پژوهش هستند.

واژگان کلیدی: *معماری سازمانی، معماری امنیت اطلاعات سازمانی، سازمان‌های دفاعی.*

---

۱. استادیار دانشکده رایانه و فناوری اطلاعات دانشگاه شهید ستاری، نویسنده مسئول (mdeypir@ssau.ac.ir)
۲. دانشجوی دکترای امنیت سایبر دانشگاه عالی دفاع ملی و عضو هیئت‌علمی دانشگاه شهید ستاری (kh.halili@sndu.ac.ir)
۴. دانشجوی دکترای امنیت سایبر دانشگاه عالی دفاع ملی (d.abiri@sndu.ac.ir)

مقدمه

امروزه بهره‌گیری از ابعاد مختلف فناوری اطلاعات و ارتباطات، حجم زیادی از داده‌ها و اطلاعات متنوع را به‌وجود آورده است که بخشی از دارایی و سرمایه مهم هر سازمان شناخته می‌شود. ازآنجاکه تمام فعالیت‌های یک سازمان بر پایهٔ اطلاعات بنا شده است؛ استفاده از سامانه‌های اطلاعاتی برای تولید و مدیریت اطلاعات، امری دوری ناپذیر است. این سامانه‌ها شامل انواع مختلفی مانند پردازش مبادلات[۱]، اطلاعات مدیریتی[۲]، پشتیبانی از تصمیم‌گیری[۳]، اطلاعات اجرایی[۴] و اتوماسیون اداری[۵] است.

الگوسازی و توصیف روابط سامانه‌های مختلف و پیچیدگی فرایندها در ارتباط بین کاربران، مدیریت و سامانه‌ها یکی از چالش‌های اساسی است که ضرورت به‌کارگیری معماری سازمانی[۶] را را مشخص می‌سازد. چارچوب‌های مختلفی برای معماری سازمانی ارائه شده است که از معروف‌ترین آن‌ها می‌توان به چارچوب‌های زکمن[۷]، چارچوب معماری دولت فدرال آمریکا[۸]، چارچوب معماری C4ISR[۹]، چارچوب توگاف[۱۰] و... اشاره کرد. این چارچوب‌ها قالب‌های کلی برای جنبه‌ها و دیدگاه‌های معماری سازمانی را مطرح می‌کنند (صمدی اوانسر، ۱۳۸۴: ۴۵).

استفاده از معماری سازمانی در صورتی بازدهی لازم را خواهد داشت که در تمامی ابعاد آن مسئله امنیت درنظر گرفته شود، در غیر این صورت با ایجاد مشکلات جدید سد راهی در برابر توسعه سازمان خواهد بود. در دنیای پر از آشوب و تلاطم و رقابتی امروز، تنها سازمان‌هایی قادر به تداوم حیات و عرضه موفق خدمات و کالاهای خود هستند که نگاهی متفاوت به ساختار

1.Transaction Processing Systems (TPS)
2.Management Information Systems (MIS)
3. Decision Support Systems (DSS)
4.Executive Information Systems (EIS)
5.Office Automation Systems (OAS)
6.Enterprise Architecture
7.Zachman
8.FEAF: Federal Enterprise Architecture Frameworke
9.Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
10.TOGAF: The Open Group Architecture

سازمانی و روش‌های عملیاتی داشته و امنیت را در تمامی فرآیندها، اهداف، چشم‌اندازها، راهبردها و برنامه‌ریزی‌ها درنظر گرفته باشند. برای این کار باید چارچوبی با عنوان چارچوب معماری امنیت تدوین و اجرا نمود. معماری امنیت اطلاعات سازمانی[1] (آیزا[2]) برای ترکیب دو موضوع امنیت و فرایند معماری سازمانی مطرح می‌شود. در این معماری با ایجاد زبان مشترک برای امنیت اطلاعات در یک سازمان، نحوه تعامل مناسب با معماری سازمانی مورد توجه قرار می‌گیرد.

برای آیزا، چارچوب‌های مختلفی وجود دارد. برخی از سازمان‌ها، چارچوب‌های اختصاصی خود را دارند که اطلاعات چندانی از آن‌ها موجود نیست. تعدادی از این چارچوب‌ها نیز مانند سابسا[3] سابسا[3] و گارتنر[4] جنبه عمومی پیدا کرده‌اند. در این مقاله با معرفی اجمالی و مقایسه این دو چارچوب معماری، ضرورت انجام معماری امنیت‌سازمانی و نقش آن در سازمان‌های دفاعی بررسی شده و در ادامه چگونگی اجرای آن به‌صورت بومی مورد بحث و ارزیابی قرار می‌گیرد.

بیان مسئله

برای انجام معماری سازمانی برخی از سازمان‌ها چارچوب‌های داخلی دارند و یا یکی از چارچوب‌های مرجع را شخصی‌سازی کرده‌اند. صرف‌نظر از چارچوب انتخابی، در معماری سازمانی سه هدف عمده؛ تدوین وضع موجود، تدوین وضع مطلوب و برنامه انتقالی برای حرکت از وضع موجود به وضع مطلوب، پیش‌بینی و درنظر گرفته شده است. این اهداف در تدوین، پیاده‌سازی و اجرای چارچوب معماری امنیت سازمانی نیز باید درنظر گرفته شود.

موضوع امنیت و طراحی و پیاده‌سازی آن، همواره یکی از دغدغه‌ها و چالش‌های اساسی و جدی یک سازمان قلمداد می‌شود. امنیت، فرایندی پویا به‌موازات سایر فرایندهای یک سازمان و فراتر از یک ابزار قابل‌واگذاری به یک شخص یا بخشی از سازمان، در یک محدوده زمانی مشخص

1. Enterprise Information Security Architecture (EISA)
2. EISA
3. SABSA
4. Gartner

است. این مسئله، اهمیت و لزوم تدوین معماری، برای برطرف نمودن مشکلات امنیتی را روشن می‌سازد. معماری امنیت اطلاعات سازمان، چارچوبی برای ارزیابی وضع موجود و ترسیم وضع مطلوب است. ایده اصلی آن، برگرفته از مباحث معماری سازمانی بوده و درواقع مفهومی جدای از آن نیست. این چارچوب می‌تواند براساس یکی از چارچوب‌های رایج بنا شود به‌شرطی‌که سازمان آن را در جهت اهداف و با توجه به شرایط خود، شخصی‌سازی و یا بومی‌سازی کند.

عده‌ای از کارشناسان معماری سازمانی اعتقاد دارند که در چارچوب‌های معماری سازمانی مانند زکمن، راه‌حل‌های امنیتی را هم می‌توان لحاظ کرد و نیازی به چارچوب‌های جداگانه برای معماری امنیت‌سازمانی نیست (خیامی، ۱۳۸۸: ۲۱)؛ اما در الگوی مفهومی ارائه شده در این پژوهش، با توجه به چارچوب‌های معماری سازمانی متداول، چارچوب‌های امنیت‌سازمانی تهیه شده است.

پژوهش‌های متعددی با هدف ارائه الگوهای معماری امنیت سازمانی انجام شده است. «استقرار معماری سازمانی به‌عنوان زیرساخت انجام معماری اطلاعات با توجه به ساختارها و فرایندهای سنتی سازمان‌ها» (نادری، فقیه و میرعباسی،۱۳۹۱: ۶۱-۹۶) و «مشخص نمودن خطوط راهنمای پیاده‌سازی معماری امنیت براساس لایه‌های کسب‌وکار، فرآیند، یکپارچه‌سازی، نرم‌افزار و زیرساخت در یک سازمان» (کارخانه و لامعی،۱۳۹۳ :۴۱۸- ۴۲۵) ازجمله این پژوهش‌هاست. بااین‌حال این الگوها لزوماً برطرف‌کننده نیازهای سازمان‌هایی با معماری خاص مانند سازمان‌های دفاعی نیستند.

الگوهای یادشده در کشورهای مختلف برای اهداف خاصی طراحی شده‌اند و نسخه‌برداری از آن‌ها پاسخگوی نیازهای سازمان‌های دفاعی کشور نخواهد بود. اجرای این الگوها پس از صرف هزینه‌های زیاد حتی ممکن است سازمان را با چالش‌های جدیدی روبرو کند. در سازمان‌های دفاعی کشور به‌دلیل وجود دشمن خارجی و ازطرفی حیطه‌بندی و سطوح دسترسی، تأمین امنیت اطلاعات از اهمیت بالایی برخوردار است. علاوه بر این، اهداف، دارایی‌ها، فرآیندها و

مأموریت‌ها در سازمان‌های دفاعی ما نسبت به سازمان‌های تجاری بسیار متفاوت است. فرهنگ سازمانی و مباحث انگیزشی مدیران در سطوح مختلف، در چگونگی اجرا و اثربخشی یک معماری امنیت اطلاعات سازمانی بسیار تأثیرگذار است؛ بنابراین با توجه به اهداف، سیاست‌ها، چشم‌اندازها و برنامه‌های کلان، بومی‌سازی چارچوب‌های موجود در این سازمان‌ها ضروری به‌نظر می‌رسد، که به همین جهت در این مقاله به آن پرداخته می‌شود.

اهمیت و ضرورت

به دلایلی مانند نبود بلوغ لازم برای معماری سازمانی، مجزا بودن و نا هماهنگی گروه‌های امنیتی و فناوری اطلاعات، معمولاً چارچوب‌های مجزایی برای معماری سازمانی و معماری امنیت اطلاعات سازمانی درنظر گرفته می‌شود. در سازمان‌های دفاعی توجه به مباحث امنیتی، از اهمیت و حساسیت ویژه‌ای برخوردار است، بنابراین تهیه و تدوین چارچوب معماری امنیت، امری ضروری قلمداد می‌شود. در کشورهای توسعه‌یافته، چارچوب‌های معماری سازمانی بومی برای افزایش کارایی و توان رزمی سازمان‌های دفاعی ایجاد شده است. استفاده از آیزا، مکمل معماری سازمانی است و برای دست‌یابی به اهدافی مانند بهینه‌سازی و چابک‌سازی فرایندها، کاهش پیچیدگی در سامانه‌های اطلاعاتی، ایجاد یکپارچگی، انعطاف‌پذیری در برابر تغییرات محیطی، کنترل، نظارت و اشراف اطلاعاتی، تضمین امنیت اطلاعات و ایجاد هماهنگی در سطوح مختلف مدیریت تدوین می‌شود. بررسی نحوه تدوین این معماری، جوابگو بودن در برابر نیازها و مأموریت‌های سازمان‌های دفاعی، ارتباطات فراسازمانی و چالش‌های اجرای معماری از اهمیت بالایی برخوردار است. همچنین، ذهنی و مجرد بودن چارچوب‌های رایج سبب سردرگمی در چگونگی اجرای معماری‌ها می‌شود. با توجه به شرایط سازمان‌های دفاعی و دقت در انجام فعالیت‌ها، نیازمند شناسایی جزئیات پیاده‌سازی و چگونگی اجرا در حوزه دفاعی هستیم. بااین‌حال چارچوب‌های موجود به‌صورت کلی هستند و چگونگی دقیق انجام کار و الزامات آن را در لایه‌های مختلف بیان نکرده‌اند. از دید حساسیت و دارای اهمیت امور نظامی و

دفاعی و ازآنجاکه بسیاری از مباحث سیاسی، امنیتی، اقتصادی و... به قدرت نظامی و دفاعی وابسته است؛ بنابراین لازم است چارچوب معماری امنیت سازمانی در سازمان‌های نظامی و دفاعی طراحی، تدوین، پیاده‌سازی و اجرا گردد.

اهداف پژوهش

هدف اصلی در این مقاله این است که بررسی و اولویت‌بندی الزامات اجرایی معماری امنیت اطلاعات سازمانی در سازمان‌های دفاعی چیست و هدف‌های فرعی آن عبارتند از:

۱. تعیین الزامات اجرایی معماری امنیت اطلاعات سازمانی در سازمان‌های دفاعی
۲. اولویت‌بندی الزامات و شاخص‌های مربوط به آن در سازمان‌های دفاعی

سؤال‌های پژوهش

سؤال اصلی پژوهش این است که الزامات اجرایی معماری امنیت اطلاعات سازمان‌های دفاعی چیست و اولویت‌بندی آن چگونه است؟ و سؤال‌های فرعی آن عبارتند از:

۱. الزامات اجرایی معماری امنیت اطلاعات در سازمان‌های دفاعی کشور چیست؟
۲. اولویت‌بندی الزامات و شاخص‌های مربوط به آن در سازمان‌های دفاعی کدامند؟

پیشینه پژوهش

در زمینه پیاده‌سازی و اجرای معماری سازمانی روش‌های مختلفی وجود دارد که در (Rouhani و Mahrin، 1:2015-20) بررسی و مقایسه شده است. ازآنجاکه دارایی‌های اطلاعاتی از سرمایه‌های مهم و باارزش سازمان قلمداد می‌شوند؛ الگوی جامعی برای طبقه‌بندی اطلاعات و معماری امنیت اطلاعات لازم است که در مقاله (تمتاجی و همکاران ،۱۳۹۴:۲۴۱-۲۶۴) معماری امنیت براساس رایانش ابری، برای آن ارائه شده است.

تلاش‌هایی برای یکپارچه‌سازی چارچوب معماری سازمانی با معماری امنیت اطلاعات انجام شده که از آن جمله می‌توان به یکپارچه‌سازی معماری امنیت سابسا با معماری سازمانی توگاف در مقاله (Kasarkod، 1:2011) اشاره کرد. در این ترکیب، امنیت محصول مجزایی نیست بلکه

نیازمندی‌های امنیتی سابسا و خدمات مربوطه به‌عنوان فرآورده‌های معمول توگاف درنظر گرفته می‌شوند. هدف از این کار، فراهم ساختن راهنمایی‌هایی برای توصیف چگونگی ترکیب دو معماری و تجمیع آسیب پذیری‌ها و فرصت‌های آن‌هاست.

یکی از اولین چارچوب‌های آیزا چارچوب گارتنر است که توسط (Scholtz، 2006:11-1) و (Robertson & Kreizman، 2006:8-1) بررسی شده است. پس‌ازآن چارچوب‌ها و الگوهای دیگری نیز مطرح شدند که از آن جمله می‌توان به چارچوب سابسا[1] (Clark & Sherwood، 2009:25-1)، چارچوب معماری امنیت خدمات‌گرای (Yan & Jianguang، 2008:358-351)، چارچوب اندرسون و راچامادوگو (Rachamadugu & Anderson، 2008:)، چارچوب ارزیابی امنیت سامانه‌های اطلاعاتی[2] (OISSG، 2006:13) و چارچوب بخش امنیت ملی آمریکا (GOA، 2007:82-1) اشاره کرد.

بررسی مستندات این چارچوب‌ها نشان می‌دهد که حتی جامع‌ترین این چارچوب‌ها، یعنی سابسا نیز در سطحی ذهنی تعریف شده و دارای مشکلاتی مانند تعریف نشدن مؤلفه‌های معماری امنیت و ارتباط آن‌ها، تعریف نشدن معماری امنیت اطلاعاتی سازمانی در سطوح پایین‌تر، نداشتن پوشش کامل نیازهای امنیت در ارتباطات فرا سازمانی باهدف تسهیل ارتباطات و حمایت از راهبرد حرفه، ارزیابی نکردن کامل و اثبات الگوهای ارائه شده برای معماری امنیت اطلاعات، هستند (Shariati، Shams & Bahmani، 2011:543 -537).

در همه این چارچوب‌ها، اصول پایه امنیت مانند محرمانگی، صحت و دسترس‌پذیری سرلوحه کار قرارگرفته است. برخی از این چارچوب‌ها مانند گارتنر به‌طور مستقیم و یا غیرمستقیم از چارچوب زکمن الهام گرفته و برخی نیز چارچوب‌های مستقلی هستند.

1.SABSA: Sherwood Applied Business Security Architecture
2.ISSAF: Information Systems Security Assessment Framework

در زمینه به‌کارگیری معماری سازمانی برای سازمان‌های دفاعی در مقاله (مرآتی، ۱۳۹۱: ۳۳-۶۰) به مزایایی مانند کاهش زمان توسعه چارچوب، کاهش خطر، کاهش هزینه و مدیریت بهتر فرایند توسعه چارچوب‌های معماری اشاره شده است.

مفاهیم و مبانی نظری پژوهش

معماری سازمانی

در هر سازمان برای هدایت و پشتیبانی از مأموریت‌های سازمانی، تداوم کسب‌وکار و تعامل با سایر سازمان‌ها، نیازمند یک معماری محوری هستیم که مستقل از اندازه، نوع مأموریت و گستردگی جغرافیایی سازمان، جهت‌گیری فعالیت‌ها و چشم‌انداز دست‌یابی به اهداف سازمان را مشخص کند. معماری سازمانی روشی است برای توصیف کامل جنبه‌ها و لایه‌های مختلف یک سازمان که قادر است با استفاده از الگوها و روش‌های استاندارد و شناخته‌شده، اقدام به توصیف وضع موجود یا وضع مطلوب سازمان نماید. معماری سازمانی حاوی طرح خاصی به‌نام طرح گذار نیز است که چگونگی رسیدن از وضع موجود به وضع مطلوب یک سازمان را مشخص می‌کند. خروجی شامل توصیف‌های متنی و ترسیمی از جنبه‌ها و لایه‌های مختلف معماری سازمانی است. نقشه‌های فنی، نمودارها و مستنداتی برای تعریف مأموریت‌ها، اطلاعات و فناوری‌های موردنیاز برای انجام مأموریت‌ها و فرآیندهای انتقالی لازم جهت راه‌اندازی فناوری های جدید در پاسخ به تغییرات مأموریت‌ها به‌کار می‌رود (صمدی اوانسر، ۱۳۸۴: ۴۲).

در معماری سازمانی، سازمان مشابه یک ساختمان فرض می‌شود که مالک خصوصیات و قابلیت‌هایی را که از ساختمان در ذهن دارد برای معمار بیان می‌کند. معمار، با استفاده از شکل‌ها و نقشه‌های مناسب، خواسته‌ها، انتظارها و تصورهای ذهنی مالک را در قالب معماری ترسیم نموده و ساختمان ایجاد می‌شود.

از دیدگاه زکمن، معماری سازمانی شامل مجموعه‌ای از الگوهای منطبق بر نیازمندی‌های مدیریت، برای توصیف یک سازمان است که در دوره حیات مفید خود قابل استفاده باشد و

تغییر نکند. تعریف معماری سازمانی در سال‌های اخیر به‌واسطه پیدایش سازمان‌های بزرگ، سامانه‌های اطلاعاتی پیچیده، تغییر مأموریت و ساختار سازمانی، فشار بازار و تغییر در فناوری‌های پدید و... دچار تغییر و تکامل شده است. برخی از مهم‌ترین مزایای استفاده از معماری سازمانی را می‌توان، کاهش هزینه و پیچیدگی، بهبود فرایندها، یکپارچگی توصیف نیازها و آینده‌نگاری تغییرات در مأموریت و کسب‌وکار سازمان درنظر گرفت.

معمولاً معماری سازمانی، توسط سه گروه مختلف با محوریت‌های فناوری اطلاعات، فرایند و دولت قابل استفاده است. معماری سازمانی برپایهٔ فناوری اطلاعات برای بهبود کارایی و بازدهی انجام می‌شود. برای مدیریت و سازمان‌دهی فرایندهای یک سازمان نیز معماری سازمانی کاربرد دارد. در معماری سازمانی دولت‌محور، با تقسیم سازمان به زیرمجموعه‌هایی با مدیریت خاص، هماهنگی ستادی بین آن‌ها توسط دولت انجام می‌شود.

معماری سازمانی را می‌توان پایگاه داده‌ای از اطلاعات راهبردی دانست که سازمان برای انجام مأموریت‌های خود از آن استفاده می‌کند. این معماری براساس الگوهای مختلف، سازمان را از دید کسب‌وکار و فناوری توصیف می‌کند. بنابراین از جهت پرداختن به کلیه جنبه‌های سازمانی، کامل و جامع است و می‌تواند تصویری یکپارچه از کلیه نیازمندی‌ها، ابعاد راهبردی، فرآیندی، فنی و عملیاتی را در گستره یک سازمان، نمایش دهد.

برای دست‌یابی به یک الگوی مفهومی برای ارائه راهنمایی‌های لازم در معماری سازمانی از چارچوب معماری استفاده می‌شود. در چارچوب معماری با استفاده از الگوهای پایه وضعیت فعلی و موجود مشخص می‌شود و با به‌کارگیری معماری سازمانی وضعیت آینده نیز معلوم می‌گردد. چارچوب‌های معماری راهنمای تکمیل و انجام عملی معماری سازمانی هستند. ازجمله چارچوب‌های موجود می‌توان به چارچوب معماری زکمن یا توگاف اشاره کرد.

یکی از اهداف اولیه در تدوین معماری، اطمینان از هم‌راستایی راهبردهای سازمانی و امنیت فناوری اطلاعات و ارتباطات است. استفاده از معماری امنیت در کنار معماری‌های رایج حرفه،

اطلاعات و فناوری[1]، آیزا را برای مرتبط ساختن راهبردهای حرفه به لایه‌های زیرین فناوری ایجاد نموده است (شریعتی،۱۳۸۹:۱۸).

معماری امنیت اطلاعات سازمانی (EISA)[2]

معماری امنیت اطلاعات سازمانی (آیزا)، مسیری از راهبردهای حرفه به لایه‌های زیرین فناوری ترسیم می‌کند. این معماری شامل مجموعه‌ای از اقدامات و روش‌های جامع و سخت‌گیرانه، برای توصیف ساختار و رفتار فرآیندهای امنیتی سازمان، سامانه‌های امنیت اطلاعات و زیربخش‌های شخصی و سازمانی است. هرچند در این معماری وابستگی زیادی به فناوری امنیت اطلاعات وجود دارد؛ اما بر بهینه‌سازی حرفه و هم‌راستایی اهداف اصلی و راهبردی سازمان با مأموریت نیز متمرکز است.

برای شناسایی نیازمندی‌های اطلاعاتی حرفه، تشخیص، تحلیل، ارزیابی مدیریت و اولویت‌بندی خطرها و تصمیم‌گیری در مورد بهترین راه‌حل‌های پیاده‌سازی امنیت یکپارچه در یک سازمان از چارچوب‌های معماری امنیت اطلاعات استفاده می‌شود.

در چارچوب‌های امنیت اطلاعات سازمانی، انگیزه اصلی برای شکل‌گیری چارچوب امنیتی، حفاظت از دارایی‌های اطلاعاتی سازمان، تحلیل خطر و نیازمندی‌های امنیتی حرفه است. برخی از مزایای اساسی که معماری امنیت سازمانی برای حرفه ایجاد می‌کند، عبارت‌اند از:

- **بهبود فرآیندهای نرم‌افزاری**: استانداردها، ممیزی، زمان و هزینه توسعه کم، مجموعه‌های سنجش امنیت اشتراکی و محیط‌های ساخت ساده‌شده که در آن برنامه‌های کاربردی می‌توانند محیطی را برای انجام آزمون‌های جامعیت برای نیازمندی‌هایی مانند کارایی و... به اشتراک بگذارند.
- **بهبود فرآیندهای حرفه**: به اشتراک گذاشتن مؤلفه‌های امنیتی که باعث کاهش هزینه‌های کل مالکیت فرآیندها می‌شود. ایجاد یک معماری مشترک امنیت برای

1.Business – Information -Technology
2.Enterprise Information System Architecture

بیشتر برنامه‌های کاربردی که به‌کار بستن آن، سریع‌تر و ساده‌تر خواهد بود. یعنی لازم نیست سازمان‌ها چرخ را از ابتدا اختراع کنند، درنتیجه مدیریت سامانه‌ها ساده‌تر خواهد شد.

- **بهبود در نیازمندی‌های غیر وظیفه‌مندی:** مانند بهبود امنیت تراکنش‌های مشتریان، قابلیت اطمینان و استحکام که شرکت‌ها از این روش می‌توانند خطری که باعث از دست رفتن شهرت یا سود شرکت می‌شود را کاهش دهند.
- **پاسخگویی بهتر به دلیل سازوکارهای سراسری تشخیص هویت و مجازشناسی.**

یک معماری قوی امنیت اطلاعات باید بتواند به پرسش‌های زیر پاسخ دهد:

۱. آیا معماری کنونی امنیت سازمان را پشتیبانی می‌کند و برای آن ارزش‌افزوده‌ای به‌همراه دارد؟
۲. چگونه می‌توان معماری امنیت سازمان را اصلاح کرد به‌گونه‌ای که ارزش‌افزوده به‌همراه داشته باشد؟
۳. براساس اهدافی که سازمان قصد دارد در آینده محقق سازد آیا معماری امنیت کنونی این اهداف را پشتیبانی می‌کند یا مانع آن‌ها می‌شود؟

یک معماری امنیت اطلاعات خوب، بایستی فرآیندی را طراحی و پیاده‌سازی کند که در آن نقش‌هایی برای حرکت از وضع موجود به وضع مطلوب، ارائه شده باشد. وضع مطلوب باید ترکیبی از موارد زیر باشد:

۱. کم کردن فاصله میان راهبردهای سازمان و قابلیت‌های زیاد امنیتی فناوری اطلاعات و ارتباطات برای پشتیبانی از سازمان.
۲. کم کردن فاصله میان راهبردهای آتی سازمان و قابلیت‌های امنیتی فناوری اطلاعات و ارتباطات برای پشتیبانی از آن‌ها.

۳. ارتقاء و به‌روزرسانی‌های لازم و جایگزینی‌هایی که باید در معماری امنیت فناوری اطلاعات و ارتباطات انجام شوند. این تغییرات باید متناسب با قابلیت‌های تأمین‌کنندگان، طول عمر و کارایی سخت‌افزارها و نرم‌افزارها، نیازمندی‌های تنظیم‌کننده شناخته‌شده یا قابل پیش‌بینی باشد.

۴. آیزا یک رویکرد کل‌نگر در مورد امنیت اطلاعات است که در قالب یک چارچوب معماری سازمانی ارائه می‌شود. چارچوب آیزا در سال ۲۰۰۶ مطرح شد و اولین تلاش برای معرفی معماری امنیت‌سازمانی بود که روی توصیف ساختار متمرکز شد؛ اما روش خاصی برای پیاده‌سازی نداشت. دو چارچوب اصلی در زمینه آیزا که نسبت به سایر چارچوب‌ها عمومی‌تر و فراگیرتر هستند عبارت‌اند از: چارچوب گارتنر و چارچوب سابسا که در ادامه مشخصات کلی آن‌ها بررسی می‌شود.

چارچوب معماری امنیت گارتنر[1]

چارچوب معماری امنیتی گارتنر یک چارچوب لایه‌بندی (سطح‌بندی) شده برپایهٔ معماری زکمن است. خروجی نهایی این چارچوب، مجموعه‌ای از مستندات معماری امنیت اطلاعات سازمانی، شامل کنترل‌های امنیتی (فرآیندها، سیاست‌ها و فناوری‌های مورداستفاده) است. از دیدگاه گارتنر، معماری امنیت باید در منطق حرفه و فرآیندهای سازمان نیز وارد شود و به همین دلیل بهتر است باید معماری امنیت با پروژه معماری سازمانی ادغام شود (Scholtz، 2006:11-1).

سه لایه اصلی در اینجا عبارت‌اند از: مفهومی، منطقی و پیاده‌سازی. دولایه مفهومی و منطقی، جان‌مایه چارچوب آیزا هستند. لایه حرفه به‌صورت مشخص در گارتنر وجود ندارد و این بخش در قسمت‌های چشم‌انداز و مفهومی، مستتر است. لایه پیاده‌سازی معادل لایه‌های فیزیکی و اجزاء در دیگر الگوهای معماری است. در شکل (۱) لایه‌های معماری امنیت‌سازمانی گارتنر

1.Gartner Information Security Architecture

نشان داده شده است. چارچوب گارتنر در کل، دیدی انتزاعی دارد و مستندات و جزئیات آن در دسترس نیست. با حرکت از لایه‌های بالاتر به لایه‌های پایین‌تر، نیازمندی‌ها، اصول و راه‌حل‌ها تقسیم شده و از ذهنی بودن آن‌ها کاسته می‌شود.

شکل ۱. معماری امنیت‌سازمانی گارتنر

(Scholtz، 2006:11-1)

این چارچوب که تشابهی با چارچوب‌های شناخته‌شده دیگر مانند زکمن، توگاف و... ندارد؛ یک چارچوب کاربردی است که سه دیدگاه وابسته به هم یعنی کسب‌وکار، اطلاعات و فناوری را درنظر گرفته است. در این معماری، با فرض اینکه معماری به‌عنوان یک راهبردی است؛ روی اجرای معماری تأکید شده است. در این الگو، موفقیت معماری سازمانی در گرو داشتن چشم‌انداز، رهنمودها، استانداردها و تصمیم‌گیری سازمانی است که نمایانگر جهت حرکت سازمان و چگونگی رسیدن به آن هستند.

ج) چارچوب سابسا[1]

سابسا یک الگوی جامع در زمینه معماری امنیت‌سازمانی ارائه می‌دهد که ساختاری مشابه با چارچوب زکمن دارد. لایه‌های افقی، دیدی امنیتی دارد و با چارچوب زکمن متفاوت است. ستون‌های ماتریس سابسا نیز مشابه زکمن، شامل شش سؤال اصلی است: چه چیز؟ (دارایی‌ها)، چرا؟ (انگیزه)، چگونه؟ (فرایند)، چه کسانی؟ (افراد)، کجا؟ (محل)، چه وقت؟ (زمان). در سطرهای ماتریس سابسا دیدگاه‌های کسب‌وکار، معمار، طراح، سازنده، تأمین‌کننده و مدیر خدمات با الگوهای معماری زمینه‌ای، مفهومی، منطقی، فیزیکی، مؤلفه‌ها و مدیریت خدمات امنیت قرار می‌گیرد. در جدول (۱) ماتریس معماری امنیت‌سازمانی سابسا نشان داده شده است.

چارچوب سابسا چارچوبی برپایهٔ خطر و کاملا عملیاتی است که مستندات آن موجود است. این چارچوب یک استاندارد باز، شامل چارچوب، الگوها، روش‌ها و فرایندهاست که به‌رایگان قابل‌دسترس است. چارچوب سابسا در مقایسه با گارتنر عملی‌تر است و با طراحی واضح، قابل‌فهم، متوازن و کامل براساس اصول طراحی سامانه‌ها بناشده است. این چارچوب توصیف‌های لازم را از همه جنبه‌ها و دیدگاه‌های سازمان ارائه می‌دهد. وابسته نبودن به راه‌حل‌های فناوری اطلاعات، بی‌طرف بودن نسبت به فروشنده و مقیاس‌پذیر بودن آن از دیگر ویژگی‌های این معماری است (Scott،2012:53).

1.SABSA: Sherwood Applied Business Security Architecture

جدول ۱: ماتریس معماری امنیت‌سازمانی سابسا

معماری(دید)	چه چیز؟ [دارایی ها]	چرا؟ [انگیزه]	چگونه؟ [فرآیند]	چه کسانی؟ [افراد]	کجا؟ [محل]	چه وقت؟ [زمان]
معماری امنیت زمینه (دید حرفه)	دارایی های حرفه(برند، شهرت، حرفه الکترونیکی امن، پیوستگی عملیاتی و پایداری)	تهدیدات و مخاطرات حرفه(اجبارهای قانونی، جلوگیری از کلاهبرداری و زیان، تضمین استمرار حرفه)	فرآیند های تأمین کننده امنیت(تعاملات، تراکنشها وارتباطات)	جنبه های سازمانی(حکمرانی و مدیریت ساختارها، روابط برون سپاری، شراکت های راهبردی)	جنبه های مکانی مرتبط با امنیت(بازار مجازی، سایت های همکار، دورکاری)	جنبه های مرتبط با زمان در حرفه(زمان ارائه به بازار، طول عمر و ضرب الاجل ها)
معماری امنیت مفهومی (دید معمار)	نیازمندیهای حرفه (نمایه سازی مشخصه های حرفه)	مدیریت ریسک (اهداف کنترلی و توانمندساز، معماری سیاست های امنیتی)	راهبردهای اطمینان از فرآیندها (چارچوب نگاشت فرآیند، معماری راهبردهای فناوری اطلاعات و ارتباطات)	نقش ها و مسئولیت ها (مالکان،،کاربران، تأمین کنندگان سرویس و مشتریان)	چارچوب دامنه (چارچوب و مفاهیم دامنه امنیت)	چارچوب مدیریت زمان (چارچوب مدیریت ریسک در دوره زمانی هر ریسک)
معماری امنیت منطقی (دید طراح)	دارایی های اطلاعاتی (انبار دارایی های اطلاعاتی)	سیاست های مدیریت ریسک (سیاست های دامنه)	نقشه فرآیندها و سرویس ها (جریان اطلاعات، تبدیلات عملیاتی، معماری سرویسگرا)	چارچوب اعتماد و موجودیت (شمای موجودیت، مدلهای اعتماد، نمایه های امتیازات)	نقشه های دامنه (تعاریف دامنه، تعامل ها و ارتباطات بین دامنه ای)	تقویم و جدول زمانی (زمان های شروع، دوره های زمانی و مهلت های زمانی)
معماری امنیت فیزیکی (دید سازنده)	دارایی های داده ای (دیکشنری داده، انبار داده)	فعالیت های مدیریت ریسک (روال ها و قوانین مدیریت ریسک)	مکانیزم های فرآیند (برنامه های کاربردی، میان افزارها، سیستم ها، مکانیزم های امنیتی)	واسط کاربری (واسط کاربری سیستم های اطلاعاتی و ارتباطی، سیستم های کنترل دسترسی)	فراساختار اطلاعات و ارتباطات (زیرساخت میزبان، شبکه ها و ساختار)	زمانبندی پردازش (زمانبندی و مرتب سازی فرآیندها و جلسات)
معماری اجزاء (دید	اجزاء فناوری اطلاعات و ارتباطات	استانداردها و ابزارهای مدیریت ریسک	استانداردها و ابزار فرآیند (ابزارها و	استانداردها و ابزارهای مدیریت کارکنان	استانداردها و ابزار مکان یابی (گره	زمانبندی گام ها و ابزارهای

فروشنده)	(محصولات ICT مانند، داده، انباره ها و پردازشگرها)	(ابزار تحلیل ریسک، ثبت کننده های ریسک، ابزارهای پایش و گزارش ریسک)	پروتکل های انتقال و نصب فرآیند)	(شناسه ها، توصیف مشاغل، نقش ها، توابع، لیست های کنترل دسترسی و فعالیت)	ها، آدرسی ها و سایز مکان یاب ها)	ترتیب (زمانبندها، ساعت، زمانسنج ها و وقفه ها)

(1-25:2009،Clark & Sherwood)

آیزا در سازمان‌های دفاعی

در هر کشور، سازمان‌های دفاعی وظیفه حفظ امنیت ملی، پاسداری از تمامیت ارضی، مقابله با تهدیدهای امنیتی و تأمین منافع ملی و دولتی را برعهده دارند. این سازمان‌ها با داشتن ویژگی‌هایی مانند وابستگی به دولت، اعتبار و مشروعیت دائمی بر پایهٔ قانون اساسی تأسیس می‌شوند. امنیت این سازمان‌ها پیش‌نیاز و زمینه‌ساز امنیت یک کشور است. در محیط پیچیده، پویا و پرخطر امروزی، سازمان‌های دفاعی با توجه به اهمیت مأموریت خود، ازنظر ساختار سازمانی، تجهیزات، فرماندهی‌وکنترل، آماد و پشتیبانی، خدمات اداری و ... نیاز به همگام شدن با تغییرات فناوری‌های نوپدید به‌ویژه فناوری اطلاعات و ارتباطات دارند. این امر، نیاز به ارائه رویکردی نوین در طراحی و بازآفرینی جنبه‌های مختلف این سازمان‌ها دارد که در عمل با معماری سازمانی دست‌یافتنی است.

همانند سایر سازمان‌ها، سازمان‌های دفاعی نیز باید مجموعه‌ای از سیاست‌های امنیتی را تنظیم کرده و راهنمایی‌هایی برای تمام کاربران تدوین کنند تا اهمیت محافظت از دارایی‌های سازمانی را برای آن‌ها روشن سازد (مرآتی، ۱۳۹۱:۶۰-۳). این دارایی‌ها، شامل مالکیت معنوی، اطلاعات مشتریان، برنامه‌های کاربردی حرفه، شبکه‌ها، ۳۳ مکان‌ها، تأسیسات فیزیکی و تجهیزات هست. یک سیاست امنیتی خوب باید برای هر موجودیت سازمانی، نیازمندی‌های امنیتی تعریف کند و بتواند از راه‌حل‌ها و حفاظت‌هایی که برای تأمین امنیت آن موجودیت طراحی شده‌اند، دفاع کند. به‌کار بستن سیاست‌های امنیتی نمی‌تواند تنها به‌وسیلهٔ احکام اداری انجام شود، بلکه باید به‌صورت یک فرهنگ سازمانی دربیاید که از سازمان و جذابیت‌های آن در برابر حمله‌های سایبری محافظت کند. در زمینه آیزا اقدامات و تجارب مفید و ارزشمندی در کشور انجام شده

است. در این پژوهش، ضمن بررسی آیزا در سازمان‌های دفاعی ابعاد اجرایی آن با استفاده از یک الگوی مفهومی پس از تأیید خبرگان، ارزیابی و اولویت‌بندی شده است.

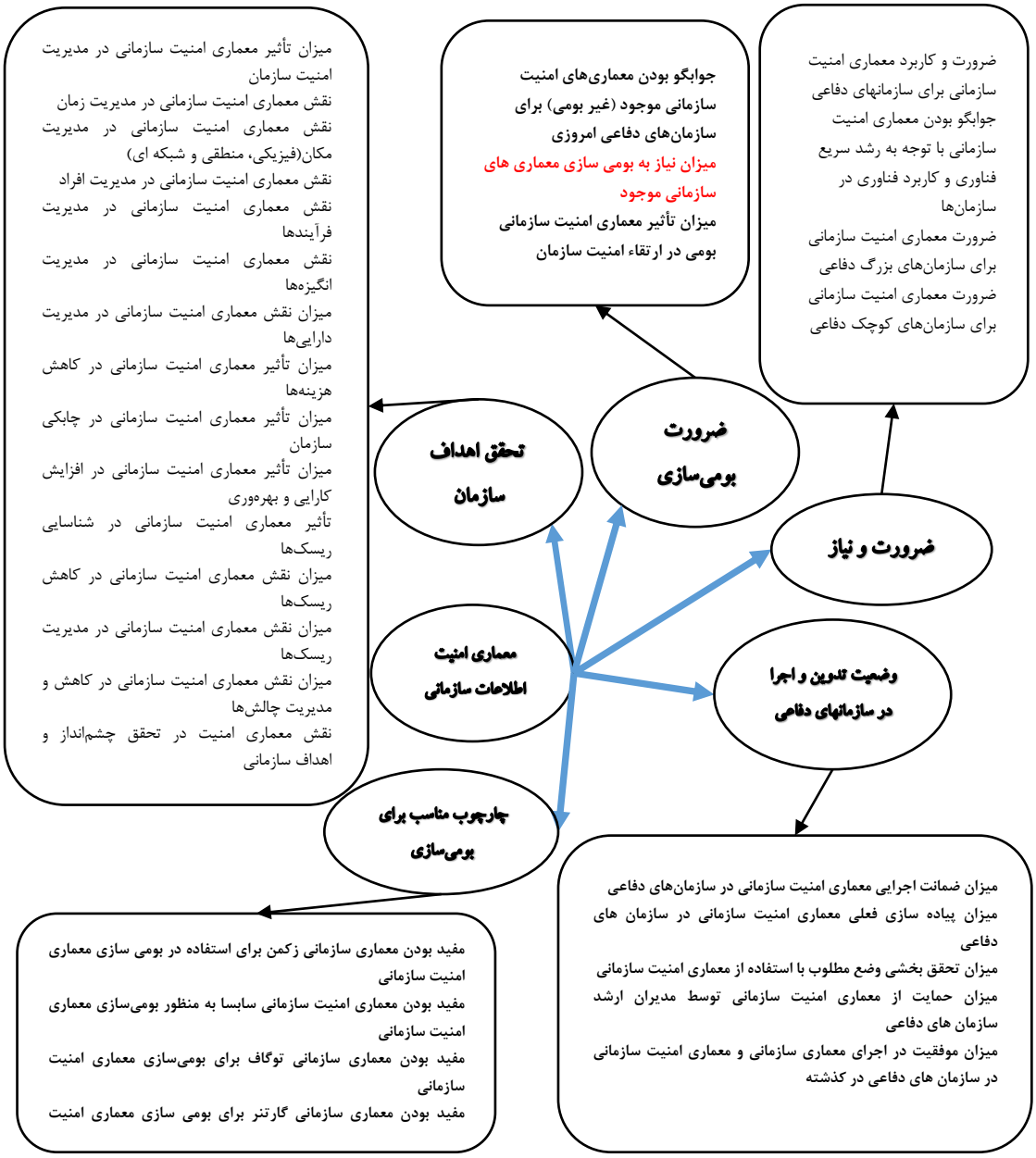
روش پژوهش

این پژوهش ازنظر هدف کاربردی و ازنظر روش از نوع توصیفی-پیمایشی است، جامعه آماری این پژوهش خبرگان و متخصصان حوزه امنیت فضای سایبر و جامعه نمونه نیز به روش نمونه‌گیری هدفمند و به روش اشباع نظری انجام و درمجموع از ۴۰ نفر متخصص یا خبره این حوزه استفاده شده است. ابزار گردآوری اطلاعات به روش مطالعه کتابخانه‌ای (سوابق، کتب، مجله‌ها، مقاله‌ها، پایگاه‌های اینترنتی) و همچنین نظر خبرگان و پرسشنامه محقق ساخته است که ازنظر روایی به تأیید خبرگان رسیده است؛ برای پایایی پرسشنامه نیز از ضریب آلفای کرونباخ، استفاده شد که نتیجه استخراج و میزان مورد تأیید ۰/۸۳۹ به‌دست آمده است. برای تجزیه‌وتحلیل داده‌ها، از نرم‌افزار SPSS و برای تعیین وزن مؤلفه‌ها و شاخص‌ها از نرم‌افزار Smart PLS استفاده شده است.

یافته‌های پژوهش

در این پژوهش، الزامات اجرایی معماری سازمانی توسط خبرگان (جامعه نمونه) بررسی شده و پرسش‌های مربوطه توسط اساتید و صاحب‌نظران تکمیل و در بخش مربوط به تجزیه‌وتحلیل آماری، نتیجه ارائه شده است. در شکل (۲) الگو مفهومی مربوط به این ابعاد نشان داده شده است. در این الگو پنج مؤلفه ضرورت و نیاز به چارچوب معماری امنیت برای مراکز دفاعی، ضرورت بومی‌سازی چارچوب معماری امنیت برای این مراکز، نقش چارچوب معماری امنیت در تحقق اهداف و چشم‌اندازهای سازمان‌های نظامی و دفاعی، انتخاب چارچوب‌ها و معماری‌ها مناسب برای بومی‌سازی و همچنین وضعیت تدوین و اجرای چارچوب‌های معماری امنیت در مراکز و سازمان‌های دفاعی از طریق ۳۱ شاخص تعیین شد؛ سپس نقش آن‌ها در سازمان‌های دفاعی بررسی‌شده، در ادامه چگونگی اجرای آن را به‌صورت بومی مورد بحث و ارزیابی قرارگرفته است.

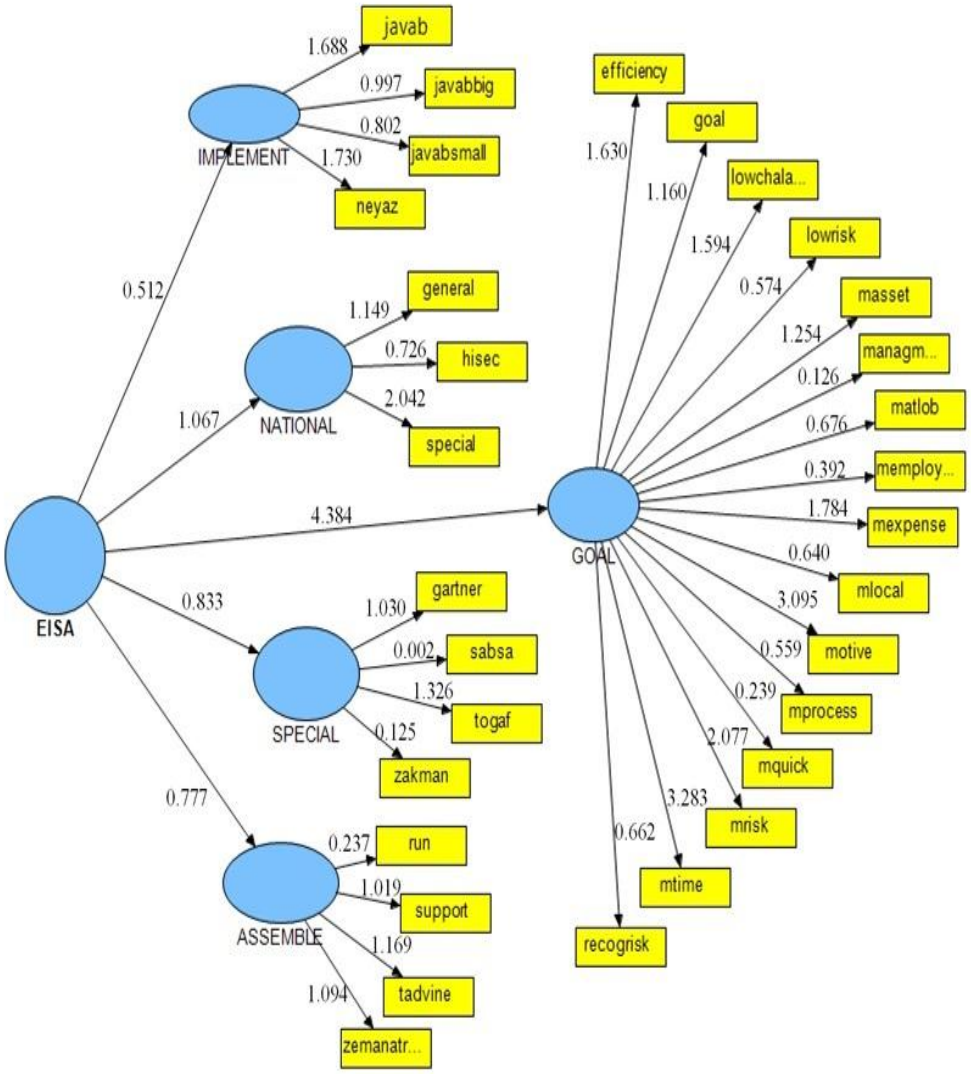
شکل ۲. الگوی مفهومی پژوهش



(یافته های پژوهش محققین)

برای اولویت‌بندی مؤلفه‌ها و شاخص‌های الگـوی مفهـومی از بخـش Bootstrapping نـرم‌افـزار Smart PLS برای محاسبه t-values استفاده شد. با رسم الگوی مفهومی، نتایج به‌دست آمـده از اجرای نرم‌افزار در شکل (۳) نشان داده شده است.

شکل ۳. الگوی آزمون bootstrapping **با استفاده از نرم‌افزار** smart pls



با توجه به مقادیر نشان داده‌شده، اولویت‌بندی مؤلفه‌ها در جدول (۲) نشان داده شده است.

جدول ۲. اولویت‌بندی مؤلفه‌های معماری

مؤلفه	اولویت
نقش چارچوب امنیتی در تحقق اهداف سازمان‌ها	۱
ضرورت بومی‌سازی چارچوب‌ها	۲
بومی‌سازی چارچوب امنیتی براساس چارچوب‌ها و معماری‌های موجود	۳
تدوین و اجرای چارچوب‌های امنیتی در سازمان‌های دفاعی	۴
ضرورت و نیاز به چارچوب‌های معماری امنیتی در سازمان‌های دفاعی کشور	۵

حال با توجه به اولویت‌بندی صورت گرفته به تشریح هرکدام از شاخص‌ها (سؤال‌ها) می‌پردازیم. در جدول (۳) تا (۷) نتایج اولویت‌بندی شاخص‌ها آمده است.

جدول ۳. شاخص‌های نقش چارچوب‌های امنیتی در تحقق اهداف سازمان‌ها (اولویت اول)

شاخص	امتیاز
نقش معماری امنیت سازمانی در مدیریت زمان	۳.۲۹۳
نقش معماری امنیت سازمانی در مدیریت انگیزه‌ها	۳.۰۹۵
میزان نقش معماری امنیت سازمانی در مدیریت خطرها	۲.۰۷۷
میزان تأثیر معماری امنیت سازمانی در کاهش هزینه‌ها	۱.۷۸۴
میزان تأثیر معماری امنیت سازمانی در افزایش کارایی و بهره‌وری	۱.۶۳۰
میزان نقش معماری امنیت سازمانی در کاهش و مدیریت چالش‌ها	۱.۵۹۴
میزان تأثیر معماری امنیت سازمانی در مدیریت امنیت سازمان	۱.۲۵۴
نقش معماری امنیت در تحقق چشم‌انداز و اهداف سازمانی	۱.۱۶۰
تأثیر معماری امنیت سازمانی در شناسایی خطرها	۰.۶۶۲
نقش معماری امنیت سازمانی در مدیریت مکان (فیزیکی، منطقی و شبکه‌ای)	۰.۶۴۰
میزان نقش معماری امنیت سازمانی در کاهش ریسک‌ها	۰.۵۷۴

نقش معماری امنیت سازمانی در مدیریت فرآیندها	۰.۵۵۹
نقش معماری امنیت سازمانی در مدیریت افراد	۰.۳۹۲
میزان تأثیر معماری امنیت سازمانی در چابکی سازمان	۰.۲۳۹
میزان نقش معماری امنیت سازمانی در مدیریت دارایی‌ها	۰.۱۲۶

جدول ۴. شاخص‌های ضرورت بومی‌سازی چارچوب‌های امنیتی است (اولویت دوم)

شاخص	امتیاز
میزان نیاز به بومی‌سازی معماری‌های سازمانی موجود	۲.۰۴۲
میزان تأثیر معماری امنیت سازمانی بومی در ارتقاء امنیت سازمان	۱.۴۱۹
جوابگو بودن معماری‌های امنیت سازمانی موجود (غیربومی) برای سازمان‌های دفاعی امروزی	۰.۷۲۶

جدول ۵. شاخص‌های بومی‌سازی چارچوب امنیتی براساس چارچوب‌ها و معماری‌های موجود (اولویت سوم)

شاخص	امتیاز
مفید بودن معماری امنیت‌سازمانی سابسا برای بومی‌سازی معماری امنیت سازمانی	۱.۳۲۶
مفید بودن معماری سازمانی گارتنر برای بومی‌سازی معماری امنیت‌سازمانی	۱.۰۳۰
مفید بودن معماری سازمانی زکمن برای استفاده در بومی‌سازی معماری امنیت‌سازمانی	۰.۱۲۵
مفید بودن معماری سازمانی توگاف برای بومی‌سازی معماری امنیت‌سازمانی	۰.۰۰۲

جدول ۶. شاخص‌های تدوین و اجرای چارچوب‌های امنیتی در سازمان‌های دفاعی (اولویت چهارم)

شاخص	امتیاز
میزان پیاده‌سازی فعلی معماری امنیت سازمانی در سازمان‌های دفاعی	۱.۱۶۹
میزان ضمانت اجرایی معماری امنیت سازمانی در سازمان‌های دفاعی	۱.۰۹۴

میزان حمایت از معماری امنیت سازمانی از سوی مدیران ارشد سازمان‌های دفاعی	۱.۰۱۹
میزان موفقیت در اجرای معماری سازمانی و معماری امنیت سازمانی در سازمان‌های دفاعی درگذشته	۰.۲۳۷

جدول ۷. شاخص‌های تدوین و اجرای چارچوب‌های امنیتی در ایران (اولویت پنجم)

شاخص	امتیاز
ضرورت و کاربرد معماری امنیت‌سازمانی برای سازمان‌های دفاعی	۱.۷۳۰
جوابگو بودن معماری امنیت‌سازمانی با توجه به رشد سریع فناوری و کاربرد فناوری در سازمان‌ها	۱.۶۸۸
ضرورت معماری امنیت سازمانی برای سازمان‌های بزرگ دفاعی	۰.۹۹۷
ضرورت معماری امنیت سازمانی برای سازمان‌های کوچک دفاعی	۰.۸۰۲

نتیجه‌گیری و پیشنهاد

نتایج پژوهش نشان می‌دهد از میان پنج مؤلفه انتخاب شده، دست‌یابی به اهداف سازمانی به‌وسیلهٔ چارچوب امنیتی در اولویت اول قرار دارد. ازآنجاکه هر سازمان متشکل از منابع انسانی، فناوری، ساختار و سرمایه اطلاعاتی است، هرکدام از این اجزاء با معماری سازمانی باید در راستای دست‌یابی اهداف سازمانی، به‌کار گرفته شوند. از طرفی هرچه اهداف شفاف، قابل دست‌یابی، واقع‌بینانه، منطبق با ارزش‌ها، دارای محدوده زمانی مشخص، مشارکتی و رقابتی باشند، فرایند استفاده از معماری امنیت اطلاعاتی سازمانی در تحقق اهداف سازمانی را هموارتر می‌سازند. توجه به مدیریت زمان در برنامه‌ریزی، شناخت و مدیریت انگیزه‌ها، مدیریت خطر و کاهش هزینه ازجمله مواردی هستند که در این مورد ترجیح داده می‌شوند.

ضرورت بومی‌سازی چارچوب‌های رایج در اولویت دوم قرار دارد که نشان می‌دهد چارچوب معماری انتخابی باید متناسب با شرایط و منطبق بر وضعیت موجود باشد؛ بنابراین توجه و عنایت ویژه از طرف مدیران و تصمیم‌گیرندگان سطح بالای سازمان‌های نظامی و دفاعی به این

موضوع و تأکید بر بومی‌سازی این چارچوب‌ها قبل از طراحی و اجرا، از اقدامات اساسی و قابل‌تأمل است.

در بسیاری از کشورها، به لزوم استفاده از چارچوب‌های امنیتی در معماری سازمانی پرداخته شده است. در جمهوری اسلامی ایران فعالیت‌هایی در سازمان‌ها و دستگاه‌های مختلف مانند وزارت جهاد کشاورزی، وزارت راه و ترابری، وزارت دفاع، وزارت امور خارجه و برخی شرکت‌های خصوصی، در زمینه این نوع معماری انجام شده است. بااین‌حال تدوین و اجرای چارچوب‌های امنیتی برای این معماری‌ها در شرایط کنونی کشور، از موارد دارای ابهام است که توجه کمتری به آن شده است.

با توجه به این‌که چارچوب‌های تدوین‌شده در ایران، شفاف، گویا و کامل نیستند، پس به‌طور کامل اجرا هم نشده‌اند. بنابراین ذهنیت خوبی نسبت به چارچوب‌های امنیتی در دید مدیران وجود ندارد. بنابراین لازم است ضمن تشریح اهمیت چارچوب‌های امنیتی، مطابق با اهداف سازمان، چارچوب بومی تهیه، تولید و زمینه اجرای آن توسط مسئولان فراهم گردد.

نبود حمایت و درک مناسب، از دلایل آن بی‌توجهی به این مسئله است. ازاین‌رو فرهنگ‌سازی مناسب و ایجاد زبان و فهم مشترک برای مدیران سطوح عالی این مسئله از الزامات ورود به این عرصه است.

پیشنهادهای زیر ازجمله اقداماتی است که می‌تواند در این زمینه مورد توجه قرار گیرد:

۱. شناخت کافی از اهداف، چشم‌اندازها، قوانین و اسناد بالادستی و... قبل از تدوین چارچوب امنیتی برای انطباق الزامات اجرایی معماری با تحقق اهداف سازمانی.
۲. ترغیب، تشویق و استفاده از تجارب موفق شرکت‌ها، مؤسسات و سازمان‌های خصوصی برای مشارکت در تدوین و اجرای معماری آیزا توسط دولت.
۳. تعامل سازمان‌های دفاعی با مراکز دانشگاهی و صنعتی برای مطالعه تطبیقی، انتخاب چارچوب معماری مناسب و بومی‌سازی آن با انجام نیازسنجی.

۴. آگاه‌سازی و جلب حمایت مدیران، متولیان و تصمیم‌گیران حوزه فناوری اطلاعات و ارتباطات برای اطمینان از تدوین مناسب و تضمین پیاده‌سازی کارآمد چارچوب معماری انتخاب‌شده.

۵. انجام ممیزی، بازرسی، دریافت بازخوردها و چک فهرست‌های امنیتی دوره‌ای برای اطمینان از جوابگو بودن چارچوب معماری، حرکت از وضع موجود به وضع مطلوب، هم‌راستایی با نیازمندی‌های امنیتی، انعطاف‌پذیری مناسب آن در رویارویی با تغییرات روزافزون فناوری.

منابع

۱. تمتاجی، مصطفی، مهدی نقیان فشارکی و غلامحسین طباطبایی .(۱۳۹۴). **الگوی طبقه بندی دارایی های اطلاعاتی سازمانی و متدولوژی معماری امنیت آن**. *پژوهشنامه پردازش و مدیریت اطلاعات*. ۱، ۲۴۱–۲۶۴.

۲. خیامی، سید رئوف .(۱۳۸۸). ***ارزیابی و تحلیل معمار سازمانی***. رساله دکترا، دانشگاه شیراز.

۳. شریعتی، مرضیه .(۱۳۸۹). *معماری امنیت اطلاعات سازمانی*. پایان‌نامه کارشناسی ارشد، دانشگاه شهید بهشتی، تهران.

۴. صمدی اوانسر، عسگر .(۱۳۸۴). ***مقدمه‌ای بر معماری سازمانی (ویژه مدیران)***. تهران: دبیرخانه شورای عالی اطلاع‌رسانی.

۵. کارخانه، هانیه و افشین لامعی .(۱۳۹۳). ***تدوین معماری بومی امنیت سازمانی براساس نیازمندی‌های لایه‌های معماری سازمانی***. هشتمین اجلاس فرماندهی و کنترل، تهران: انجمن فرماندهی و واپایش (کنترل) ایران، ۴۱۸-۴۲۵.

۶. مرآتی، احسان .(۱۳۹۱). ***تدوین روش توسعه چارچوب‌های معماری سازمان‌های دفاعی***. *فصلنامه سیاست دفاعی*، شماره ۷۹ زمستان ۱۳۹۱، ۳۳-۶۰.

۷. نادری، علیرضا، هادی فقیه و رمضان میر عباسی .(۱۳۹۱). ***معماری سازمانی زمینه‌ساز استقرار و توسعه معماری اطلاعات در دستگاه‌های دفاعی و اجرایی کشور***، فصلنامه سیاست دفاعی شماره ۷۹، زمستان ۱۳۹۱، ۶۱-۹۶.

8. Rachamadugu, V. & Anderson, J. A. (2008, July). ***Managing Security and Privacy Integration Across Enterprise Business Process and Infrastructure***. In *Services Computing, 2008. SCC'08. IEEE* International Conference on (Vol. 2, pp. 351-358). IEEE.
9. GOA. (2007). ***HOMELAND SECURITY. DHS Enterprise Architecture.*** United States Government Accountability Office.

10. Sun, J. & Chen, Y. (2008, November). ***Intelligent Enterprise Information Security Architecture Based on Service Oriented Architecture***. In Future Information Technology and Management Engineering, 2008. FITME'08. International Seminar on (pp. 196-200). IEEE.
11. Kasarkod ،J. (2011). ***Integration of SABSA Security Architecture Approaches with TOGAF ADM***. White Paper.
12. Kreizman, G. & Robertson, B. (2006). ***Incorporating Security into the Enterprise Architecture Process***. *Gartner, Inc*.
13. OISSG. (2006). ***Information Systems Security Assessment Framework.*** ISSAF.
14. Rouhani, B. D. Mahrin, M. N. R. Nikpay, F. Ahmad, R. B. & Nikfard, P. (2015). ***A systematic literature Review on Enterprise Architecture Implementation Methodologies.*** Information and Software Technology, 62, 1-20.
15. Scholtz ،T. (2006). ***Structure and Content of an Enterprise Information Security Architecture***. *Gartner Inc*.
16. Scott ،J. (2012). ***The Sabsa Model Excerpted from the Sabsa ،An Analysis of the sabsa Framework***. SABSA website.
17. Shariati, M. Bahmani, F. & Shams, F. (2011). ***Enterprise Information Security, a Review of Architectures and Frameworks from interoperability perspective***. Procedia Computer Science, 3, 537-543.
18. Sherwood ،J و A Clark. (2009). *Enterprise Security Architecture-A Business Driven Approach*. CRC Press ،by Taylor & Francis Group.