فصلنامه علمی امنیت ملی
سال دهم، شماره سی‌وششم، تابستان ۱۳۹۹
مقاله پنجم از صفحات ۱۸۲-۱۴۹

مقاله پژوهشی: ارائه چهارچوبی مفهومی جهت ایمن‌سازی سیستم‌های اطلاعاتی در سازمان‌های مبتنی بر رویکرد فراترکیب

سیما صدیقی گاریز[۱]، حمید زارع[۲]، ابوذر عرب‌سرخی[۳]، سید محمد محمودی[۴]

تاریخ دریافت: ۱۳۹۸/۰۴/۲۲ **تاریخ پذیرش: ۱۳۹۸/۰۷/۱۱**

چکیده

امنیت سیستم‌های اطلاعاتی معرف یک مسئله حیاتی است که امروزه بسیاری از سازمان‌ها با آن روبه‌رو هستند. این مقوله دربرگیرنده سه بعد انسانی، فنی و فرآیندی است. البته در اکثر تحقیقات صورت‌گرفته در این زمینه نوعی نگرش و رویکرد فنی وجود دارد. هدف پژوهش حاضر ارائه الگوی جدیدی است که الزامات امنیتی مناسب جهت مواجهه با تهدیدها و رفع آسیب‌پذیری‌های سیستم‌های اطلاعاتی را در هر سه بعد مذکور آدرس‌دهی می‌نماید. ازاین‌رو با استفاده از رویکرد فراترکیب ۲۵۵ مقاله بررسی گردید که پس از ارزیابی، ۷۶ مقاله جهت بررسی نهایی و استخراج کُدها تأیید گردیدند. از این مقالات تعداد ۴۷ تهدید (در هشت طبقه)؛ ۳۱ آسیب‌پذیری (در هشت طبقه)؛ ۱۵ الزام انسانی؛ ۳۴ الزام فنی (در هفت طبقه کلی) و ۱۷ الزام فرآیندی استخراج شده است. در پایان نیز الزامات امنیتی مناسب جهت مواجهه با هر تهدید و رفع آسیب‌پذیری‌های مربوطه – بر اساس استناد به بهترین تجربه‌های منتشرشده– انتخاب و در قالب یک چهارچوب جامع (سه‌بعدی) ارائه شده است. بیشترین فراوانی در بین تهدیدات مربوط به فعالیت‌های مجرمانه/ سوءاستفاده و کمترین فراوانی مربوط به چالش‌های انسانی است. در بین آسیب‌پذیری‌ها نیز بیشترین فراوانی مربوط به بروز فعالیت مجرمانه/ سوءاستفاده و کمترین فراوانی مربوط به ضعف در کنترل شکست/ خرابی است. بیشترین الزام انسانی مربوط به تدوین و اجرای برنامه‌های آموزشی در زمینه امنیت اطلاعات است و بیشترین الزام فنی مربوط به سازوکارهای امنیت اطلاعات و سامانه‌ها می‌باشد. این در حالی است که بیشترین الزام فرآیندی مربوط به تدوین قوانین، خط‌مشی‌ها، دستورالعمل‌ها و الزامات امنیت سیستم‌های اطلاعاتی در سازمان است.

کلیدواژه‌ها: تهدید، آسیب‌پذیری، الزام امنیتی، امنیت سیستم اطلاعاتی، فراترکیب

۱. دانشجوی دکترای مدیریت سیستم‌ها، پردیس فارابی دانشگاه تهران sima. sedighi@gmail. com
۲. دانشیار و عضو هیئت‌علمی دانشکده مدیریت و حسابداری پردیس فارابی دانشگاه تهران hzarea@ut. ac. ir
۳. استادیار و عضو هیئت‌علمی پژوهشگاه ارتباطات و فناوری اطلاعات (نویسنده مسئول) abouzar_arab@itrc. ac. ir
۴. دانشیار و عضو هیئت‌علمی دانشکده مدیریت و حسابداری پردیس فارابی دانشگاه تهران mahmoudi@ut. ac. ir

مقدمه

اطلاعات یکی از مهم‌ترین دارایی‌های سازمانی محسوب می‌شود. اهمیت اطلاعات و سیستم‌های اطلاعاتی تا جایی است که عده‌ای آن را به خونی در رگ‌های سازمان تشبیه کرده و عامل حیات‌بخش سازمان می‌دانند. با به خطر افتادن این جریان، سازمان از بین می‌رود؛ بنابراین به دلیل ارزش حیاتی اطلاعات برای سازمان باید حفاظت از آن به‌خوبی انجام شود (مسکل و همکاران، ۲۰۱۵). اهمیت اطلاعات در سازمان‌ها با توجه به فعالیت هر سازمان، سرمایه و نیز فناوری‌های اطلاعاتی در آن مجموعه بررسی می‌شود (الگزوی و همکاران، ۲۰۱٤).

سازمان‌ها دارای اطلاعات حساسی هستند که برای مزیت رقابتی بلندمدت آن‌ها اهمیت دارد؛ بنابراین هر نقصی در سیستم‌های امنیت اطلاعات می‌تواند برای آن‌ها تهدیداتی در پی داشته باشد. ازاین‌رو حفاظت از این اطلاعات به‌عنوان یکی از اهداف اصلی امنیت سیستم‌های اطلاعاتی به رسمیت شناخته شده است (تیسای و ژونگ، ۲۰۱٦).

تجمیع و استفاده مؤثر از اطلاعات تولید و منتشرشده در سازمان برای تصمیم‌گیری‌ها مستلزم مدیریت صحیح و نظام‌مند اطلاعات همانند سایر منابع سازمانی است. در این راستا چندین مدل سیستم اطلاعاتی با اهداف متفاوت – و بسته به نیاز کاربران– توسعه داده شده‌اند. سیستم پردازش تراکنش (TPS)، سیستم اطلاعاتی مدیریت (MIS)، سیستم پشتیبان تصمیم (DSS)، سیستم پشتیبان مدیران اجرایی (EIS)، سیستم برنامه‌ریزی منابع سازمان (ERP)، سیستم مدیریت ارتباط با مشتریان (CRM)، سیستم مدیریت گردش کار (WFMS) و سیستم مدیریت فرآیند کسب‌وکار (BPMS) از رایج‌ترین این موارد هستند. حجم سرمایه‌گذاری در حوزه ارتباطات و فناوری اطلاعات در سال ۲۰۱۸ میلادی برابر چهار تریلیون دلار برآورد شده است که این امر بیانگر اهمیت فزاینده این فناوری‌ها است(اخبار رایانش ابری، ۲۰۱۸).

در دو دهه گذشته تعداد سازمان‌های وابسته به سیستم‌های اطلاعاتی رو به افزایش بوده و نقش این سیستم‌ها به‌طور گسترده‌ای مورد پذیرش قرار گرفته است. در مواجهه با چنین روندی، هزینه‌های سازمان‌ها برای مقابله با حملات سایبری نیز به‌شدت افزایش داشته

است (گِرَندویو، ۲۰۱۸). بر اساس گزارش مک‌کافی تعداد حملات مخرب در سه ماه اول سال ۲۰۱۸ میلادی (نزدیک به ۷ میلیون) نسبت به سه ماه اول ۲۰۱۷ میلادی (نزدیک به پنج میلیون) تقریباً ۳۰٪ افزایش داشته است (مک‌کافی، ۲۰۱۸). بر اساس پیش‌بینی‌های مؤسسه گارتنِر و با توجه به افزایش تهدیدات، میزان سرمایه‌گذاری سازمان‌ها در حوزه امنیت اطلاعات در سال ۲۰۱۸ نسبت به سال ۲۰۱۷ بیش از ۸٪ افزایش داشته است. این رشد سرمایه‌گذاری در سال ۲۰۱۹ میلادی به میزان ۸,۷ درصد خواهد بود (گارتنِر، ۲۰۱۸).

با توجه به اینکه این سازمان‌ها در معرض انواع تهدیدات داخلی و خارجی قرار می‌گیرند، عدم کنترل مناسب سیستم‌ها و حفاظت از آن‌ها می‌تواند نتایج مخربی را به همراه داشته باشد. لذا ضرورت توجه به «امنیت اطلاعات» و «مدیریت امنیت اطلاعات» پیش از پیش احساس می‌شود (پاتاری و سونار، ۲۰۱۲). این امر سازمان‌ها را وادار به تغییر دیدگاه خود در مورد جنبه‌های امنیتی سیستم‌های اطلاعاتی نموده است (الگزوی و همکاران، ۲۰۱٤)؛ بنابراین در طی سال‌های اخیر، مسئله تأمین امنیت سیستم‌های اطلاعاتی به یکی از مهم‌ترین چالش‌ها و موضوعاتی تبدیل شده که مدیریت سازمان‌ها با آن مواجه هستند (بلانکو و همکاران،۲۰۱٤). البته مواجهه مؤثر با این چالش‌ها مستلزم توجه به جنبه‌های فرآیندی و عوامل انسانی امنیت – در کنار موارد فنی– است. ازاین‌رو، هدف اصلی تحقیق حاضر ارائه چهارچوبی مفهومی و جامع (با در نظر گرفتن جنبه‌های مختلف) برای ایمن‌سازی سیستم‌های اطلاعات در سازمان است. بر این اساس، محقق به دنبال آدرس‌دهی به سه رکن ایمن‌سازی در منابع اطلاعاتی سازمان (به‌عنوان اهداف فرعی تحقیق) است: شناسایی تهدیدات رایج علیه سیستم‌های اطلاعاتی سازمان و ارائه دسته‌بندی مناسب برای آن‌ها؛ شناسایی آسیب‌پذیری‌ها (ضعف‌های امنیتی) سیستم‌های اطلاعاتی سازمان و ارائه دسته‌بندی مناسب برای آن‌ها و شناسایی الزامات امنیتی (کنترل‌های امنیتی) مناسب برای مواجهه با هر دسته از تهدیدات یا آسیب‌پذیری‌های امنیتی – بر اساس نگاشت به تهدیدات/ آسیب‌پذیری‌های مرتبط– و ارائه دسته‌بندی مناسب برای آن‌ها.

باید به این موضوع توجه داشت که در مطالعات اخیر در حوزه امنیت اطلاعات به سازمان‌ها پیشنهاد می‌شود که از یک راهبرد کلی در زمینه امنیت اطلاعات استفاده نمایند. این راهبرد دربرگیرنده «افراد، فرایندها، فنّاوری و قابلیت‌های عملیاتی» است که دفاع اثربخش در سراسر سازمان را تضمین می‌نماید (هال و همکاران،۲۰۱۱)؛ بنابراین نیاز به استخراج معیارهای خوب برای تعریف الزامات امنیتی مناسب جهت مواجه با تهدیدها و رفع آسیب‌پذیری‌ها – به‌منظور تأمین امنیت اطلاعات در قالب یک چهارچوب جامع- امری ضروری است. ازاین‌رو، سؤال اصلی تحقیق حاضر عبارت است از: «چهارچوب جامع جهت ایمن‌سازی سیستم‌های اطلاعاتی چیست و ابعاد آن کدامند؟» برای پاسخ به این سؤال، محقق مجموعه‌ای از روش‌های نظام‌مند پژوهش را برای آدرس‌دهی به سه سؤال فرعی استفاده می‌نماید: تهدیدات رایج علیه سیستم‌های اطلاعاتی سازمان کدامند و دسته‌بندی مناسب برای آن‌ها چگونه است؟؛ آسیب‌پذیری‌ها (ضعف‌های امنیتی) سیستم‌های اطلاعاتی سازمان کدامند و دسته‌بندی مناسب برای آن‌ها چگونه است؟ و الزامات امنیتی (کنترل‌های امنیتی) مناسب برای مواجهه با هر دسته از تهدیدات یا آسیب‌پذیری‌های امنیتی کدامند و دسته‌بندی مناسب برای آن‌ها چگونه است؟

پیشینه تحقیق

با بررسی پژوهش‌های انجام‌شده در حوزه امنیت سیستم‌های اطلاعاتی طی سال‌های اخیر –ازجمله پژوهشی که توسط ENISA در سال ۲۰۱۷ انجام شده است- درمی‌یابیم که تأکید اصلی بر روند روبه‌رشد تهدیدات امنیتی است. حمله‌های بدافزاری، حمله‌های تحت وب، انسداد سرویس، تهدیدات درونی (عمدی/سهوی) و نشت اطلاعات از عمده این موارد هستند. نگاهی گذرا به پژوهش‌های انجام‌شده در حوزه امنیت سیستم‌های اطلاعاتی بیانگر خلأ تحقیقاتی در زمینه ارائه یک چهارچوب جامع است که دربرگیرنده تمامی ابعاد امنیتی در حوزه سیستم‌های اطلاعاتی و الزامات امنیتی مناسب برای مواجهه با تهدید و رفع آسیب‌پذیری‌ها باشد. لذا با توجه به روند روبه‌رشد تهدیدات امنیتی و خلأ دانشی موجود،

لزوم انجام پژوهش حاضر بیش از پیش نمایان می‌شود. خلاصه‌ای از مطالعات مهم انجام‌شده در این حوزه در قالب جدول (۱) ارائه شده است.

جدول ۱. پژوهش‌های انجام‌شده در حوزه امنیت سیستم‌های اطلاعاتی

عنوان پژوهش	مؤلف و سال پژوهش	محورهای پیشنهادی	روش‌شناسی
نقش تأثیرات درونی و بیرونی بر امنیت سیستم‌های اطلاعاتی-یک دیدگاه نوبنیادین	هیو و همکاران (۲۰۰۷)	-تهدید -الزام انسانی/ فرآیندی	مصاحبه و مطالعه موردی
مشارکت کاربر در مدیریت مخاطرات امنیتی سیستم‌های اطلاعاتی	اِسپیر و بارکی (۲۰۱۰)	-تهدید -الزام انسانی/ فرآیندی	پرسشنامه
اشتباهات امنیتی در پروژه‌های توسعه سیستم‌های اطلاعاتی	سامستاد و همکاران (۲۰۱۱)	-آسیب‌پذیری	شبکه بیزین
امنیت سیستم‌های اطلاعاتی مؤسسه (مطالعه موردی: بانک‌داری)	چائودری و همکاران (۲۰۱۳)	-تهدید -آسیب‌پذیری -الزام انسانی/فنی	مصاحبه‌های عمیق و مطالعه موردی
مدل‌سازی و ارزیابی تأثیر تهدیدات امنیتی بر سیستم‌های اطلاعاتی مؤسسه	جیمائیل و بودریگا (۲۰۱٤)	-تهدید	استفاده از مدل Petri Net
طبقه‌بندی تهدیدات امنیتی در سیستم‌های اطلاعاتی	جویینین و همکاران (۲۰۱٤)	-تهدید -آسیب‌پذیری	بررسی ادبیات موضوعی و ارائه یک مدل هیبریدی
طراحی معماری جدید امنیت سیستم‌های اطلاعاتی مبتنی بر تحلیل پوششی داده‌ها	یائو و وی (۲۰۱٤)	-تهدید -الزام فنی	تحلیل پوششی داده‌ها (DEA)
تهدیدات و آسیب‌پذیری‌های امنیت سیستم‌های اطلاعاتی	سافیانو و همکاران (۲۰۱٦)	-تهدید -آسیب‌پذیری -الزام انسانی/فنی	مصاحبه و آزمایش در چهار سناریو
یکپارچگی سیستم و امنیت سیستم‌های اطلاعاتی	بویکو و شنریک (۲۰۱۷)	-تهدید -آسیب‌پذیری -الزام انسانی/ فنی/ فرآیندی	بررسی ادبیات موضوعی
یک مدل مفهومی یکپارچه برای مدیریت ریسک امنیت سیستم‌های اطلاعاتی حمایت‌شده توسط مدیریت معماری سازمانی	مِیر و همکاران (۲۰۱۹)	-تهدید -آسیب‌پذیری -الزام انسانی/ فنی/ فرآیندی	استفاده از مفاهیم مدل‌های معماری سازمانی و مدیریت ریسک امنیت سیستم-های اطلاعاتی

عنوان پژوهش	مؤلف و سال پژوهش	محورهای پیشنهادی	روش‌شناسی
ارائه روشی مبتنی بر معیار کمّی و هفت‌بعدی جهت ارزیابی ریسک امنیتی در بستر سیستم‌های اطلاعاتی	باجلان و علی‌محمد ملایری (۱۳۹۱)	-آسیب‌پذیری -الزام فنی	مطالعه موردی
بررسی امنیت در سیستم‌های اطلاعاتی توسعه‌یافته با روش معماری سرویس‌گرا	تقوا و ایزدی (۱۳۹۲)	-الزام فنی/فرآیندی	مصاحبه با خبرگان و پرسشنامه
شناسایی و اولویت‌بندی عوامل مؤثر بر امنیت سیستم‌های اطلاعاتی سازمان با استفاده از مدل‌های تصمیم‌گیری چندمتغیره	خاک بیز (۱۳۹۵)	-تهدید -آسیب‌پذیری -الزام انسانی/فنی	استفاده از پرسشنامه با استفاده از روش تلفیقی DANP

از منظر بین‌المللی نیز معیار ارزیابی پذیرفته‌شده در زمینه امنیت سیستم‌های اطلاعاتی می‌تواند در سه دسته زیر قرار گیرد:

۱- معیار ارزیابی کارکردی برای امنیت رایانه (CC/ISO 15408)

۲- استانداردهای مدیریت امنیت اطلاعات (BS7799/ISO17799؛ ISO13335؛ ISO/IE27001؛ COBIT)

۳- استانداردهای ایمنی و فنی برای صنایع و حوزه‌های خاص (استاندارد رمزنگاری متقارن، استانداردهای امنیتی در حوزه و استانداردهای تبادلات امن الکترونیکی) (یون و همکاران، ۲۰۱۲).

سازمان‌ها نیز اغلب از بهترین تجربه‌های مندرج در استانداردهای مدیریت امنیت سیستم‌های اطلاعاتی -نظیر ISO/IEC27001؛NIST-SP800 و PCIDSS- پیروی می‌نمایند. با توجه به افزایش تهدیدات امنیتی در زمینه سیستم‌های اطلاعاتی، سازمان‌ها با فشارهای زیادی جهت پذیرش این استانداردها مواجه هستند (هسو و همکاران،۲۰۱۲).

باید به این موضوع توجه داشت که بررسی فعالیت‌های مرتبط بیانگر خلأهای دانشی جدی در این حوزه تحقیقاتی است که برخی از آن‌ها عبارت‌اند از: ۱) موضوعی/ بخشی بودن بسیاری از تحقیقات انجام‌شده (با تمرکز بیشتر بر ملاحظات فنی امنیت)؛ ۲) عدم جامعیت بررسی مؤلفه‌های ایمن‌سازی (تهدیدات، آسیب‌پذیری‌ها و الزامات) با توجه به روند فناوری‌های جدید و ظهور موارد تازه در این حوزه؛ ۳) عدم دسته‌بندی فراگیر

تهدیدات، آسیب‌پذیری‌ها و الزامات امنیتی (به‌واسطه بررسی موضوعی و موردی در تحقیقات قبلی)؛ ٤) عدم نگاشت تهدیدات به آسیب‌پذیری‌ها به‌صورت جامع و ارائه راهکار در این زمینه. ازاین‌رو، محقق با انجام تحقیق حاضر به دنبال آدرس‌دهی و پوشش خلأهای دانشی موجود در حدود محدودیت‌های پژوهش است.

روش‌شناسی پژوهش

فراترکیب یک مطالعه کیفی است که اطلاعات و یافته‌های استخراج‌شده از مطالعات دیگر را با موضوع مرتبط و مشابه بررسی می‌نماید؛ بنابراین نمونه مورد نظر برای فراترکیب از مطالعات منتخب و بر اساس ارتباط آن‌ها با سؤال پژوهش تشکیل می‌شود. فراترکیب مرور یکپارچه ادبیات کیفی موضوع مورد نظر نیست بلکه تجزیه‌وتحلیل یافته‌های این مطالعات است (خنیفر و همکاران، ۱۳۹۷). فراترکیب با ارائه نگرشی نظام‌مند برای پژوهشگران – از طریق ترکیب پژوهش‌های کیفی مختلف– به کشف موضوعات و استعاره‌های جدید و اساسی می‌پردازد. این روش معرف یک عصاره از تفسیر مطالعات مشابه نیست، بلکه یکپارچه‌سازی تفسیر یافته‌های اصلی مطالعات منتخب – به‌منظور ایجاد یافته‌های جامع و تفسیری– را در برمی‌گیرد که حاکی از فهم عمیق پژوهشگر در این زمینه است (زیمر،۲۰۰٦). فراترکیب مستلزم این است که پژوهشگر بازنگری دقیق و عمیقی انجام دهد و یافته‌های پژوهش کیفی مرتبط را ترکیب کند. از طریق بررسی یافته‌های مقالات اصلی پژوهش، پژوهشگران واژه‌هایی را آشکار و ایجاد می‌کنند که نمایش جامع‌تری از پدیده مورد بررسی را نشان می‌دهد (جعفری‌نژاد، مقبل باعرض و آذر، ۱۳۹۳).

در بخش اول، سؤال پژوهش مطرح می‌شود. اگر سؤال پژوهش خیلی محدود و سخت‌گیرانه باشد، سبب می‌شود که مطالعات معدودی شناسایی شوند و احتمال تعمیم یافته‌ها کاهش می‌یابد. حال چنانچه سؤال خیلی وسیع و نامحدود تنظیم شود، ممکن است نتیجه‌گیری کاربردی برای جامعه مورد نظر نداشته باشد. در این راستا و برای دستیابی به هدف مورد نظر با استفاده از روش فراترکیب سؤال‌های زیر تدوین شده است.

سؤال ۱- «تهدیدات امنیتی در حوزه سیستم‌های اطلاعاتی کدامند؟» شناسایی تهدید و عامل تهدید

سؤال ۲- «آسیب‌پذیری‌های امنیتی در حوزه سیستم‌های اطلاعاتی کدامند؟» شناسایی ضعف و عامل بروز تهدید

سؤال ۳- «الزامات امنیتی انسانی، فنی و فرآیندی در حوزه سیستم اطلاعاتی کدامند؟» شناسایی راهکار و ماهیت مواجهه

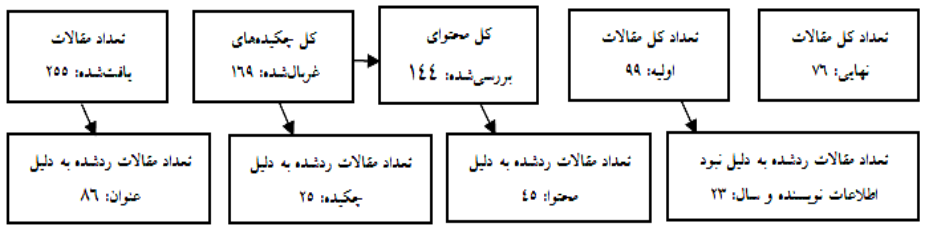
سؤال ٤- «از کدام الزام امنیتی در مواجهه با تهدید یا رفع آسیب‌پذیری استفاده می‌شود؟» نگاشت راهکار به مسئله

برای گردآوری داده‌های پژوهش از پژوهش‌های انجام‌شده (اعم از پژوهشی و مروری) در زمینه امنیت سیستم‌های اطلاعاتی استفاده شده است. به‌منظور شناسایی مؤلفه‌های چهارچوب امنیتی سیستم‌های اطلاعاتی به‌وسیله روش فراترکیب از روش هفت‌مرحله‌ای باروسو و ساندلوسکی (۲۰۰٦) استفاده شده است. پژوهشگر از انواع موتورهای جست‌وجو برای پیشبرد فعالیت پژوهشی استفاده نموده است. واژه‌های کلیدی که برای جستجو در پایگاه داده‌های IEEE، ساینس دایرکت، اِمِرالد، اشپرینگِر، گوگل اِسکولار، اِبسکو، پروکوئِست، وایلی اینتِرساینس، پایگاه مرکز اطلاعات علمی جهاد دانشگاهی (سیویلیکا)، مقالات علمی کنفرانس‌های کشور، پایگاه نشریات کشور (ماگ‌ایران)، ایران‌داک استفاده شده عبارت‌اند از: «امنیت سیستم‌های اطلاعاتی، تهدیدها، آسیب‌پذیری، الزامات امنیتی سیستم‌های اطلاعاتی، چهارچوب امنیتی، مدل امنیتی سیستم‌های اطلاعاتی، ریسک‌های امنیتی، اهداف امنیتی، معماری امنیتی سیستم‌های اطلاعاتی، ابعاد امنیتی در سیستم‌های اطلاعاتی، کنترل‌های امنیتی، مکانیزم‌های امنیتی، متغیرهای امنیتی، چالش‌های امنیتی در سیستم‌های اطلاعاتی و نیازهای امنیتی». معیارهای پذیرش مقالات نیز در قالب جدول (۲) ارائه شده است.

جدول ۲. معیارهای پذیرش مقالات

موضوع	معیار پذیرش
محدوده جغرافیایی	مطالعات معتبر داخلی و خارجی
زبان تحقیقات	فارسی و انگلیسی
زمان مطالعات	سال ۲۰۰۷ میلادی به بعد/ سال ۱۳۸۵ خورشیدی به بعد
روش‌های مطالعه	کیفی–مبتنی بر جمع‌آوری اطلاعات
جامعه مطالعه‌شده	مقالات مبتنی بر روش‌های کیفی
شرایط مطالعه	سنجش امنیت سیستم‌های اطلاعاتی
نوع مطالعه	مقالات چاپ‌شده در نشریات و کنفرانس‌های علمی معتبر داخلی و بین‌المللی؛ گزارش‌های معتبر جهانی؛ پایان‌نامه‌های کارشناسی ارشد و رساله‌های دکتری در داخل و خارج از کشور

در مرحله بعد، بررسی و انتخاب مقالات مناسب بر اساس مجموعه‌ای از شاخص‌ها در دستور کار پژوهشگر قرار گرفت. بر این اساس، شاخص‌های حاصل از گزینش مقاله‌ها طی روند جستجوی مقالات نهایی – برای پیشبرد روش فراترکیب– استخراج شدند. خلاصه‌ای از فرآیند انتخاب مقالات در قالب شکل (۱) به تصویر کشیده شده است.



شکل ۱. فرآیند انتخاب مقالات در روش فراترکیب

پژوهشگر در این تحقیق و به‌منظور تعیین روایی روش فراترکیب از ابزار ارزیابی حیاتی کَسپ (CASP) استفاده نموده است. بدین منظور تمامی پژوهش‌های انتخاب‌شده با ابزار CASP مورد ارزشیابی قرار گرفته‌اند. خروجی نشان‌دهنده آن است که ۷۶ کارهای پژوهشی منتخب، ارزش بالاتر از ۲۵ را به خود اختصاص داده‌اند. برای بررسی پایایی روش فراترکیب نیز از روش پایایی ارزیاب‌ها استفاده شده است. بدین‌صورت که علاوه بر محقق

-که نسبت به شناسه‌گذاری اولیه اقدام می‌نماید- یک محقق دیگر نیز همان متن را بدون اطلاع از شناسه‌های محقق و به‌صورت کاملاً مجزا شناسه‌گذاری می‌نماید. درصورتی‌که شناسه‌های این دو محقق به هم نزدیک باشد، نتیجه امر نشان‌دهنده توافق زیاد در بین این دو شناسه‌گذار است که بیان‌کننده پایایی روش فراترکیب است. ضریب توافق دو شناسه‌گذار یا پایایی ارزیاب‌ها از طریق رابطه شماره ۱ محاسبه می‌شود (سلکایند، ۱۳۸۵):

رابطه شماره ۱. تعداد توافق امکان‌پذیر / تعداد توافق = پایایی ارزیاب‌ها

در این راستا تعدادی از مقالات انتخابی در اختیار یکی از خبرگان قرار گرفت و ارزیابی کیفی مقالات (نمره‌دهی) به کمک ابزار CASP توسط خبره انجام شد. در ادامه نتایج حاصل از طریق ضریب توافق بین دو کُدگذار با شاخص کاپا و به کمک نرم‌افزار SPSS ارزیابی شد. از آنجایی که نتایج ضریب کاپا بالاتر از ۰/٦ است می‌توان گفت ضریب توافق در سطح خوبی واقع شده و مقالات استخراج‌شده با روش فراترکیب از پایایی خوبی برخوردار هستند.

یافته‌های تحقیق

یافته‌های این مرحله بیانگر این است که در مطالعات قبلی تاکنون چنین مطالعه نظام‌مندی انجام نشده است و هر یک از مطالعات، فقط به جنبه خاصی از امنیت سیستم اطلاعاتی -به‌ویژه جنبه‌های فناورانه- توجه نموده‌اند، بدون اینکه ابعاد چندگانه را در قالبی پویا و نظام‌مند در نظر گرفته باشند.

تهدیدات، آسیب‌پذیری‌ها و الزامات امنیتی سیستم‌های اطلاعاتی استخراج‌شده بر اساس تحلیل محتوای مقاله‌های منتخب در قالب جدول‌های ۳، ٤ و ۵ ارائه شده است. این جدول‌ها دربرگیرنده کُد استخراج‌شده (جواب‌های سؤالات تحقیق)، منابع استخراج کُدها و فراوانی آن‌ها در منابع مربوطه است. کُدهای استخراج‌شده در قالب گروه‌های مختلف تهدید، آسیب‌پذیری و الزامات امنیتی خوشه‌بندی شده‌اند که این فعالیت بر اساس روش تحلیل تِم انجام شده است. نام‌گذاری برای هریک از این خوشه‌ها (تهدید، آسیب‌پذیری و

الزامات امنیتی) در مرحله اول بر اساس استانداردهای مرجع (ISO، NIST، BS و ...) و در ادامه از طریق برگزاری پنل خبرگی یا مدل‌های مرجع موجود اعتبارسنجی شده است.

جدول ۳. تهدیدات امنیتی شناخته‌شده در سیستم‌های اطلاعاتی (کُدهای استخراج‌شده)

خانواده تهدید	تهدیدات (کُد استخراج‌شده)	مرجع	فراوانی
تهدیدات فیزیکی (عمدی/ غیرعمدی)	کلاه‌برداری	[۱۳] [۳۵] [۳۶] [۴۱] [۴۴] [۴۸][۶۱]	۷
	تخریب	[۲۱] [۳۱] [۳۲] [۳۵] [۳۶] [۴۱] [۶۶] [۷۲] [۷۴]	۹
	سرقت دارایی (دستگاه‌ها، حافظه و اسناد)	[۱۲] [۱۳] [۲۱] [۲۲] [۲۵] [۲۷] [۳۱] [۳۲] [۳۳] [۳۵] [۳۶] [۴۱] [۴۴] [۴۵] [۴۷] [۴۹] [۵۵] [۶۲] [۶۵] [۶۷] [۶۸] [۶۹] [۷۳]	۲۳
	نشت / اشتراک اطلاعات	[۳۱] [۴۴] [۴۷] [۵۶] [۶۰] [۶۶] [۶۸] [۷۱]	۸
	دسترسی فیزیکی غیرمجاز (ورود غیرمجاز)	[۱۰] [۱۳] [۱۸] [۲۰] [۲۲] [۲۵] [۲۶] [۲۷] [۲۹] [۳۱] [۳۲] [۳۴] [۳۹] [۴۱] [۴۴] [۴۹] [۵۵] [۶۰] [۶۴] [۶۵] [۶۶] [۶۹] [۷۲]	۲۳
	اخاذی	[۲۴] [۳۵]	۲
خسارت‌های غیرعمدی (مخدوش شدن منابع اطلاعاتی)	نشت اطلاعات به دلیل خطای انسانی	[۳۱] [۴۴] [۴۷] [۵۶] [۶۰] [۶۶] [۶۸] [۷۱]	۸
	استفاده / مدیریت نادرست سیستم	[۱۲] [۱۳] [۳۱] [۳۵] [۴۴] [۵۰] [۵۵] [۶۲] [۶۵]	۹
	استفاده از اطلاعات منابع غیرقابل اعتماد	[۱۸] [۳۱]	۲
	تغییر غیرعمدی داده در سیستم	[۱۳] [۱۸] [۲۱] [۳۱] [۳۵] [۴۴] [۴۷] [۴۸] [۴۹] [۵۱] [۵۶] [۶۴] [۷۶]	۱۳
	خسارت ناشی از رفتار طرف ثالث	[۳۱] [۴۴] [۶۸]	۳
	خسارت ناشی از تست نفوذ	[۱۸] [۶۰] [۶۵] [۶۸] [۶۹]	۵
	از دست رفتن اطلاعات در فضای ابر	[۲۱] [۳۱] [۳۲]	۳
	از دست رفتن/ تخریب/ مخدوش شدن دارایی	[۲۰] [۳۱] [۴۸] [۶۸]	۴

خانواده تهدید	تهدیدات (کُد استخراج‌شده)	مرجع	فراوانی
فاجعه (طبیعی/ محیطی) (T3)	سیل/ طوفان	[۱۳] [۳۱] [۳۵] [٤۸] [٦٥] [٦٦] [۷۲]	۷
	آتش‌سوزی	[۱۳] [۲۷] [۳۱] [۳٥] [٤۸] [٦٥]	٦
	زلزله	[۱۳] [۳۱] [۳٥] [٤۸] [٦٥] [۷٤]	٦
	آلودگی (گردوغبار، زنگ‌خوردگی و ...)	[۳۱] [٦٦] [۷۲]	۳
	شرایط نامساعد آب و هوایی	[۱۳] [۳۱] [۳٥] [٦٥]	٤
شکست / خرابی	خرابی یا اختلال لینک‌ها/ شبکه‌های ارتباطی	[۳۱] [٥۲] [۷۰] [۷٤]	٤
	خرابی یا اختلال زنجیره تأمین خدمت	[۳۱] [٤۸]	۲
	خرابی تجهیزات (دستگاه یا سیستم)	[۲۱] [۲٦] [۲۷] [۳۱] [۳۲] [٤٤] [٥۲] [٥٥] [٦۲] [٦٦] [۷۰] [۷۲]	۱۲
چالش‌های انسانی	غیبت کارکنان	[۳۱] [٦٦]	۲
	اعتصاب	[۳۱]	۱
انسداد خدمت	استراق سمع در مسیر انتقال داده‌ها/ سرقت نشست / ره‌گیری اطلاعات محرمانه	[۱] [۱۲] [۱۳] [۱۸] [۲۱] [۲٥] [۲۹] [۳۱] [۳۲] [۳۹] [٤۹] [٥٦] [٦۲] [٦٤] [٦٦] [٦۸] [٦۹] [۷۳] [۷٤]	۱۹
	گشت‌زنی در شبکه‌های بی‌سیم بی‌حفاظ	[۳۳] [٥٦]	۲
	دست‌کاری ترافیک شبکه / حمله مرد میانی/ جمع‌آوری و دست‌کاری اطلاعات	[۳۱] [٤۸] [٥٤]	۳
فعالیت مجرمانه/ سوءاستفاده	سرقت هویت (حساب)/ کلاه‌برداری/ استفاده از گواهی‌نامه‌های تقلبی	[۱۲] [۱۳] [۲۲] [۳۱] [۳۳] [۳٥] [٤٤] [٤۸] [٥٤] [٦۲]	۱۰
	دریافت پست‌های الکترونیکی ناخواسته (هرزنامه)	[٤] [۱۲] [۲٥] [۳۲] [۳۳] [۳٥] [۳۸] [٤٦] [٥٥] [٦۰] [٦٦] [٦۸] [٦۹]	۱۳
	انسداد سرویس	[۱۲] [۱۳] [۲٥] [۲٦] [۳۱] [۳۲] [۳۳] [۳٥] [٤٤] [٤۹] [٥۲] [٥٥] [٦۰] [٦٤] [٦٥] [٦۷] [۷۳]	۱۷
	اجرا (تزریق) کد/ نرم‌افزار/ فعالیت مخرب	[۱] [٤] [۱۰] [۱۲] [۱۳] [۲۰] [۲۲] [۲٥] [۲۹] [۳۱] [۳۲] [۳۳] [۳٤] [۳٥] [۳٦] [۳۸] [٤۰] [٤٤] [٤٥] [٤۹] [٥٥] [٦۰] [٦۲] [٦٤] [٦٥] [٦٦] [٦۷] [٦۸] [٦۹] [۷۲]	۳۰

خانواده تهدید	تهدیدات (کُد استخراج‌شده)	مرجع	فراوانی
	مهندسی اجتماعی	[٤] [٥] [١٢] [١٣] [١٤] [١٨] [٢١] [٢٦] [٣٢] [٣٣] [٣٥] [٣٨] [٤٥] [٤٦] [٥٩] [٦١] [٦٢] [٦٥] [٦٦] [٦٨] [٦٩]	٢١
	دست‌کاری سخت‌افزار و نرم‌افزار	[٣١] [٦١] [٦٢] [٦٦]	٤
	دست‌کاری اطلاعات	[٩] [١٢] [١٣] [٣١] [٥٦] [٦١] [٦٤] [٧٥]	٨
	سوءاستفاده از ابزارهای ممیزی	[٣١] [٣٩]	٢
	نصب و راه‌اندازی غیرمجاز نرم‌افزار	[١٩] [٣١] [٥٦] [٦٩]	٤
	سوءاستفاده از اطلاعات محرمانه	[١٢] [٢٠] [٣١] [٣٣] [٣٦] [٤٤] [٦٧] [٧٣] [٧٦]	٩
	فعالیت مخرب از راه دور	[٤٤] [٦٨] [٦٩]	٣
	حملات هدفمند (APT)	[١٢] [٣١] [٣٢] [٤٤] [٦٩]	٥
	جستجوی جامع	[١٣] [١٨] [٢٥] [٤٤] [٥٦] [٦٨]	٦
تهدیدات قانونی	دور زدن الزامات قراردادی	[٣١] [٤٤] [٦٦]	٣
	استفاده غیرمجاز از منابع حفاظت‌شده (IPR)	[١٣] [٢٥] [٥٥]	٣
	سوءاستفاده از داده‌های خصوصی	[١٣] [٢٥] [٣١] [٥٢] [٧٣]	٥

جدول ٤. آسیب‌پذیری‌های امنیتی استخراج‌شده در سیستم‌های اطلاعاتی (کُدهای استخراج‌شده)

خانواده آسیب‌پذیری	عنوان آسیب‌پذیری (کُدهای استخراج‌شده)	مرجع	فراوانی
دسترسی فیزیکی غیرمجاز (عمدی/ سهوی)	ضعف در آموزش کارکنان	[١٤] [١٨] [٢٧] [٣٣] [٣٨] [٤٤] [٤٥] [٤٦] [٤٩] [٥٠] [٥٢] [٥٥] [٦٢] [٦٧] [٦٩] [٧٦]	١٦
	احراز هویت ناکارآمد	[٢٥] [٢٩] [٣٥] [٥٦] [٦٤] [٧٣]	٦
	قابلیت خواندن حافظه خارجی در دستگاه‌های قابل حمل	[٣٠]	١
ضعف در نگهداری منابع اطلاعاتی	مدیریت خطا به شیوه نادرست	[٣٥]	١
	امکان تغییر در اطلاعات سامانه	[٤٨] [٧٣] [٧٤] [٧٦]	٤
	تفویض اختیار ناکارآمد	[٢٥]	١

خانواده آسیب‌پذیری	عنوان آسیب‌پذیری (کُدهای استخراج‌شده)	مرجع	فراوانی
	پیکربندی ضعیف سامانه	[۱۸] [۳۲] [٤٤] [٤٩] [٦٢] [٦٦]	٦
	ارزیابی امنیتی ناکارآمد فناوری‌ها	[٤٤] [٦١]	٢
	خط‌مشی و دستورالعمل‌های ناکارآمد	[٢٥] [٣١] [٣٩]	٣
محیطی	سازوکار نادرست در قفل‌گذاری منابع	[٤١] [٥٢] [٥٦] [٥٩] [٦٨] [٦٩]	٦
	مکان‌یابی ناکارآمد تجهیزات	[٦٣]	١
	تأثیر تجهیزات از شرایط آب و هوایی	[٣٧] [٤١]	٢
ضعف در کنترل شکست/ خرابی	شکست در اجرای سازوکار حفاظتی	[٥٥] [٥٦] [٧٣]	٣
	ضعف در مدیریت انرژی تجهیزات	[٣٩] [٦٦]	٢
نقص در زیرساخت ارتباطی	طراحی ضعیف سیستم	[٢٨] [٦٣] [٧٦]	٣
	از دسترس خارج شدن شبکه ارتباطی	[٢٧] [٣١] [٧٠]	٣
	در دسترس نبودن پشتیبان خدمات ارتباطی	[٣١] [٣٥]	٢
	شبکه اینترنتی ناامن	[١٨] [٤٤] [٥٥] [٦٥]	٤
	طراحی و برنامه‌ریزی ناکارآمد	[١٨] [٢١] [٣١] [٣٥] [٤٥] [٤٨] [٥٠] [٥٦] [٥٩] [٧٢]	١٠
حفاظت ناکافی در مقابل شنود/ ره‌گیری	وجود شبکه ارتباطی بی‌سیم ناامن	[٤٨] [٦٣]	٢
	انتقال ناامن اطلاعات	[٤٩] [٧١]	٢
	مدیریت نادرست ارتباطات و سرقت نشست	[١٢] [٢٥] [٣٢] [٤٩] [٦٨] [٦٩] [٧٣]	٧
بروز فعالیت مجرمانه/ سوءاستفاده	ضعف در سازوکارهای کنترل دسترسی	[٣٩] [٥٦] [٥٩] [٦٣] [٦٩]	٥
	اجرای کُدها/ دستورات غیرمجاز	[١] [٤] [١٠] [١٢] [٢٥] [٢٩] [٣١] [٣٣] [٣٤] [٣٥] [٣٦] [٤٠] [٤٤] [٤٥] [٤٩] [٥٤] [٦٠] [٦٧] [٦٨] [٦٩] [٧٢]	٢١
	عدم به‌کارگیری الگوریتم‌های معتبر رمزنگاری	[٤١] [٣٢] [٥٦] [٥٩] [٦٨] [٦٩]	٦
	امکان دست‌کاری در ورودی‌ها	[٢٩] [٣٩] [٦٢]	٣
	ضعف در مواجهه با روش‌های مهندسی اجتماعی	[١٤] [٢٤] [٣٣] [٣٨] [٤٤] [٤٦] [٥٥] [٦١] [٦٧] [٦٩]	١٠
	ضعف در شناسایی شبکه‌های طعمه و فعالیت‌های مخرب	[١٤] [٣٣] [٣٨] [٤٤] [٥٥] [٦١] [٦٧] [٦٩]	٨

خانواده آسیب‌پذیری	عنوان آسیب‌پذیری (کُدهای استخراج‌شده)	مرجع	فراوانی
مسائل قانونی	حفاظت ناکافی در مقابل چالش‌های حریم خصوصی	[۱۳] [۲۱] [۳۵] [۵۲] [۵۹] [٦٥]	٦
	خلأهای قانونی پیرامون فعالیت‌های طرف ثالث	[۳۱]	۱
	قوانین بازدارنده و ناکارآمد	[۳۱] [٦٨]	۲

جدول ۵. الزامات انسانی/ فنی/ فرآیندی در حوزه امنیت سیستم‌های اطلاعاتی (کُدهای استخراج‌شده)

خانواده الزام	زیرگروه/ عنوان الزام (کُدهای استخراج‌شده)	مرجع	فراوانی
انسانی	همراهی کارکنان با خط‌مشی‌های امنیت اطلاعات سازمان	[۲۲] [٢٤] [٣٦] [۳۸] [۵۷]	۵
	حمایت مدیریت عالی از برنامه‌ها، پروژه‌ها و خط-مشی‌های امنیتی سازمان	[۵] [٦] [۹] [۱۱] [۲۳] [۳۸] [۵۰] [۵۷] [٦١] [٦٢] [۷۰] [۷٤]	۱۲
	افزایش مهارت، تجربه، آگاهی و آموزش کاربران در زمینه امنیت اطلاعات	[۱] [۲] [٤] [٦] [۱۲۱] [۱۵] [۲۳] [۳۸] [٤٤] [۵۲] [٦١] [٦٢] [۷۵]	۱۳
	درک نیازهای امنیتی در سطوح مختلف سازمان	[۵۲]	۱
	رفتار محافظه‌کارانه کاربران در زمینه امنیت سیستم-های اطلاعاتی	[٥٤] [٦٧]	۲
	پیروی از استانداردها و دستورالعمل‌های امنیتی	[٤٩] [۵۲] [۵۵] [٦١]	٤
	حس پاسخگویی، خودارزیابی و خودگزارش‌دهی	[۹] [۱۳] [۱۷] [٤٥] [۵۷] [۷٤]	٦
	تدوین و اجرای برنامه‌های آموزشی در حوزه امنیت اطلاعات (تکنیک‌های نفوذ، هک، اخلاقیات، قوانین و مقررات، ممیزی و ...)	[۱] [٤] [۹] [۱۵] [۱۸] [۲۰] [۲۲] [۲٦] [۳۳] [۳۵] [٤١] [٤٤] [٤٦] [٤٩] [۵۰] [۵۵] [۵۷] [۵۹] [٦٠] [٦٢] [٦٥] [٦٧] [٦٨] [۷۳] [۷٤] [۷٦]	۲٦

خانواده الزام	زیرگروه/ عنوان الزام (کُدهای استخراج‌شده)		مرجع	فراوانی
	تشویق کارمندان به گزارش مخاطرات و مشکلات امنیتی		[١٤] [٢٤] [٢٦]	٣
	تعیین مسئولیت‌های امنیتی در سطح سازمان و استقرار سازمان امنیتی		[١] [٦]	٢
	تعهد و وفاداری کارمندان به سازمان و ملاحظات امنیتی رایج		[٥] [٨] [١٨]	٣
	غربالگری و ارزیابی دوره‌ای کارمندان از منظر ملاحظات امنیت اطلاعات		[٥] [٩] [٦٠]	٣
	تعریف کاربری‌های مجاز سیستم و حقوق دسترسی		[١] [٥] [١١] [٧١]	٤
	حاکمیت فرهنگ همکاری در فعالیت‌ها و برنامه‌های امنیتی سازمان		[٦] [١٥] [٢٤] [٤٠] [٥٢] [٥٤] [٥٧] [٦٢]	٨
	نظارت و پایش مستمر فعالیت‌های طرف ثالث در حوزه امنیت اطلاعات		[٤٤] [٦٨]	٢
فنی	استفاده مؤثر از سازوکارهای احراز هویت	استفاده از کلمه‌های عبور قوی	[١] [١٨] [٢١] [٤١] [٤٧] [٤٩] [٥٤] [٦٢] [٦٧] [٦٩] [٧٦]	١١
		استفاده از کارت‌های هوشمند و توکن‌های امنیتی	[٢] [٣٥] [٤١] [٤٩] [٦٢] [٧٣]	٦
	استفاده مؤثر و کارا از سازوکار کنترل دسترسی	صدور مجوز و تفویض اختیار	[١٣] [٥٧] [٦٨] [٧٤]	٤
		دسترسی افراد بیرونی به داده‌های سیستم (از طریق VPNهای ایمن و کانال‌های ارتباطی امن)	[٤٠] [٦٨]	٢
		حفاظت از منابع در مقابل دسترسی و نفوذ فیزیکی (جایابی تجهیزات، پایش،کنترل تردد و ...)	[١٨] [٣٢] [٧٤]	٣
		محدود کردن دسترسی بسیاری از کاربران (به اینترنت، گزارش‌های جدید، کلمه عبور، رسانه‌های قابل حمل و ...)	[٣٢] [٦٥] [٦٩] [٧١]	٤

خانواده الزام	زیرگروه/ عنوان الزام (کُدهای استخراج‌شده)		مرجع	فراوانی
		مدیریت و تعیین خط‌مشی‌های حقوق دسترسی برای کاربران (تحلیل نقش، تعیین کاربری، تعیین محدودیت دسترسی به منابع، پیکربندی تجهیزات دسترسی)	[۱] [۲] [۵] [۱۱] [۱۳] [۱۵] [۱۷] [۱۸] [۲۱] [۲۳] [۲۶] [۳۴] [۴۱] [۴۵] [۴۹] [۵۲] [۵۵] [۵۷] [۶۰] [۶۵] [۶۸] [۶۹] [۷۱] [۷۳] [۷۴]	۲۵
		استفاده از سازوکار کنترل دسترسی منطقی (قفل‌گذاری فایل، مدیریت دسترسی به سیستم، کنترل دسترسی به شبکه، کنترل جابجایی رسانه‌ها و تجهیزات و ...)	[۱۰] [۲۶] [۳۲] [۶۵] [۷۳] [۷۴]	۶
		کنترل دسترسی طرف ثالث و پیمانکاران	[۴۴]	۱
	سازوکارهای امنیت ارتباطات	استفاده از سیستم‌های پایش و سامانه‌های جامع نظارتی	[۱] [۶] [۱۱] [۱۸] [۲۶] [۶۰] [۶۸]	۷
		به‌کارگیری پروتکل‌های امنیت اطلاعات/ ارتباطات امن	[۱۷] [۲۲] [۷۳]	۳
		استفاده از الگوریتم‌های رمزنگاری	[۱] [۲] [۵] [۹] [۲۱]	۵
		کابل‌کشی امن مابین سیستم‌ها/ تجهیزات (موقعیت، جلوگیری از شنود، مقاوم‌سازی و ...)	[۱] [۵۵]	۲
		کنترل و کُدگذاری رسانه‌های قابل حمل	[۶۰] [۶۵] [۷۴]	۳
		محرمانگی (امنیت اطلاعات)	[۲] [۴] [۱۰]	۳
		مدیریت ارتباطات در برون-سپاری خدمات امنیتی	[۷۴]	۱
		مدیریت تجهیزات و رسانه‌های ارتباطی (لینک ارتباطی، سرورها، ایستگاه‌های کاری، سوئیچ‌ها، روترها و ...)	[۱۸] [۲۰] [۳۲] [۶۵] [۶۹]	۵

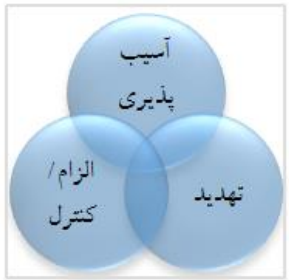
خانواده الزام	زیرگروه/ عنوان الزام (کُدهای استخراج‌شده)		مرجع	فراوانی
		گمنام‌سازی داده‌ها و لینک‌های ارتباطی	[۲۱]	۱
	سازوکارهای امنیت اطلاعات و سامانه‌ها	استفاده از پویشگرها و سیستم-های تشخیص نفوذ و سامانه-های ضد بدافزار (آنتی‌ویروس، IPS، IDS)	[۱] [۱۰] [۱۲] [۱٤] [۱٥] [۱۸] [۲٤] [۲٦] [۳۲] [٤٥] [٤٦] [٤۷] [٤۹] [٦۲] [٦۸] [۷۱] [۷٤] [۷٦]	۱۸
		استفاده از دیواره آتش و سازوکار یکپارچه مدیریت تهدیدات (UTM)	[۱۸] [۲۲] [۲٤] [۲٥] [۲٦] [۲۷] [۳۲] [٤۱] [٤٥] [٤۷] [٤۹] [٥٥] [٥۹] [٦۲] [٦٥] [٦۷] [٦۸] [۷۰] [۷٤] [۷٦]	۲۰
		مدیریت، انتقال و نگهداری امن داده‌ها	[۳] [٤] [٥۱]	۳
		صیانت از صحت و یکپارچگی داده‌ها	[۱۷] [٤٤] [٦۱] [۷۱] [۷۳]	٥
		امضاهای دیجیتالی	[۱۷] [۲۱] [۲۳] [۲٥] [٤۹] [۷۰] [۷٤]	۷
		فناوری نهان‌نگاری	[٤٦]	۱
	سازوکار پاسخگویی و عدم انکار	سازوکار پالایش محتوا (شبکه، پست الکترونیکی و ...)	[۱۲] [۲۲] [۳۸]	۳
		سازوکارهای پایش عملیات	[۱۲]	۱
		بازرسی سیستم‌های اطلاعاتی/ تجهیزات	[۱] [٦]	۲
		ممیزی امنیت اطلاعات (سیستم‌ها، روال‌ها، محتوا و عوامل انسانی)	[۱۸] [۲۱] [۲٦] [۳۲] [۳٤] [٤۱] [٤٤] [٤۹] [٥٥] [٦٥] [۷۱] [۷۳]	۱۲
	سازوکار امنیت فیزیکی/ محیطی	مدیریت انرژی (پشتیبان برق و مدیریت شرایط اضطراری)	[۱] [۱۱] [۷٤]	۳
		سامانه‌های اطفاء حریق و اعلام هشدار حرارتی	[۱۱]	۱

خانواده الزام	زیرگروه/ عنوان الزام (کُدهای استخراج‌شده)		مرجع	فراوانی
		سازوکارهای مقابله با زلزله (مقاوم‌سازی، جایابی و ...)	[۷٤]	۱
		ایمن‌سازی فیزیکی دستگاه‌های الکترونیکی شخصی/ سامانه-های اطلاعاتی و زیرساخت‌های فنی	[۱] [۵] [۱۱] [۲٦] [۳٤] [٦۵]	٦
		ایمن‌سازی اماکن و فضاهای حساس (اتاق سرور و ...)	[۱] [۱۱] [۱۸]	۳
		استانداردها و سازوکارهای کنترل دما و رطوبت	[۱]	۱
	سازوکار پشتیبان-گیری و دسترس‌پذیری	استفاده از دارایی‌ها و تجهیزات اضافی	[۲٦]	۱
		پشتیبان‌گیری منظم از سیستم‌ها	[۱۷] [٤۷] [۵٤]	۳
		افزایش ظرفیت حافظه	[۳۰]	۱
فرآیندی/ رویه‌ای	استفاده از چک‌لیست‌های امنیتی		[۵۵] [٦۲]	۲
	تدوین قوانین، خط‌مشی‌ها، دستورالعمل‌ها و الزامات امنیت سیستم‌های اطلاعاتی در سازمان		[۱] [۲] [٤] [٦] [۱۱] [۱۳] [۱۸] [۲۰] [۲۳] [۲٤] [۲۵] [۳٤] [٤۰] [٤۱] [٤٤] [٤۹] [۵۲] [٦۲] [٦۸] [٦۹] [۷۳] [۷٤] [۷٦]	۲۳
	عضویت و تعامل با انجمن‌های حرفه‌ای و تخصصی امنیت اطلاعات		[٤۰]	۱
	تعیین جریمه برای عدم پیروی از خط‌مشی‌های امنیتی		[۵۷]	۱
	تعیین راهبردها و اهداف مدیریتی بر اساس شرایط حاکم بر سازمان		[۱۲]	۱
	برنامه‌ریزی، تحلیل پیامد و بودجه‌بندی امنیتی در سازمان		[۱] [۹] [٤۹]	۳
	سازمان‌دهی سایت‌های مشکوک توسط کاربران/		[۲۸] [۳۸] [٦۸]	۳

خانواده الزام	زیرگروه/ عنوان الزام (کُدهای استخراج‌شده)	مرجع	فراوانی
	اپراتورها (تهیه لیست‌های سیاه و خاکستری)		
	تدوین اصول و روال‌های پایش و کنترل کارمند/ فعالیت‌ها	[٤] [٥٠] [٦٨]	۳
	ارزیابی و به‌روزرسانی منظم قوانین، خط‌مشی‌ها، رویه‌ها و الزامات امنیتی	[١٥] [٥٢] [٦٥]	۳
	اصول و روش‌های جمع‌آوری، نظارت و تحلیل اطلاعات جهت مشکلات احتمالی امنیت	[١٥] [٥٢]	۲
	روش‌ها و دستورالعمل‌های بررسی صحت، محرمانگی و دسترس‌پذیری خدمات و سیستم‌ها	[٢] [١٧]	۲
	اصول طبقه‌بندی داده‌ها و منابع اطلاعاتی (بر مبنای سطح حساسیت)	[١٨] [٥١]	۲
	روش شناسایی و طبقه‌بندی دارایی‌ها و تعیین مالکان منابع اطلاعاتی و مسئول نگهداری و ذخیره‌سازی آن‌ها (مدیریت دارایی)	[٦] [٥١] [٦١]	۳
	طراحی معماری امن (برای دفاع در برابر حمله شبکه طعمه)	[٢٢]	۱
	برنامه‌ریزی آموزشی و آگاهی‌رسانی امنیتی	[١٢] [٢٣] [٤٣] [٥٢] [٧٦]	۵
	رویه‌های تشخیص، گزارش‌دهی و پاسخ به رخدادهای امنیتی	[٤] [٢٦] [٣٨] [٥٧] [٦٨] [٧٠] [٧٤]	۷
	تدوین استانداردهای امنیتی	[٩] [٣٤] [٥٢]	۳

چهارچوب پیشنهادی ایمن‌سازی سیستم‌های اطلاعاتی

چهارچوب پیشنهادی ایمن‌سازی سیستم‌های اطلاعاتی در مقاله حاضر بر اساس مدل مرجع معماری امنیت سایبری استاندارد X.805 مؤسسه ITU طراحی شده است. در این مدل، تأمین امنیت اطلاعات تحت تأثیر سه مؤلفه سازنده قرار دارد. این مؤلفه‌ها در قالب شکل (۲) ارائه شده است.



شکل ۲. مؤلفه‌های سازنده امنیت اطلاعات بر اساس ITU X.805

این معماری بر اساس دارایی اطلاعاتی بنا نهاده شده است که در تحقیق حاضر این محوریت با سیستم‌های اطلاعاتی است. این امر بدان معنا است که آسیب‌پذیری (ضعف امنیتی) در فضای طراحی، توسعه، پیاده‌سازی، بهره‌برداری یا مدیریت سیستم اطلاعاتی مطرح می‌شود. تهدید (عامل بروز تهدید) نیز با سوءاستفاده از آسیب‌پذیری موجود در دارایی –در قالب یک حادثه– به فِعلیت در می‌آید. علاوه بر این، الزام (کنترل یا حفاظ امنیتی) نیز برای مواجهه با تهدید یا رفع آسیب‌پذیری در سطح دارایی یا محیط فعالیت آن پیاده‌سازی و به‌کارگیری می‌شود.

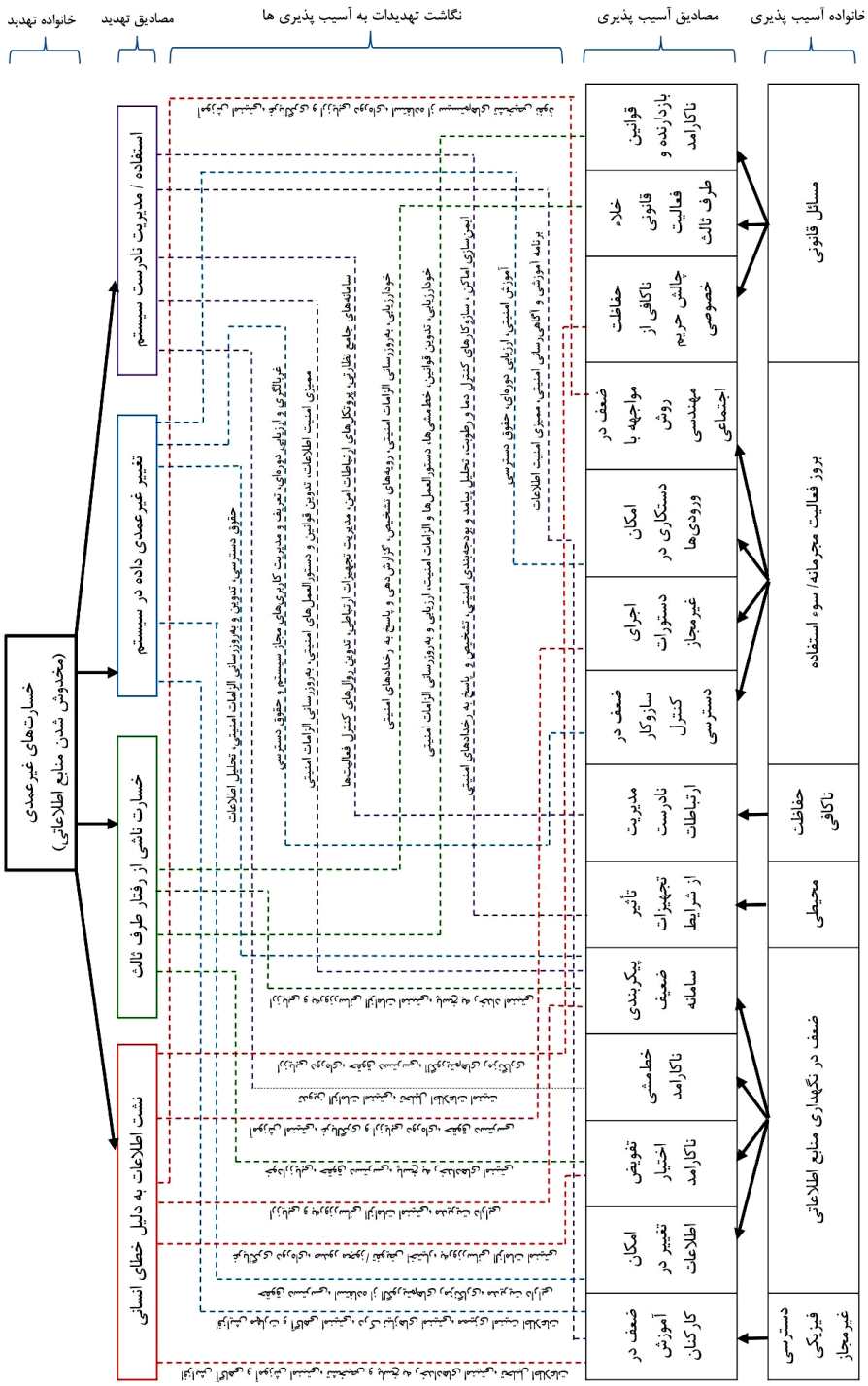
ارائه چهارچوب امن‌سازی سیستم‌های اطلاعاتی بر اساس معماری فوق مستلزم استفاده از یک ساختار سه‌بعدی است. این کار با به‌کارگیری یک شماتیک عملیاتی شده است. این شماتیک و مؤلفه‌های امنیتی به کار گرفته شده در آن در قالب شکل (۳) ارائه گردیده است. تدوین این چهارچوب بر اساس اصول زیر انجام شده است:

- تهدیدها و آسیب‌پذیری‌های امنیتی سیستم‌های اطلاعاتی در دو سطح در چهارچوب پیشنهادی ارائه شده‌اند. سطح دوم (سطح تفصیلی) دربرگیرنده مصادیق تهدیدها و آسیب‌پذیری‌ها است که به‌طور مستقیم از خروجی‌های روش فراترکیب و تحلیل مقاله‌های منتخب (مندرج در جدول‌های ۳ و ٤ و ٥) احصاء شده‌اند. سطح اول (سطح راهبردی چهارچوب) معرف خانواده یا گروه‌های تهدیدها و آسیب‌پذیری‌ها است که نام‌گذاری آن‌ها مبتنی بر نتایج روش تحلیل تِم و تأیید پنل خبرگان امنیتی انجام شده است.

- الزامات امنیتی سیستم‌های اطلاعاتی در داخل سلول‌های ماتریس چهارچوب پیشنهادی ارائه شده است. این الزام‌ها نیز در دو سطح تعریف شده‌اند. سطح دوم (سطح تفصیلی) دربرگیرنده مصادیق الزامات است که به‌طور مستقیم از خروجی‌های روش فراترکیب و تحلیل مقاله‌های منتخب شناسایی شده است. سطح اول (سطح راهبردی چهارچوب) معرف خانواده یا گروه‌های الزامات امنیتی است که نام‌گذاری آن‌ها مبتنی بر مدل‌های مرجع ارائه‌شده در استانداردها و بهترین تجربه‌های امنیتی انجام شده است.
- نگاشت تهدیدها به آسیب‌پذیری‌های امنیتی بر اساس رهنمودهای استانداردهای ITU X.805، سری ISO 27000، COSO و NIST FIPS-200 انجام شده است. این نگاشت معرف سلول‌هایی از مدل پیشنهادی است که با الزامات امنیتی پر شده است. درواقع بردار یک حمله (اینکه چه تهدیدی از چه آسیب‌پذیری‌هایی استفاده می‌نماید) از طریق سلول‌های پرشده در چهارچوب پیشنهادی مشخص خواهد شد.
- چیدمان الزامات امنیتی سیستم‌های اطلاعاتی در قالب چهارچوب پیشنهادی (نگاشت تهدید به آسیب‌پذیری به‌وسیله سلول‌های تکمیل‌شده) بر اساس رهنمودهای استانداردهای مرجع (ISO، NIST، BS و ITU) و تأیید یک پنل شش‌نفره از خبرگان امنیتی انجام شده است.

بر اساس موارد فوق یک برش کوچک اما واقعی از چهارچوب ایمن‌سازی سیستم‌های اطلاعاتی تدوین و در قالب شکل (۳) ارائه شده است. شایان ذکر است که سازمان‌دهی چهارچوب پیشنهادی - به‌واسطه محدودیت فضای چاپ- بر اساس مصادیق تهدیدات اولویت‌دار ذیل خسارت‌های غیرعمدی (مخدوش شدن منابع اطلاعاتی) انجام شده است. بر این اساس، بروز و ظهور هر یک از تهدیدات این حوزه (نشت اطلاعات به دلیل خطای انسانی، خسارت ناشی از رفتار طرف ثالث، تغییر غیرعمدی داده در سیستم و استفاده/ مدیریت نادرست سیستم) به‌واسطه وجود برخی

از ضعف‌ها و آسیب‌پذیری‌های امنیتی در این حوزه است. به‌عنوان مثال، نشت اطلاعات به دلیل خطای انسانی می‌تواند ناشی از پیکربندی ضعیف سامانه، اجرای دستورات غیرمجاز، ضعف در مواجه با روش‌های مهندسی اجتماعی و مواردی از این دست باشد. درک ارتباط تهدید با آسیب‌پذیری‌های امنیتی مستلزم نگاشت منطقی این موارد است که این امر در قالب چارچوب پیشنهادی به تصویر کشیده شده است. علاوه بر این، چگونگی مواجهه با هر تهدید یا رفع آسیب‌پذیری مربوطه جزء مواردی است که در قالب الزامات امنیتی به آن آدرس‌دهی شده است. در این راستا، الزامات امنیتی اولویت‌دار شناسایی‌شده از استانداردها و روش‌ها -که به تأیید پنل خبرگی رسیده است- در نگاشت هر تهدید نسبت به آسیب‌پذیری مربوطه مشخص و در قالب چارچوب پیشنهادی ارائه گردیده است. باید به این موضوع توجه داشت که چارچوب ارائه‌شده در قالب شکل (۳) تنها برش کوچکی از نقشه مفهومی بزرگ‌تر است که در قالب رساله دکترای مؤلف ارائه و اعتبارسنجی شده است. به‌هرحال، به‌واسطه محدودیت فضا و نیز گستردگی مصادیق تهدید، آسیب‌پذیری و الزامات امنیتی -که در قالب جداول ۳، ٤ و ۵ ارائه شده‌اند- در اینجا تنها به نگاشت یک خانواده از تهدیدات مهم به آسیب‌پذیری‌های امنیتی مربوطه و بیان الزامات امنیتی اولویت‌دار (و نه همه الزامات امنیتی قابل کاربرد) اشاره شده است.

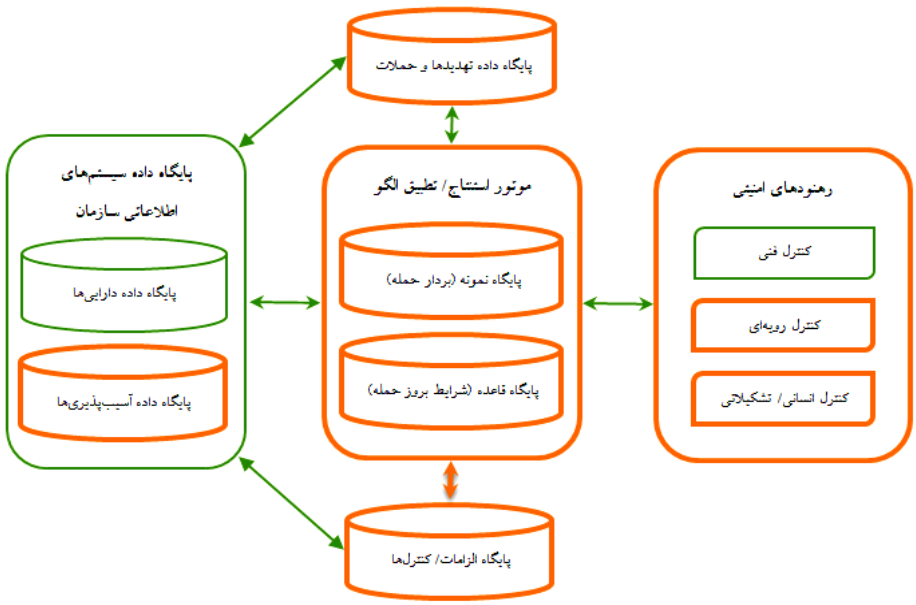


شکل ۳. چهارچوب پیشنهادی نمونه برای ایمن‌سازی سیستم‌های اطلاعاتی

کاربردپذیری چهارچوب ایمن‌سازی پیشنهادی

نکته بسیار مهم در پیشنهاد چهارچوب ایمن‌سازی سیستم‌های اطلاعاتی امکان به‌کارگیری آن در امر پشتیبانی از تصمیمات متخصصین و مدیران امنیتی سازمان است. در این زمینه توجه به نکته‌های زیر الزامی است:

- چهارچوب ایمن‌سازی پیشنهادی بیانگر نوعی خط فکری برای تصمیم‌ساز/ سیاست‌گذار است.
- چهارچوب ایمن‌سازی پیشنهادی بر اساس مفاهیم و مضامین بردار حمله (نگاشت تهدید به آسیب‌پذیری امنیتی موجود در سیستم) طراحی شده است.
- اعتبار الزامات امنیتی چهارچوب ایمن‌سازی پیشنهادی به‌واسطه آدرس‌دهی مستقیم به تهدیدات و آسیب‌پذیری‌های حول سیستم‌های اطلاعاتی است. بر این اساس، به‌کارگیری هر الزام صرفاً تحت تأثیر این موضوع است که آیا امکان مواجه با تهدید یا رفع آسیب‌پذیری مربوطه را دارد یا خیر؟



شکل ٤. معماری یک سیستم پشتیبان تصمیم امنیتی مبتنی بر چهارچوب ایمن‌سازی پیشنهادی

بر اساس مجموعه موارد فوق می‌توان معماری یک سیستم پشتیبان تصمیم امنیتی را ارائه نمود که ورودی‌های اصلی و خروجی‌ها و موارد قابل تحویل آن دربرگیرنده مؤلفه‌های سازنده چهارچوب پیشنهادی ایمن‌سازی سیستم‌های اطلاعاتی در تحقیق حاضر هستند. این معماری در قالب شکل (٤) به تصویر کشیده شده است.

ورودی این سیستم دربرگیرنده تهدیدات، آسیب‌پذیری‌ها و الزامات امنیتی مرتبط با سیستم‌های اطلاعاتی است. مبنای نگاشت سیستم‌های اطلاعاتی، تهدیدات و آسیب‌پذیری‌های امنیتی استفاده از سیستم تطبیق الگو – مبتنی بر پایگاه نمونه‌بردار حمله یا پایگاه قواعد شرایط بروز حمله– است. بر این اساس یک نمونه کاربرد (Use Case) انتخاب می‌شود که دربرگیرنده یک سیستم اطلاعاتی، تهدیدهای امنیتی رایج پیرامون آن و آسیب‌پذیری‌هایی است که هر تهدید/ عامل تهدید از آن‌ها سوءاستفاده می‌نماید. در نهایت این سیستم پشتیبان است که بر اساس پایگاه قواعد خود ارائه‌گر مجموعه‌ای از کنترل‌های فنی، رویه‌ای و انسانی – برای مواجهه با تهدیدات یا رفع آسیب‌پذیری‌های تعیین‌شده– است.

نتیجه‌گیری

موضوع طرح چهارچوب ایمن‌سازی سیستم‌های اطلاعاتی

عدم توجه به جنبه‌ها و لایه‌های مختلف امنیتی در حفاظت از سیستم‌های اطلاعاتی در سازمان‌ها نه‌تنها چهارچوب‌ها و سازوکارهای امن‌سازی به کار گرفته شده را ناکارآمد می‌نماید بلکه اثربخشی سرمایه‌گذاری در این حوزه را زیر سؤال خواهد برد. این امر لزوم به‌کارگیری یک چهارچوب جامع و مانع برای ایمن‌سازی سیستم‌های اطلاعاتی که تمامی این دغدغه‌ها را به شکلی صحیح آدرس‌دهی نماید نمایان می‌سازد.

درک ملاحظات امنیتی حاکم بر سیستم‌های اطلاعاتی سازمان بر اساس مطالعات کیفی

عامل‌های تهدید از انواع آسیب‌پذیری‌های موجود در حوزه‌های فناورانه، فرآیندی و انسانی برای سوءاستفاده از سیستم‌های اطلاعاتی استفاده می‌نماید. ازاین‌رو باید ضمن

در نظر داشتن تمامی جنبه‌ها به فکر مواجهه با تهدید یا رفع آسیب‌پذیری بود تا جلوی بروز خسارت‌های احتمالی گرفته شود. در بررسی‌های انجام‌شده مشخص گردید که بیشترین فراوانی در زمینه تهدیدات مربوط به فعالیت‌های مجرمانه/ سوءاستفاده بوده است. در بین فعالیت‌های مجرمانه این اجرا (تزریق) کُد/ نرم‌افزار/ فعالیت مخرب است که بیشترین فراوانی را به خود اختصاص داده است و کمترین فراوانی مربوط به چالش‌های انسانی می‌باشد. در زمینه آسیب‌پذیری‌ها نیز بیشترین فراوانی مربوط به بروز فعالیت مجرمانه/ سوءاستفاده است. در این فضا بیشترین سهم مربوط به فعالیت‌های مخرب کارکنان داخلی می‌باشد که جای تأمل جدی دارد. البته کمترین فراوانی نیز به ضعف در کنترل شکست/ خرابی مربوط می‌شود. در زمینه الزامات امنیتی بیشترین فراوانی مربوط به الزامات فنی و کمترین فراوانی مربوط به رویه‌ها و دستورالعمل‌های امنیتی می‌باشد. از بین الزامات انسانی نیز بیشترین فراوانی، مربوط به تدوین و اجرای برنامه‌های آموزشی در حوزه امنیت اطلاعات (تکنیک‌های نفوذ، هک، اخلاقیات، خط‌مشی‌های امنیتی، قوانین و مقررات، آموزش ممیزان و ...) و کمترین فراوانی مربوط به درک نیازهای امنیتی در سطوح مختلف سازمان است. در بین الزامات فنی بیشترین فراوانی مربوط به سازوکارهای امنیت اطلاعات و سامانه‌ها و کمترین فراوانی مربوط به سازوکارهای پشتیبان‌گیری و دسترس‌پذیری می‌باشد که در مورد دوم، دلیل شناخته‌شده بودن، فضا و الزامات است. در بین الزامات فرآیندی نیز بیشترین فراوانی مربوط به تدوین قوانین، خط‌مشی‌ها، دستورالعمل‌ها و الزامات امنیت سیستم‌های اطلاعاتی در سازمان و کمترین فراوانی مربوط به تعیین راهبردها و اهداف مدیریتی بر اساس اصول و شرایط حاکم بر سازمان؛ عضویت و تعامل با انجمن‌های حرفه‌ای و تخصصی در زمینه امنیت اطلاعات؛ تعیین جریمه برای عدم پیروی از خط‌مشی‌های امنیتی و طراحی معماری امن (برای دفاع در برابر حمله شبکه طعمه) است.

باید به این موضوع توجه داشت که چنین تحلیل و ارزش‌گذاری‌ای تنها بر اساس بررسی مطالعات کیفی تحقیقات منتشرشده انجام شده است. این در حالی است که

امنیت و شرایط و الزامات حاکم بر آن می‌تواند از یک نمونه به نمونه دیگر دستخوش تغییر شود.

یافته‌های تحقیق و بسط آن در قالب چهارچوب پیشنهادی

در طی سال‌های گذشته تحقیقات متعددی در زمینه ایمن‌سازی سیستم‌های اطلاعاتی سازمان انجام شده است. برخی از آن‌ها بر تهدیدها، تعدادی بر آسیب‌پذیری‌ها و برخی بر الزامات و شرایط مواجهه تمرکز داشته‌اند. البته تحقیقاتی بودند که بر هر سه مورد در نمونه‌ای خاص و به‌صورت موردی تمرکز نموده‌اند. این شرایط لزوم تدوین چهارچوب امنیتی جامع در این حوزه را بیش از بیش نمایان می‌سازد. البته نحوه تدوین چهارچوب به‌صورت جامع و مانع و شکل‌دهی آن در قالبی که امکان به‌کارگیری آن جهت ایمن‌سازی سیستم‌های اطلاعاتی وجود داشته باشد از دغدغه‌های اصلی محقق بوده است. برای تأمین جامعیت چهارچوب از روش فراترکیب و بررسی جامع مطالعات کیفی استفاده شده است. این در حالی است که برای تأمین مانعیت چهارچوب از مدل‌های مرجع امنیتی و نظرات خبرگان امنیتی استفاده شده است. جمع‌بندی تهدیدات، آسیب‌پذیری‌ها و الزامات امنیتی سیستم‌های اطلاعاتی در قالب چهارچوب پیشنهادی نیز بر اساس نگاشت تهدید به آسیب‌پذیری و تعریف الزام امنیتی مربوطه مبتنی بر همین نگاشت است. درواقع، متخصص یا سیاست‌گذار امنیتی بر اساس اینکه یک عامل تهدید برای انجام یک حمله از چه آسیب‌پذیری‌هایی سوءاستفاده می‌نماید، می‌تواند الزام مربوطه را به کار گیرد. ازاین‌رو چهارچوب ایمن‌سازی پیشنهادی می‌تواند به‌عنوان یک ساختار پشتیبان تصمیم برای متخصصین یا مدیران امنیتی عمل نماید.

فهرست منابع ومآخذ

الف. منابع فارسی

- اسماعیل‌پور، حمیدرضا، (۱۳۸۸)، شناسایی و رتبه‌بندی عوامل و شاخص‌های کلیدی مؤثر بر بهبود سیستم مدیریت امنیت اطلاعات، پایان‌نامه کارشناسی ارشد رشته مدیریت فناوری اطلاعات، دانشگاه شهید بهشتی.
- تقوا، محمدرضا و ایزدی، ماندانا، (۱۳۹۲)، بررسی امنیت در سیستم‌های اطلاعاتی توسعه‌یافته با روش معماری سرویس‌گرا (SOA)، مدیریت فناوری اطلاعات، دوره ۵، شماره ۳، ۴۲-۲۵.
- جعفری‌نژاد، نوید؛ مقبل باعرض، عباس و آذر، عادل، (۱۳۹۳)، شناسایی و استخراج مؤلفه‌های اصلی مدیریت ریسک سازمان با استفاده از روش فراترکیب، چشم‌انداز مدیریت صنعتی، شماره ۱۵، ۸۵-۱۰۷.
- حسن‌زاده، محمد؛ کریم‌زادگان‌مقدم، داوود و جهانگیری، نرگس، (۱۳۹۱)، ارائه یک چهارچوب مفهومی برای ارزیابی پرمایگی و آموزش آگاهی از امنیت اطلاعات کاربران، فصلنامه نظام‌ها و خدمات اطلاعاتی، سال اول، شماره ۲، ۱۶-۱.
- خاک‌بیز، مسلم، (۱۳۹۵)، شناسایی و اولویت‌بندی عوامل مؤثر بر امنیت سیستم‌های اطلاعاتی سازمان با استفاده از مدل‌های تصمیم‌گیری چندشاخصه، پایان‌نامه کارشناسی ارشد- دانشگاه یزد.
- خضری‌پور، فاطمه، (۱۳۹۲)، ارائه یک مدل برای بهبود مدیریت امنیت دارایی‌های اطلاعاتی سازمان در سیستم مدیریت امنیت اطلاعات ادارات دولتی شهر کرمان، پایان‌نامه کارشناسی ارشد رشته مدیریت فناوری اطلاعات، دانشگاه پیام نور تهران.
- خنیفر، حسین؛ میرزایی، نقی؛ پریشانی، علی و پوربهروزان، علی، (۱۳۹۷)، آسیب‌شناسی پژوهش‌های داخلی در زمینه مسئولیت‌پذیری اجتماعی با رویکرد فراترکیب، فصلنامه علمی- پژوهشی مدیریت سازمان‌های دولتی، دوره ۶، شماره ۳، ۸۳-۹۸.
- سلکایند، نیل جی، (۱۳۸۵)، کاربرد آمار و spss در پژوهش‌های علوم انسانی، ترجمه خلیل میرزایی و علی بقایی سرابی. تهران، انتشارات حفیظ.
- سیف، یاسر؛ نادری بنی، ناهید، (۱۳۹۶)، شناسایی مؤلفه‌های مؤثر بر مدیریت امنیت اطلاعات در فناوری اطلاعات شرکت نفت قاره ایران، مدیریت فناوری اطلاعات، دانشکده مدیریت دانشگاه تهران، دوره ۹، شماره ۴، ۸۷۰-۸۵۱.
- علی‌محمد ملایری، عصمت؛ باجلان، سعید و علی‌محمد ملایری، نیره، (۱۳۹۱)، ارائه روشی مبتنی بر معیار به‌طور کمّی و هفت‌بعدی جهت ارزیابی ریسک امنیتی در بستر سیستم‌های اطلاعاتی، اولین همایش ملی فناوری اطلاعات و شبکه‌های کامپیوتری دانشگاه پیام نور.
- مهرآیین، اسماعیل؛ آیت‌اللهی، هاله و احمدی، مریم، (۱۳۹۲)، وضعیت امنیت اطلاعات در سیستم‌های اطلاعات بیمارستانی، مدیریت اطلاعات سلامت، دوره ۱۰، شماره ۶، ۷۷۹-۷۸۸.

ب. منابع انگلیسی

- Abraham, Sherly & Chengalur-Smith, InduShobha. (2010). An Overview of Social Egineering Malware: Trends, Tactics and Implications. Sciencedirect, Technology in Society 32, 183-196.
- Abomhara, Mohamed & Koien, Geric M. (2015). Cyber Security and The Internet of Things (IoT): Vulnerabilities, Threats, Intruders and Attacks. Journal of Cyber Security, Vol.4, 65-88.
- Alavi, Reza & Islam, Shareeful. (2016). An Information Security Risk-Driven Investment Model for Analysing Human Factors. Emeraldinsight, Information and Computer Security, 24(2), 205-227.
- Albrechtsen, Eirik. (2014). Major Accident Prevention and Management of Information Systems Security in Technology-Based Work Processes, Journal of Loss Preventation in The Process Industries.
- Alghazzawi, Daniyal M., Hasan, Syed Hamid, Trigui, Mohamed Salim. (2014). Information Systems Threats and Vulnerabilities. International Journal of Computer Applications, 89(3), 25-29.
- Alotaibi, Youseef & Liu, Fei. (2012). How to Model a Aeure Information System: A Case Study, Internationa Journal of Information and Education Technology, Vol.2, No.2, 94-102.
- Awodele, Oludele, Enyinnaya Onuiri, Ernest & Okolie, Samuel O. (2012). Vulnerabilities in Network Infrastructures and Prevention/ Containment Measures.Proceedings of Information Science & IT Education Conference (InSITE).
- Blanco, Carlos, Rosado, David G., Enrique Sanchez, Luis & Jurjens, Jan. (2014). Security in Information System: Advances and New Challenges. Journal of Computer Standards & Interfaces, 36(4), 687-688.
- Boiko, Andrii & Shendryk, Vira. (2017). System Integration and Security of Information Systems. Sciencedirect, Procedia Computer Science 104, 35-42.
- Carneiro Cavalcante, Rodolfo, Bittencourt, Ig Ibert, Silva, Alan Pedro da, Silva, Marlos, Costa, Evandro & Santos, Roberio. (2012). A Survey of Security in Multi-Agent Systems. Sciencedirect, Expert Systems with Applications 39, 4835-4846.
- Crossler, Robert E., Belanger, France & Ormond, Dustin. (2017). The Quest for Complete Security: An Emprical Analysis of Users' Multi-Layered Protection From Security Threats. Springer, InfSyst Front.
- Chaudhry, Peggy E., Chaudhry, Sohail S., Clark, Kevin D. & Jones, Darryl S. (2013). Enterprise Information Systems Security: A Case Study in The Banking Sector. International Federation for Information Processing, LNBIP 139, 206-214.
- Cheng, Lijiao, Li, Ying, Li, Wenli, Holm, Eric & Zhai, Qingguo. (2013). Understanding the Violation of IS Security Policy in Organizations: An Integrated Model Based on Social Control and Deterrence Theory. Sciencedirect, Computers & Security 39, 447-459.
- Chou, Te-Shun. (2013). Security Threats on Cloud Computing Vulnerabilities. International Journal of Computer Science & Information Technology (IJCSIT).

- Chuessler, Josef H. (2009). General Deterrence Theory: Assessing Information Systems Security Effectiveness in Large Versus Small Business University of North Texas, Theses.
- Cowan, Christian & Gaskins, Chris. (2011). Monitoring Physical Threats in The Data Center, Schneider Electric's Data Center Science Center.
- Dang, Khanh & Dang, Tri. (2013). A Survey on Security Visualization Techniques for Web Information Systems. Emeraldinsight, International Journal of Web Information Systems, 9(1), 6-31.
- Djemaiel, Yacine & Boudriga, Noureddine. (2014). Modeling and Assessing The Impact of Security Attacks on Enterprise Information Systems, Springer International Publishing Switzerland, LNBIP 183, 281-292.
- Djemaiel, Yacine & Boudriga, Noureddine. (2014). Modeling and Assessing The Impact of Security Attacks on Enterprise Information Systems, Springer International Publishing Switzerland, LNBIP 183, 281-292.
- Elahi, Golnaz, Yu, Eric & Zannone, Nicola. (2010). A Vulnerability-Centric Requirements Engineering Framework: Analyzing Security Attacks, Countermeasures and Requirements Based on Vulnerabilities. Springer, Requirements Eng (15), 41-62.
- ENISA Threat Taxonomy: A Tool for Structuring Threat Information, 2016.
- Fernandes, Diogo A.B., Soares, Liliana F.B., Gomes, Joao V., Freiro, Mario M. & Inacio, Pedro R.M. (2014). Security Issues in Cloud Environments: A Survey, International Journal Information Security 13: 113-170.
- Gamagedara Arachchilage, Nalin Asanak & Love, Steve. (2014). Security Awareness of Computer Users: A Phishing Threat Avoidance Perspective. Sciencedirect, Computers in Human Behavior 38, 304-312.
- Gebremedhin Kassa, Shemles, CISA & MSCS. (2016). Inforrmation Systems Security Audit: An Ontological Framework, ISACA Journal 5.
- Geric, Sandro & Hutinski, Zeljko. (2007). Information System Security Threats Classifications. Journal of Information and Organizational Sciences, 13(1).
- Guo, Ken H. (2013). Security-Related Behavior in Using Information Systems in The Workplace: A Review and Synthesis, Sciencedirect, Computers & Security32, 242-251.
- Hall, Jacqueline H., Sarkani, Shahram & Mazzuchi, Thomas A. (2011). Impacts of Organizational Capabilities in Information Security. Emeraldinsight, Information Management and Computer Security, 19 (3), 155-176.
- Hassanzadeh, Mohammad, Jahangiri, Narges & Brewster, Ben. (2014). A Conceptual Framework for Information Security Awareness, Assessment and Training. Elsevier, Emerging Trends in ICT Security, Chapter 6, 99-110.
- Hayale, Talal H. & Abu Khadra, Husam A. (2016). Investigating Perceived Security Threats of Computerized Accounting Information Systems: An Emprical Research. Emeraldinsight, Journal of Economic and Administrative Sciences 24(1), 41-67.
- Hu, Qing, Hart, Paul & Cooke, Donna. (2007). The Role of External and Internal Influences on Information Systems Security- A Neo-Institutional Perspective. Sciencedirect, Journal of Strategic Information Systems 16, 153-172

- Hutter, David. (2016). Physical Security and Why It Is Important, SANS Institute.
- Hsu, Carol, Lee, Jae-Nam, Straub, Detmar, W. (2012). Institutional Influences on Information Systems Security Innovations, Information systems Research, 23 (3).
- Ifiendo, Princley. (2014). Information Systems Security Policy Compliance: An Empirical Study of the Effects of Socialization, Influence and Cognition. Sciencedirect, Information & Management 51, 69-79.
- Information Security Breaches Survey, PWC & Infosecurity Europe, 2015.
- Jang-Jaccard, Julian & Nepal, Surya. (2014). A Survey of Emerging Threats in Cybersecurity. Sciencedirect, Journal of Computer and System Sciences 80, 973-993.
- Jansson, K. & Von Solms, R. (2014). Phishing for Phishing Awareness. Taylor & Francis, Behaviour & Information Technology 32:6, 584-593.
- Jianrong, Yao & Minxue, Wei (2014). A New Bionic Architecture of Information System Security Based on Data Envelopment Analysis. Internation Conference on Management of E-Commerce and E- Government,IEEE, 93-97.
- Jouinin, Mouna, Ben Arfa Rabai, Latifa & Ben Aissa, Anis. (2014). Classification of Security Threats in Information Systems. Sciencedirect, 5th International Conference on Ambient Systems Networks and Technologies, Procedia Computer Science 32, 489-496.
- Kim, Tai-hoon. (2011). A Study on Security Level Management Model for Information System. Thesis, University of Tasmania. [56] Josef H. Chuessler. (2009). General Deterrence Theory: Assessing Information Systems Security Effectiveness in Large Versus Small Business University of North Texas, Theses.
- Kraemer, Sara, Carayon, Pascale & Clem, John. (2009). Human and Organizational Factors in Computer and Information Seurity: Pathways to Vulnerabilities. Sciencedirect, Computers & Security 28, 509-520.
- Kozlovs, Dmitrijs & Kirikova, Marite. (2016). Auditing Security of Information Flows, Springer, LNBIP 261, 204-219.
- Mirembe, Drake Patrick. (2015). The Threat Nets Approach to Information System Security Risk Analysis, University of Groningen, Theses. [61] Lean-Ping Ong. (2015). Awareness of Information Security Risks: An Investigation of People Aspects (A Study in Malaysia), Southern Cross University, Theses.
- Meskell, P., Burke, E., Kropmans, T. J., Byrne, E., Setyonugroho, W. & Kennedy, K.M. (2015). Back to the future: An online OSCE Management Information System for nursing OSCEs. Nurse Education Today, 35 (11), 1091-1096.
- Meskell, P., Burke, E., Kropmans, T. J., Byrne, E., Setyonugroho, W. & Kennedy, K.M. (2015). Back to the future: An online OSCE Management Information System for nursing OSCEs. Nurse Education Today, 35 (11), 1091-1096.
- Ogutcu, Gizem, Testik, Ozlem Muge & Chouseinoglou, Oumout. (2015). Analysis of Personal Information Security Behavior and Awareness. Journal of Computers and Security.
- Ong, Lean-Ping. (2015). Awareness of Information Security Risks: An Investigation of People Aspects (A Study in Malaysia), Southern Cross University, Theses.

- Papp, Dorottya, Ma, Zhendong & Buttyan Levente. (2015). Embedded Systems Security: Threats, Vulnerabilities and Attack Taxonomy. Thirteenth Annual Conference on Privacy, Security and Trust (PST).
- Parsons, Kathryn Marie, Young, Elise, Butavicius, Marcus Antanas & McCormac, Agata. (2015). The Influence of Organizational Security Culture on Information Security Decision Makin g, Journal of Cognitive Engineering and Decision Making, Vol.9, No. 2, 117-129.
- Pathari, V., Sonar, R. (2012). Identifying Linkages Between Statements in Information Security Policy, Procedures and Controls. Information Management & Computer Security, 20(4), 264-280.
- Safianu, Omar, Twum, Frimpong & Hayfron-Acquah, J. B. (2016). Information System Security Threats and Vulnerabilities: Evaluating The Human Factor in Data Protection. International Journal of Computer Applications, Vol.143, No.5, 8-14.
- Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53, 2013.
- Sohrabi Safa, Nader, Solms, Rossouw von & Futcher, Lynn. (2016). Human Aspects of Information Security in Organizations. Journal of Computer Fraud & Security, 15-18.
- Soltanmohammadi, Saeed, Asadi, Saman & Ithnin, Norafida. (2013). Main Human Factors Affecting Information System Security. Interdisciplinary Journal of Contemporary Research in Business, Vol.5,No.7, 329-354.
- Sommestad, Tedor, Ekstedt, Mathias, Holm, Hannes & Afzal, Muhammad. (2011). Security Mistakes in Information System Deployment Projects. Emeraldinsight, Information Management & Computer Security, 19(2), 80-94.
- Suleiman, Husam, Alqassem, Israa, Diabat, Ali, Arnautovic, Edin & Svetinovic, Davor. (2015). Integrated Smart Grid Systems Security Threat Model. Sciencedirect, Information Systems 53, 147-160.
- Tan, Hakan. (2011). Information System Security of an Organization and an Application. Degree of Master of Science in Computer Engineering.
- Threat Landscape and Good Practice Guide for Internet Infrastructure, ENISA, 2015.
- Tintamusik, Yanarong. (2010). Examining the Relationship Between Organization Systems and Information Security Awareness, Proquest LLC.
- Trustwave Global Security Report, 2016.
- Trustwave Global Security Report, 2018.
- Tsai, Nancy & Xiong, Yan. (2016). An Investigation of the Information System Security Issues in Taiwan. International Journal Business Information Systems, Vol.21,No.3, 309- 320.
- Wang, Hua, Zhao, GuoHong, Shi, BoShan & Meng, XianJun. (2013). The Security Protection and Technology Analysis of Information System. Applied Mechanics and Materials, vol.263-266, 3130-3134.
- Wei, Liu, Yong-feng Cui & Ya, Li. (2015). Information Systems Security Assessment Based on System Dynamics. International Journal of Security and Its Applications, Vol.9, No.2, 73- 84.

- Wu, Xianping. (2009). Security Architecture For Sensitive Information Systems, Information Technology Monash University, Austrslia, Thesis.
- Yeh, Quey-Jen & Chang, Authur Jung-Ting. (2007). Threats and Countermeasures for Information System Security: A Cross-Industry Study. Sciencedirect, Information & Management 44, 480-491.
- Yun, B., Fengming, Z., Wanfang, C., Cong, N, Na, L & Xu, Z. (2012). Lifecycle Management Framework of Information Systems Security Architecture, International Conference on Information Management, Innovation Management and Industrial Engineering, IEEE, 292-295.
- Zafar, Humayun. (2013). Human Resource Information Systems: Information Security Concerns for Organizations. Sciencedirect, Human Resource Management Review 23, 105-113.
- Zainab, A.N., Ismail, R. (2013). Assessing the State of Library Information Systems Security. Journal of Librarianship and Information Science, 45(3), 232-247.
- Zimmer, L. (2006). Qualitative meta-synthesis: A question of dialoguing with texts. Journal of Advanced Nursing, 53(3), 311–318.
- David H Deans. (2018).Global ICT investment will hit $4 trillion in 2018 – with cloud and hybrid IT infrastructure driving it. Retrieved from https://www.cloudcomputing-news.net/news/2018/feb/20/worldwide-ict-investment-will-reach-4-trillion-in-2018/.
- Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019. (2018). Retrieved from https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019.
- Janine L. Spears & Henri, Barki. (2010). User Participation In Information Systems Security Risk Management, MIS Quarterly, 34(3).
- Mayer, Nicolas, Aubert, Jocelyn, Grandry, Eric, Feltus, Christophe, Goettelmann, Elio & Wieringa, Roel. (2019). An integrated conceptual model for information system security risk management supported by enterprise architecture management. Springer, Software & Systems Modelling, 18 (3), 2285-2312.