فصلنامهٔ پدافند غیرعامل و امنیت (پژوهشی)
سال دهم: شمارهٔ ۳۸- بهار ۱۴۰۱
صص: ۵ - ۳۰
تاریخ دریافت: ۱۴۰۰/۱۱/۷
تاریخ پذیرش: ۱۴۰۰/۱۲/۸

Quarterly of Passive Defense & Security
Vol.10, No.38,Spring 2022
P-P: 5 - 30

ارائه چارچوب امنیت سایبری هوشمند و یکپارچه مرکز داده سازمان در سطح ملی با رویکرد فراترکیب

احمدکاظمی[۱]
علی معینی[۲]
نورمحمدیعقوبی[۳]
حمیدرضایزدانی[٤]

چکیده:

افزایش تهدیدات سایبری بر علیه مراکز داده سازمانی و خدمات آنهاکه به عنوان مهمترین زیرساخت حیاتی سازمان محسوب می‌شوند امروزه از اهمیت زیادی برخوردار است. حضور و فعالیت بازیگران متعدد داخل و خارج سازمانی نظیر سامانه ها و خدمات امنیت داده های سازمانی و همچنین مراکز امنیت سایبری، اپراتورهای شبکه و مراجع نظارتی و کنترلی و ارتباط تنگاتنگ میان آنها، نیازمند مدیریت هوشمند و یکپارچه در مواجهه با تهدیدات پیش رو است. در این پژوهش بمنظور شناسایی مولفه‌های چارچوب امنیت سایبری هوشمند و یکپارچه مرکز داده با روش مرور نظام‌مند از طریق جستجو در پایگاه وب او ساینس و اسکپوس و مقالات داخلی تعداد ۱۸۳۱ سند استخراج شد که پس از بررسی‌های لازم ۶۳ مورد از آن‌ها به‌عنوان اسناد مرتبط شناسایی و با استفاده از روش فراترکیب، بررسی و کدگذاری شدند. در نهایت کدهای استخراج شده در ذ ۵ مقوله اصلی و ۲۳ مولفه، قرار گرفتند که مربوط به امنیت سایبری مرکز داده یعنی شناسایی، محافظت، تشخیص، پاسخ دادن و بازیابی بودند. برخی مولفه‌های شناسایی شده عبارتند از: مدیریت دارایی، محیط کسب‌وکار، حکمرانی، ارزیابی‌ریسک، کنترل‌دسترسی، آموزش‌و آگاهی، امنیت‌داده‌ها، پایش‌مستمرامنیت، فرآیندهای‌تشخیصی، برنامه‌ریزی‌پاسخگویی، ارتباطات، تحلیل و بررسی، کاهش‌اثرات، بهبودکارایی و برنامه‌ریزی بازیابی.

واژگان کلیدی: امنیت سایبری، توسعه چارچوب، فراترکیب، مرکز داده سازمانی، مدیریت‌یکپارچه و هوشمند.

۱. عضو هیات علمی دانشگاه سیستان و بلوچستان و دانشجوی دکتری مدیریت فناوری اطلاعات دانشگاه تهران، *ahmad.kazemi@ut.ac.ir*
۲. استاد و عضو هیات علمی دانشکده علوم مهندسی، دانشکدگان فنی، دانشگاه تهران، نویسنده مسئول *moeini@ut.ac.ir*
۳. استاد و عضو هیات علمی دانشکده اقتصاد، مدیریت و حسابداری دانشگاه سیستان و بلوچستان
٤. استادیار و عضو هیات علمی دانشکده مدیریت و حسابداری دانشکدگان فارابی دانشگاه تهران

جستارگشایی

در طی سال‌های اخیر استفاده از داده‌ها تاثیرگذاری بالایی در کسب‌وکارها دارد(*Alhassan, Sammon, & Daly, 2016*). با این‌حال این افزایش حجم داده‌ها مشکلاتی را در زمینه ذخیره داده‌ها، حفظ امنیت و حریم‌خصوصی ایجاد کرده است، با توجه به پیچیدگی‌های فرآیند گردآوری، ذخیره و تحلیل این حجم از داده، بهره‌مندی از آن‌ها نیازمند مدیریت مناسب است (*Benfeldt, Persson, & Madsen, 2019*) و لزوم امنیت مرکز تولید و نگهداری و خدمات داده به عنوان یک موضوع نوظهور در مدیریت سیستم‌های اطلاعاتی مطرح گردیده است.

وجود " مجموعه ای از محصولات و خدمات بهم‌متصل- چارچوب " می‌تواند با بهره‌گیری از سرویسها و خدمات سامانه‌های فناوری‌اطلاعات موجود در سازمان، باعث ایجاد مدیریت یکپارچه و هوشمند امنیت مرکزداده سازمان در فضای‌سایبر گردیده و با پایش، دسته‌بندی و رتبه‌بندی تهدیدات مراکز داده و پاسخگویی یکپارچه و هوشمند به آنها، موجب توسعه توانایی‌های مدیریتی و فنی سازمان و تضمین سطح امنیت بالاتر در برابر تهدیدات سایبری گردد. در چارچوب مورد نظر این پژوهش، تمرکز بر نقاط با حساسیت بسیار زیاد و مورد توجه تهدیدکنندگان و مهمترین بخش اطلاعاتی و ارتباطی یک سازمان یعنی مرکز داده آن می‌باشد.

از طرفی نقطه قوت این پژوهش، تمرکز بر مراکز داده های سازمانی است که تهدیدات سایبری، سرمایه های اطلاعاتی آنها را خدشه دار می ند و به عنوان تهدیدی جدی جهت تداوم کسب و کار سازمان شناخته می‌شوند. پژوهش حاضر با توجه به شکاف موجود در ادبیات، به دنبال ارائه چارچوبی یکپارچه و هوشمند برای امنیت‌سایبری مرکز داده است.

ایجاد و استمرار امنیت سایبری زیرساخت‌های اطلاعاتی و ارتباطی با محوریت «مراکز داده» نیازمند شناسایی و ارائه چارچوبی برای امنیت سایبری در ابعاد مختلف برای مواجهه فعال و خردمندانه در شرایط قبل از وقوع، در زمان وقوع و بعد از وقوع تهدیدات است. اهمیت اجرای این تحقیق و ارائه چارچوب امنیت سایبری یکپارچه و هوشمند مرکز داده سازمان بعنوان مهم‌ترین زیرساخت‌حیاتی با نگاهی ایجابی و با در نظرداشتن فواید و آثار ناشی از انجام آن بر اساس بررسی‌ها، نیازسنجی‌ها و همچنین پیش‌بینی محقق نشان‌دهنده موارد ذیل می‌باشد:

- شناخت و توسعه دانش و ادبیات این حوزه به منظور ارتقاء امنیت سایبری مراکز داده کشور
- شناسایی ابعاد و مفاهیم چارچوب امنیت سایبری مرکز داده سازمان
- شناخت مفاهیم و کدهای موجود در چارچوب امنیت سایبری هوشمند و یکپارچه مرکز داده به منظور مواجهه فعال با آنها در چارچوب زیست بوم

همچنین با در نظرداشتن آثار ناشی از عدم انجام تحقیق و با رویکرد سلبی ضرورت اجرای این تحقیق بر اساس بررسی‌های اولیه به شرح ذیل می‌باشد:

- ضعف در شناسایی ابعاد و مفاهیم چارچوب امنیت سایبری مرکز داده سازمان
- کاهش‌توانمندی در پاسخگویی به نیازهای امنیت سایبری مراکز داده سازمان
- افزایش میزان خسارات بدلیل نبود چارچوب امنیت سایبری هوشمند و یکپارچه مرکز داده
- اخذ موضع انفعالی در تصمیم‌سازی برای ایجاد و ارتقاء امنیت سایبری مراکز داده

رویکرد اصلی محقق در این مقاله، ارائه چارچوب امنیت سایبری یکپارچه و هوشمند مرکز داده سازمان در سطح ملی است.

مبانی نظری و مفاهیم:

رشد سریع و در عین حال نامتوازن شبکه‌ها در فضای سایبر، این بسـ را به یکی از حوزه‌های کارا و در عین حال بالقوه آسیب‌پذیر، تهدیدزا و خطرناک تبدیل نموده است. در حال حاضر، فضای سایبر بستری برای تبادلات تجاری و اقتصادی، فرهنگی و هنری، آموزشی و پژوهشی است. نامتعارف بودن ساختار این شبکه‌های به هم پیوسته، آسیب پذیری‌ها و در نتیجه تهدیدهای متنوعی را بدنبال دارد که باعث وقوع حوادث خطرناک با حوزه اثر زیاد و ایجاد ناامنی و چالش در زندگی شهروندی و تهدید برای امنیت ملی کشورها می‌شود. از این موضوع چنین برداشت می‌شود که زیست بومی به نام فضای سایبر– با حضور جدی در زندگی بشر– توانسته است سهم زیادی از توجه و وابستگی افکار را به خود اختصاص دهد. (سیاهکلی، ۱۳۹۴)

چارچوب امنیت سایبری:

مفهوم چارچوب برای دسته‌بندی و تبیین فرایند امنیت سایبری در سازمان به طور کلی شامل بخش‌هایی همچون فرهنگ امنیتی، فرایند عملیاتی، فناوری و محیط است. از طرفی می‌تواند شامل مجموعه رویکردهایی باشد که کارکردها، خوشه‌بندی‌ها و مراحل امنیت سایبری را در نظر بگیرد. در این تحقیق منظور از چارچوب، قالبی است که با ارائه آن زبان مشترک و توانمندی برای درک، مدیریت یکپارچه و هوشمند در پیش‌بینی و پیشگیری، محافظت، مقابله و مدیریت آثار تهدیدهای امنیتی سایبری مراکز داده بر اساس فرهنگ امنیتی، فرایند عملیاتی، فناوری و محیط ایجاد شود.

مدیریت یکپارچه‌وهوشمند:

مفهوم یکپارچگی‌و هوشمندی درمدیریت امنیت سایبری به معنای کاهش مخاطرات ناشی از حملات امنیتی سایبری به مرکز داده به صورت سیستماتیک با فرایندسازی هوشمند و واکنش سریع و مناسب به حملات سایبری بوده تا مفاهیمی نظیر تشخیص الگو، یادگیری و ایجاد پایگاه دانش در قالب یک ساختار متمرکز

و واحد ایجاد گردد. چشم انداز این یکپارچه‌سازی و هوشمندسازی ساختار امن و قوی جهت مقابله با حملات و اختلال در حوزه سایبری مراکز داده سازمانی خواهد بود.

امنیت:

واژه «امنیت[1]» در لغت‌نامه دهخدا، با معانی بی‌خوفی و امن و در فرهنگ معین، با معانی بی‌بیمی، ایمنی، ایمن‌شدن و در امان بودن معنا شده است. این واژه در فرهنگ وبستر، با عبارت «وضعیتی که از صدمه، محافظت یا ایمن شده باشد» و «چیزهایی که افراد یا مکان‌ها را ایمن می‌سازد» تعریف شده است. مفهوم امنیت، یک مفهوم توصیف‌گرانه است. بر این اساس، مفهوم امنیت را می‌توان متشکل از دو رکن صحت[2] و محرمانگی[3]دانست. امنیت سایبری برای موضوعاتی نظیر داده و اطلاعات، سامانه‌های اطلاعاتی، شبکه‌های ارتباطی، مراکز داده، سازمان‌های اطلاعات‌محور و ملی مطرح می‌باشد.

مرکز داده:

در پژوهشکده امنیت پژوهشگاه فناوری اطلاعات و ارتباطات (۱۳۹۴) مرکز داده معرف مکانی با سیستم‌های کامپیوتری و تجهیزات جانبی مربوطه مانند سیستم‌های ذخیره‌سازی و ارتباطی تعریف شده‌است (همان، ۱۳۹۴، ۱۲) و مرکزداده‌سازمانی مجموعه‌ای از سیستم‌های سخت زاری و نرم‌افزاری مستقر در تأسیسات کاملاً مجهز و پیشرفته با تعداد مناسب پرسنل مجرب و متخصص برای ارائه خدمات سازمان می‌باشد که دسترسی به آن از طریق شبکه‌های رایانه‌ای، شبکه خصوصی مجازی و خدمات کاربردی فناوری اطلاعات با در نظر داشتن الزامات مدیریتی و امنیتی بوجود می‌آید.

پیشینه پژوهش

در این بخش به طور مختصر به تحقیقات اخیر در مفهوم امنیت داده و مراکز نگهداری و خدمات آن، مراکز داده در سطح سازمان‌ها و کشورها می‌پردازیم.

حمید رضا مختاری و ناصر مدیری (۱۳۹۹) در تحقیق خود به ارزیابی امنیت پیکربندی سیستم‌های مدیریت یکپارچه تهدیدات سایبری پرداخته و مزیت‌های استفاده و پیکربندی امنیتی این سیستم‌ها را در مرکز داده بیان نموده ند (مختاری، مدیری، ۱۳۹۹).

محسن‌آقایی و همکاران (۱۳۹۸) در تحقیق خود به ساختار تهدیدات سایبری مرکز داده پرداخته و با معرفی انواع مرکز داده سازمانی و پس از بررسی، نسبت به ارائه ساختار تهدیدات سایبری مرکز داده در قالب ۹ بعد فناوری، منشاء، ماهیت، انگیزه، دامنه بروز، آثار و پیامدها، دامنه اثرگذاری، شیوه تحقق و آسیب‌پذیری و ۳۶ مولفه اقدام نموده اند (آقایی و همکاران، ۱۳۹۸).

رویا دسترنج و همکاران (۱۳۹۸) در تحقیق خود به ارزیابی اکوسیستم کلان داده در ایران پرداخته و با

1. *Security*
2. *Integrity*
3. *Confidentiality*

ارائه مدل هزاره به ارزیابی این فناوری اقدام و نتیجه‌گیری می‌کند ظهور فناوری های جدید و استفاده از راهکارهای جدید فناورانه در حوزه کلان داده باعث ارائه خدمات و عملکرد بهتر سازمانها می‌باشد (دسترنج و همکاران، ۱۳۹۸).

امیرحسین مقدسی لیچاهی و حمید همت (۱۳۹۷) در تحقیق خود به ارائه الگوی امنیت در فضای سایبر کشور پرداخته و با واکاوی درک اجتماع علمی از وضعیت فعلی فضای سایبر نسبت به ارائه مدلی برای ارتقای امنیت اقدام نموده اند. نتایج پژوهش حاکی از اهمیت فرهنگ سازی، توسعه زیرساختها، پدافند غیرعامل سایبری، امنیت فیزیکی و تدابیر فنی و مدیریتی مرکز داده در فضای سایبر کشور دارد (مقدسی لیچاهی، همت، ۱۳۹۷).

نیر سادات سید علی (۱۳۹۷) در تحقیق خود به شناسایی پارامترهای پیاده‌سازی انواع فناوریهای مجازی‌سازی در مراکز داده سازمانها پرداخته و پس از بررسی عوامل مؤثر بر استفاده از انواع فنآوری مجازی‌سازی در مرکز داده سازمان را هفت عامل کیفیت سیستم، کیفیت اطلاعات، تسهیل در مدیریت و نگهداری، کاهش‌هزینه، سهولت پیاده‌سازی، آزمایش و توسعه، ادغام‌منابع و اجماع سازمانی بیان می‌نماید (سید علی، ۱۳۹۷).

پژوهشگران پژوهشکده امنیت ارتباطات و فناوری اطلاعات (۱۳۹۵) در گزارشی به بررسی اجزاء مرکز داده پرداخته‌اند. براین‌اساس مرکز داده از چهار جزء فیزیکی، پردازشی و محاسباتی، ارتباطی و ذخیره‌سازی تشکیل شده‌است (قرایی، ۱۳۹۵، ۳۳).

محمد حسین زاده و محمدرضا حسنی آهنگر (۱۳۹۵) در تحقیق خود به اصول طراحی یک مدل امنیتی برای مرکز داده سازمان پرداخته و یک مدل امنیتی برای مرکز داده در سه سطح امنیت فیزیکی، امنیت ارتباطات و امنیت خدمات معرفی نموده و راهکارهایی جهت بهبود امنیت در سطوح مختلف ارائه گردیده است (حسین زاده، حسنی آهنگر، ۱۳۹۵).

اکسنچر (۲۰۱۹) در گزارش چشم‌انداز تهدیدات سایبری در سال ۲۰۱۹، پنج عامل مؤثر در امنیت سایبری، را تهدیدات ژئوپلیتیک، مجرمان سایبری، باج‌افزارها، گسیختگی زیست‌بوم و سرویسهای ابری بیان نموده است (اکسنچر ۲۰۱۹).

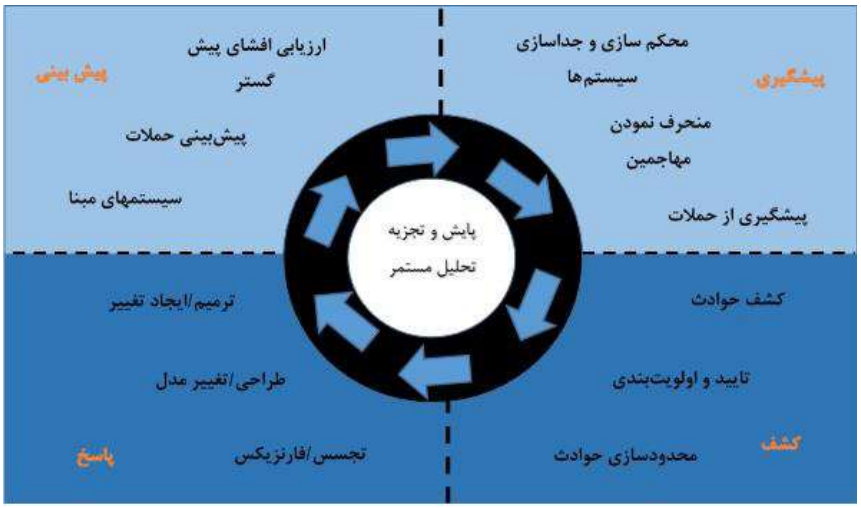
معرفی چارچوب های معماری امنیت سایبری

در دهه اخیر چارچوب‌ها و معماری‌های امنیت سایبری مختلفی معرفی گردیده است که ضمن معرفی مختصر آنها در جدول (۱)، جامع ترین و مهمترین آنها در ادامه بررسی می گردد.

جدول (۱) – معرفی چارچوب ها و معماری های امنیت سایبری ۱۰ سال اخیر (محقق)

معرفی	سال انتشار	توضیحات
TOGAF	۲۰۰۹	این چارچوب توسعه چهار حوزه معماری کسب و کار، داده، برنامه کاربردی و فناوری را ارائه میدهد.
Clark	۲۰۱۰	مدل چهارلایه‌ای فضای سایبر شامل لایه‌های انسانی، اطلاعاتی، منطقی و فیزیکی است در این مدل ضمن تفهیم نقاط کنترل فضای سایبر و اینترنت بر موضوع امنیت فضای سایبر تاکید شده است
مدل مرکز ملی فضای مجازی	۲۰۱۷	در این مدل ضمن ترسیم لایه‌های مهم فضای سایبر و اینترنت شامل زیرساخت، خدمات، محتوی، کاربر و حکمرانی، بر بعد امنیت فضای سایبر به عنوان لایه‌ای بسیار مهم تمرکز شده که کلیه لایه‌های دیگر را در بر گرفته است
Gartner	۲۰۱٤	چارچوب مشخصی را برای امنیت سایبری معرفی کرد که شامل چهار بخش پیش‌بینی، پیشگیری، کشف و پاسخ در یک فرایند مستمر پایش
NIST	۲۰۱۸	چارچوبی توسعه یافته برای شناسایی، کشف و پاسخگویی به حملات سایبری و دنبال رفع کمبود استانداردها در حوزه تأمین امنیت است.

موسسه گارتنر[1] در سال ۲۰۱۴ چارچوب زیر را برای امنیت سایبری معرفی کرد که شامل چهار بخش پیش‌بینی، پیشگیری، کشف و پاسخ در یک فرایند مستمر پایش بود.



شکل (۱) – چارچوب معماری امنیتی سازگار گارتنر

1. *Gartner's Adaptive Security Architecture.*

گارتنر تاکید دارد که به‌منظورایجاد امنیت سایبری لازم است رصد، پایش، تجزیه و تحلیل به صورت مداوم و مستمر صورت پذیرد (گارتنر ۲۰۱۴).

همچنین چارچوب امنیت سایبری NIST که با الگوگیری از مدل گارتنر و با توسعه آن در سال ۲۰۱۸ ارائه شده است مجموعه‌ای کلی از دستورالعمل‌ها برای شرکت‌های بخش خصوصی است که توسط مؤسسه ملی استاندارد و فناوری (NIST) ایالات متحده تهیه شده است، تا در شناسایی، کشف و پاسخگویی به حملات سایبری آمادگی بیشتری داشته باشند.

چارچوب امنیت سایبری NIST به دنبال رفع کمبود استانداردها در حوزه تأمین امنیت است. در حال حاضر سازمان‌ها شیوه‌های مختلفی از فناوری و قوانین را برای مبارزه با هکرها، سارقان داده و باج افزارها بکار می‌گیرند. حملات سایبری گسترده‌تر و پیچیده‌تر شده و مبارزه با این حملات نیز بسیار سخت‌تر شده است. این مسئله با فقدان یک استراتژی یکپارچه در بین سازمان‌ها همراه است و مجموعه‌های مختلف از سیاست‌ها، دستورالعمل‌ها، شیوه‌ها و فناوری‌های مورد استفاده در امنیت سایبری مشکل دیگری را ایجاد می‌کند و آن اینکه سازمان‌ها قادر به اشتراک گذاری اطلاعات در مورد حملات نیستند. (NIST, 2019).

شکل (۲) – چارچوب امنیت سایبری NIST

در این پژوهش با الگوگیری از چارچوب کلی امنیت سایبری NIST و ارائه چارچوبی ویژه برای تامین امنیت سایبری و حفاظت از زیر ساخت‌های اصلی بویژه مرکز داده سازمان در مقابل حملات سایبری اجتناب ناپذیر، کمک خواهیم کرد تا ضمن اتخاذ استراتژی یکپارچه، هوشمندی لازم با اشتراک اطلاعات و یادگیری از حملات قبلی در سازمانها جهت بهبود فرایند پاسخ و بازیابی ایجادگردد.

روش‌شناسی پژوهش

روش پژوهش مطالعه حاضر کیفی و از نوع فراترکیب است. در فراترکیب اطلاعات و یافته‌های استخراج

شده از مطالعات گذشته با موضوع مرتبط و مشابه بررسی می‌شوند. فراترکیب به واسطه رویکرد نظام‌مندی که در بررسی ادبیات ارائه می‌کند به پژوهشگران در کشف موضوع‌ها و استعاره‌های جدید کمک می‌کند (Zimmer, 2006).

در پژوهش حاضر به منظور بررسی ادبیات امنیت سایبری مرکز داده از مدل هفت مرحله‌ای ساندلوسکی[1] و باروسو[2] (کل ۳) استفاده شده است (Sandelowski & Barroso, 2006).

در مرحله اول سوال پژوهش تنظیم می‌گردد که عبارت است از: «چارچوب مناسب امنیت سایبری مرکز داده چه ابعاد و مؤلفه‌هایی دارد؟».

در مرحله دوم با استفاده از روش مرور نظام‌مند ادبیات[3]، اسناد معتبر و مرتبط به موضوع پژوهش شناسایی شدند. در پژوهش حاضر جستجو در پایگاه های وب او ساینس و اسکپوس و مقالات داخلی با استفاده از کلیدواژه‌های منتخب (*Cyber Security framework, Integrated and Intelligent Management, Organizational Data Center* و امنیت سایبری مرکز داده) انجام شد.

شکل (۳) – روند انجام روش فراترکیب

در مرحله سوم غربال اسناد حاصل از جستجو مقالات و منابع مرتبط، ابتدا به بررسی مرتبط بودن، تناسب عنوان، چکیده، محتوا و کیفیت روش با سؤال پژوهش و پالایش مجموعه مطالعات منتخب در چندین مرحله اقدام و سپس برخی منابع و مقالات از فرآیند بررسی و تحلیل فراترکیب جدا شدند. در نهایت ۶۳ سند به‌عنوان اسناد معتبر و منتخب برای تحلیل‌های بیشتر باقی ماندند که همه آن‌ها معتبر و مرتبط با موضوع پژوهش بودند.

1. *Sandelowski*
2. *Barroso*
3. *Systematic Literature Review*

در مرحله چهارم برای استخراج مفاهیم و کُدهای مرتبط با موضوع پژوهش به‌طور پیوسته مقالات منتخب جهت دستیابی به یافته‌های درون محتوا مرور شدند و با استفاده از روش کدگذاری سه مرحله ای کدها استخراج شدند.

در مرحله پنجم با توجه به هدف پژوهش، کدهای مرتبط شناسایی و استخراج گردیدند. سپس کدهای دارای ماهیت مشابه در ذیل یک دسته قرار گرفته و مفاهیم را تشکیل دادند و در ادامه نیز مفاهیم مشابه در ذیل یک مقوله قرار گرفتند.

در مرحله ششم ضرورت ایجاب می‌نماید که ترکیب اجزاء در قالب چارچوب نیز اعتبارسنجی شود. براین‌اساس اسناد منتخب در اختیار یک متخصص قرار داده شد و از وی درخواست شد که با توجه به هدف پژوهش و بدون اطلاع از نحوه ادغام کُدها و مفاهیم توسط پژوهشگر، کدگذاری کند.

جدول (۲) –پایایی روش فراترکیب

		نظر محقق		
		خیر	بله	مجموع
نظر خبره دیگر	بله	B=0	A= 3	3
	خیر	D=1	C=1	2
	مجموع	1	4	N=5

توافقات مشاهده شده = $(A+D)/N$= ۰/۸

در ادامه برای مقایسه کدهای احصا شده توسط محقق و یک نفر متخصص با استفاده از نرم افزار SPSS ضریب کاپا محاسبه گردید.

جدول (۳) – وضعیت شاخص کاپا (جنسن و آلن، ۱۹۹۶)

وضعیت توافق	وضعیت توافق	مقدار عددی شاخص	مقدار عددی شاخص
ضعیف	بی اهمیت	کمتر از ۰	۰-۰/۲۰
متوسط	مناسب	۰/۰-۲۱/۴۰	۰/۰-۴۱/۶۰
معتبر	عالی	۰/۰-۶۱/۸۰	۰/۱-۸۱

توافقات شانسی = $[(A+B)/N]*[(A+C)/N]*[(C+D)/N]*[(B+D)/N]$= 0384/0

K=(توافقات مشاهده شده – توافقات شانسی)/(توافقات شانسی -۱)= ۰/۷۳

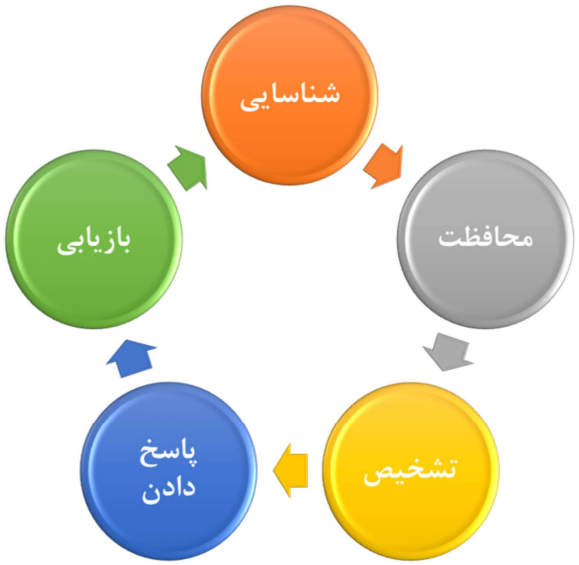
نتایج حاصل از محاسبه آزمون کاپا، ضریب کاپا را برابر ۰/۷۳ مشخص، که بیانگر توافق نسبتاً مناسبی است و علاوه بر این سطح معناداری کمتر از ۰/۰۵ نیز بیانگر ارتباط بین کدگذاری‌های صورت گرفته

بر روی سند منتخب است. نظر به اعتبار میزان بدست‌آمده عدد K براساس استاندارد اشاره‌شده در جدول (۳) موارد مستخرجه در قالب ابعاد و مؤلفه‌های چارچوب امنیت سایبری یکپارچه و هوشمند مرکز داده (جدول ۴) صحیح است.

یافته‌های پژوهش

چارچوب امنیت سایبری هوشمند و یکپارچه مرکز داده

با استناد به چارچوب امنیت سایبری NIST و براساس نتایج بررسی ادبیات و کدگذاری اسناد مقوله‌های چارچوب امنیت سایبری هوشمند و یکپارچه مرکز داده که یک چارچوب با پایش و نظارت مستمر می‌باشد بشکل زیر شناسایی شدند (شکل ۴).



شکل (۴) – چارچوب کلی امنیت سایبری مرکز داده سازمان

در چارچوب مشخص شده فوق امنیت سایبری مرکز داده سازمان در قالب یک چارچوب با فرایند مستمر و پویا بشکل یک چرخه اقدام ارائه گردیده است. در این حلقه هر مرحله که ما از آن بعنوان مقوله یاد می کنیم از مولفه‌هایی شکل گرفته است که از دسته‌بندی کدهای منتخب از منابع معتبر ذیل منتج شده است. همانطوریکه در جدول (۴) دیده می‌شود ابعاد چارچوب امنیت سایبری یکپارچه و هوشمند مرکز داده با بررسی منابع معتبر د ۵ مقوله اصلی مورد شناسایی قرار گرفتند که عبارتند از شناسایی، محافظت، تشخیص، پاسخ دادن و بازیابی.

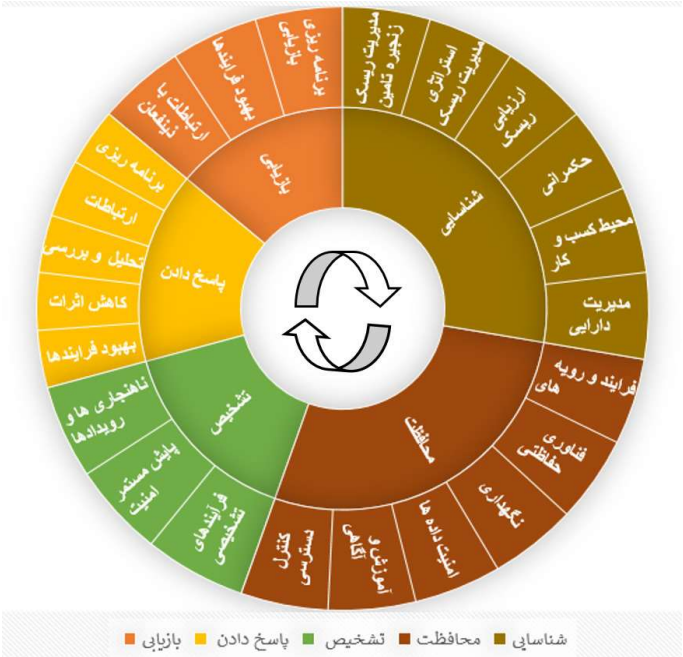
جدول (۴) – چارچوب امنیت سایبری هوشمند و یکپارچه مرکز داده

مقوله‌ها	مولفه‌ها	منبع
شناسایی	● مدیریت دارایی ● محیط کسب و کار ● حکمرانی ● ارزیابی ریسک ● استراتژی مدیریت ریسک ● مدیریت ریسک زنجیره تامین	CIS CSC COBIT 5 ISA 62443-2-1:2009 ISA 62443-3-3:2013 ISO/IEC 27001:2013 NIST SP 800-53 Rev. 4 *Baggott et al., 2020; Baig et al., 2019; Collier, 2018; Kim et al., 2019; Le et al., 2017; Lu et al., 2015; Panda et al., 2020; Pandey et al., 2020; Rowe et al., 2012; Srinivas et al., 2019; Svilicic et al., 2019; Tikk-Ringas, 2015; Bonina & Eaton, 2020; Calzada & Almirall, 2020; Jetzek, 2017; McBride et al., 2020; Micheli et al., 2020; Yoon & Copeland, 2020; Abraham et al., 2019; Lillie & Eybers, 2018; Oliveira et al., 2019; royalsociety, 2020; Attard et al., 2016; Diran et al., 2020; European Commission, 2020; Specht et al., 2015*
محافظت	● کنترل دسترسی ● آموزش و آگاهی ● امنیت داده ها ● نگهداری ● فناوری حفاظتی ● فرایند و رویه های ● حفاظت از اطلاعات	CIS CSC COBIT 5 ISA 62443-2-1:2009 ISA 62443-3-3:2013 ISO/IEC 27001:2013 NIST SP 800-53 Rev. 4 *Al-Muhtadi et al., 2020; Atoum et al., 2014; Georgiadou et al., ;2020; Hashim et al., 2016; Mendhurwar et al., 2019 Sani et al., 2019; Topal et al., 2020; Wei, 2010; Bonina & Eaton, 2020; Dawes et al., 2016; Diran et al., 2020; Janssen et al., 2020; McBride et al., 2020; Australian Government, 2020; royalsociety, 2020; Styrin et al., 2017; Gupta et al., 2020; Kampars et al., 2020; Kassen, 2017*

مقوله‌ها	مولفه‌ها	منبع
تشخیص	●ناهنجاری ها و رویدادها ●پایش مستمر امنیت ●فرآیندهای تشخیصی	CIS CSC COBIT 5 ISA 62443-2-1:2009 ISA 62443-3-3:2013 ISO/IEC 27001:2013 NIST SP 800-53 Rev. 4 Ashtiani et al., 2014; Bhardwaj et al., 2019; Evangelou et al., 2020; Otoom et al., 2013; Immonen et al., 2014; Janssen et al., 2020; Micheli et al., 2020; Oliveira et al., 2019; Styrin et al., 2017; Weber et al., 2009; Attard et al., 2016; Bonina & Eaton, 2020; Janssen et al., 2020
پاسخ دادن	●برنامه ریزی پاسخگویی ●ارتباطات با ذینفعان (هماهنگی پاسخ) ●تحلیل و بررسی ●کاهش اثرات ●بهبود فرایندهای پاسخگویی	CIS CSC COBIT 5 ISA 62443-2-1:2009 ISA 62443-3-3:2013 ISO/IEC 27001:2013 NIST SP 800-53 Rev. 4 ;Abraham et al., 2018; Ahmed et al., 2019; Atoum et al., 2016 ;Efthymiopoulos, 2019; Hahn et al., 2015; Khalid et al., 2018 Porcedda, 2018; Al-Badi et al., 2018; Dawes et al., 2016; Oliveira et al., 2019; Immonen & Kalaoja, 2019; Madaan et al., 2018; Mazumdar et al., 2019; Moreno et al., 2019
بازیابی	●برنامه ریزی بازیابی ●بهبود فرایندهای بازیابی ●ارتباطات با ذینفعان (هماهنگی بازیابی)	CIS CSC COBIT 5 ISA 62443-2-1:2009 ISA 62443-3-3:2013 ISO/IEC 27001:2013 NIST SP 800-53 Rev. 4 Hadji-Janev et al., 2017; Kapletia et al., 2014; Knight et al., 2020; Zhai L., Vamvoudakis, 2020; Alhassan et al., 2016; Jang & Kim, 2020; Janssen et al., 2020; Noorman, 2017; Oliveira et al., 2019; Lindman et al., 2015

همچنین ۲۳ مولفه شناسایی شده، که از تجمیع کدهای منتخب بدست آمده اند و پدید آورنده ابعاد چارچوب مورد نظر هستند عبارتند از: مدیریت دارایی، محیط کسب و کار، حکمرانی، ارزیابی ریسک، استراتژی مدیریت ریسک، مدیریت ریسک زنجیره تامین، کنترل دسترسی، آموزش و آگاهی، امنیت داده ها، نگهداری، فناوری حفاظتی، فرایند و رویه‌های‌حفاظت‌ازاطلاعات، ناهنجاری ها و رویدادها، پایش مستمر امنیت، فرآیندهای تشخیصی، برنامه ریزی پاسخگویی، ارتباطات با ذینفعان (هماهنگی پاسخ)، تحلیل و بررسی، کاهش اثرات، بهبود فرایندهای پاسخگویی، برنامه ریزی بازیابی، بهبود فرایندهای بازیابی، ارتباطات با ذینفعان (هماهنگی بازیابی).

کلیت چارچوب امنیت سایبری یکپارچه و هوشمند مرکز داده که دارای یک فرایند پویا و مستمر است در چرخه فوق به همراه مولفه های مرتبط ترسیم شده است (شکل ۵).



شکل (۵) – چارچوب امنیت سایبری هوشمند و یکپارچه مرکز داده سازمانی در کشور

مفهوم یکپارچگی‌و هوشمندی درمدیریت امنیت سایبری به معنای کاهش مخاطرات ناشی از حملات امنیتی سایبری به مرکز داده با مفاهیمی نظیر تشخیص الگو، یادگیری و ایجاد پایگاه دانش در قالب یک ساختار متمرکز و واحد ایجاد می گردد. چشم انداز این یکپارچه‌سازی و هوشمندسازی ساختار امن و قوی جهت مقابله با حملات و اختلال در حوزه سایبری مراکز داده سازمانی خواهد بود. با تامل در

فرایند طراحی چارچوب امنیت سایبری فوق در می‌یابیم انجام مستمر و پایش چرخشی آن هوشمندی لازم را جهت درس گرفتن از اقدامات قبلی خود و دیگران و جلوگیری از تکرار تهدیدات سایبری مراکز داده سازمان را فراهم می‌نماید. همچنین ایجاد یکپارچگی بواسطه ابعاد فوق که مانند حلقه‌های یک زنجیرهم پیوسته ترسیم شده‌اند ایجاد گردیده است. در ادامه به صورت مختصر توضیحات لازم در مورد برخی از مهمترین مولفه‌های مربوط به مقوله‌های چارچوب امنیت سایبری هوشمند و یکپارچه مرکز داده ارائه شده است.

شناسایی

همانطوریکه در شکل ۵ مشاهده می‌شود مقوله شناسایی کلیت مرکز داده و مولفه‌های امنیتی و تجهیزاتی آن دارای اهمیت بسیاری است و به صورت مختصر مهمترین مولفه‌های مربوط به آن شناسایی و ارائه شده است:

مدیریت دارایی: داده ها، تجهیزات، پرسنل فنی، دستگاه ها، سرویس‌دهنده‌ها و امکانات مرکز داده که سازمان را قادر می سازد با کمک آن به اهداف تجاری دست یابد، شناسایی شده و مطابق با اهمیت نسبی آنها در ارائه خدمات با استراتژی ریسک سازمان تطابق داده شود.

محیط کسب و کار: نقش داده‌ها و سرویسهای مرکز داده در مأموریت، اهداف، ذینفعان و فعالیتهای سازمان درک و اولویت بندی شود. این اطلاعات برای اطلاع از نقش ها، مسئولیت ها و تصمیمات مدیریت ریسک در امنیت سایبری استفاده می شود.

حکمرانی: سیاست ها، رویه ها و فرایندهای مدیریت و نظارت بر داده و الزامات نظارتی، حقوقی، ریسک محیطی و عملیاتی مرکز داده سازمان درک شده و مدیریت امنیت سایبری را آگاه می کند.

ارزیابی ریسک: سازمان خطر امنیت سایبری مرکز داده سازمانی، دارایی های داده سازمان و افراد مرتبط را درک می کند.

استراتژی مدیریت ریسک: اولویت های خدمات داده، محدودیت های دسترسی، تحمل ریسک و مفروضات مرکز داده سازمان تعیین شده و برای حمایت از تصمیمات ریسک عملیاتی مورد استفاده قرار می گیرد.

مدیریت ریسک زنجیره تامین: اولویت ها، محدودیت ها، تحمل ریسک ها و مفروضات مرکز داده تعیین شده و سازمان فرآیندهایی را برای شناسایی، ارزیابی و مدیریت ریسک های زنجیره تامین داده و پهنای باند جهت ارائه خدمات سازمان ایجاد و اجرا کرده است.

محافظت

همانطوریکه د شکل ۵ مشاهده می‌شود مقوله محافظت از دارایی‌های مرکز داده و مولفه‌های مدیریتی و

فنی آن دارای اهمیت بسیاری است و به صورت مختصر مهمترین مولفه‌های مربوط به آن ارائه شده است:
مدیریت هویت و کنترل دسترسی: دسترسی به دارایی های فیزیکی و منطقی مرکز داده و امکانات مربوط به کاربران مجاز، فرایندها و دستگاه ها است و مطابق با خطر ارزیابی شده دسترسی غیر مجاز به فعالیت ها و خدمات مجاز مدیریت می شود.
آگاهی و آموزش: به پرسنل مرتبط و شرکای سازمان آموزش آگاهی از امنیت سایبری، داده شده و آموزش دیده‌اند تا وظایف و مسئولیت های مربوط به امنیت سایبری مرکز داده خود را مطابق با سیاست ها، رویه ها و توافقنامه های مربوط انجام دهند.
امنیت داده ها: اطلاعات و سوابق (داده ها) مطابق با استراتژی خطر مرکز داده سازمان برای محافظت از محرمانه بودن، درستی و در دسترس بودن اطلاعات مدیریت می‌شوند.
فرایندها و رویه های حفاظت از اطلاعات: سیاست های امنیت سایبری مرکز داده (که هدف، محدوده، نقش ها، مسئولیت ها، تعهد مدیریت و هماهنگی بین نهادهای سازمانی را مورد بررسی قرار می دهد)، برای حفظ حفاظت از سیستم ها و دارایی های اطلاعات سازمان حفظ و مورد استفاده قرار می گیرد.
تعمیر و نگهداری: تعمیر و نگهداری تجهیزات مرکز داده و بروز نگه داشتن سامانه های اطلاعاتی و عملیاتی مطابق با خط مشی ها و رویه ها امنیت سایبری مرکز داده انجام می شود.
فناوری حفاظتی: راه های امنیتی فنی به منظور تضمین امنیت و انعطاف پذیری سیستم ها و دارایی ها مرکز داده، مطابق با سیاست ها، رویه ها و توافقنامه های مرتبط مدیریت می‌شوند.

تشخیص

همانطوریکه در شکل ۵ مشاهده می‌شود مقوله تشخیص رویدادهای مرکز داده و مولفه‌های امنیتی و تشخیصی آن دارای اهمیت بسیاری است و به صورت مختصر مهمترین مولفه‌های مربوط به آن ارائه شده است:
ناهنجاریها و رویدادها: فعالیتهای غیر عادی در مرکز داده شناسایی شده و تأثر احتمالی رویدادها درک می شود.
پایش مستمر امنیت: سیستم اطلاعات و دارایی ها مرکز داده سازمان برای شناسایی رویدادهای امنیت سایبری و تأیید اثربخشی اقدامات حفاظتی نظارت می شوند.
فرآیندهای تشخیصی: فرایندها و رویه های تشخیص برای اطمینان از آگاهی از رویدادهای ناهنجار در مرکز داده سازمان حفظ و آزمایش می شوند.

پاسخ دادن

همانطوریکه در شکل ۵ مشاهده می‌شود مقوله پاسخ دادن به تهدیدات در مرکز داده و مولفه‌های آن

دارای اهمیت بسیاری است و به صورت مختصر مهمترین مولفه‌های مربوط به آن ارائه شده است:

برنامه ریزی پاسخ: فرایندها و رویه های پاسخگویی در برابر وقایع امنیت سایبری مرکز داده سازمان اجرا و نگهداری می شوند تا از واکنش به حوادث شناسایی شده در فضای مجازی اطمینان حاصل شود.

ارتباطات با ذینفعان: فعالیتهای پاسخگویی مرکز داده سازمان با ذینفعان داخلی و خارجی هماهنگ می شود (به عنوان مثال پشتیبانی خارجی از مرکز افتا یا مرکز ماهر).

تحلیل و بررسی: تجزیه و تحلیل برای اطمینان از پاسخ موثر و پشتیبانی از فعالیت های بازیابی مرکز داده سازمان انجام می‌شود.

کاهش اثرات: فعالیتها برای جلوگیری از گسترش یک رویداد مخرب در مرکز داده سازمان، کاهش اثرات و رفع اثر حادثه انجام می شود.

بهبود فرآیندهای پاسخگویی: فعالیتهای پاسخگویی مرکز داده سازمانی با ترکیب درسهای آموخته شده از فعالیتهای تشخیص و پاسخ فعلی و قبلی بهبود می یابد.

بازیابی

همانطوریکه در ش ۵ مشاهده می‌شود مقوله بازیابی مرکز داده و تداوم ارائه سرویسها و خدمات آن دارای اهمیت بسیاری است و به صورت مختصر مهمترین مولفه‌های مربوط به آن ارائه شده است:

برنامه ریزی بازیابی: فرایندها و رویه های بازیابی مرکز داده سازمان اجرا و نگهداری می شوند تا از ترمیم سیستم ها یا دارایی‌های داده تحت تأثیر حوادث امنیت سایبری اطمینان حاصل شود.

بهبود فرآیندهای بازیابی: برنامه ریزی و فرآیندهای بازیابی مرکز داده سازمان با ترکیب درسهای آموخته شده در فعالیتهای آینده بهبود می یابد.

ارتباطات با ذینفعان: فعالیتهای ترمیم با طرفهای داخلی و خارجی (به عنوان مثال مراکز هماهنگ کننده، ارائه دهندگان خدمات اینترنت، صاحبان سیستمهای حمله کننده، قربانیان، سایر CSIRT ها[1] و فروشندگان هماهنگ می‌شود).

نتیجه‌گیری

پژوهش حاضر به دنبال ارائه چارچوب امنیت سایبری هوشمند و یکپارچه مرکز داده در سطح ملی است از این رو سعی گردید با مرور نظام‌مند ادبیات امنیت‌سایبری مرکزداده و کدگذاری و تحلیل آن‌ها با روش فراترکیب مقوله‌ها و مولفه‌های اصلی این چارچوب شناسایی شوند. در مجموع نتایج کدگذاری منابع منجر به شناسایی مولفه‌های چارچوب و ابعاد آن گردید. در پژوهش حاضر براساس بررسی‌های صورت گرفته در مجموع ۲۳ مولفه به عنوان مولفه‌های چارچوب امنیت سایبری هوشمند و یکپارچه مرکز داده استخراج شدند که از جمله آن‌ها می‌توان به مدیریت دارایی، محیط کسب و کار، حکمرانی، ارزیابی

1. *Computer Security Incident Response Teams*

ریسک، کنترل دسترسی، آموزش و آگاهی، امنیت داده ها، پایش مستمر امنیت، فرآیندهای تشخیصی، برنامه ریزی پاسخگویی، ارتباطات، تحلیل و بررسی، کاهش اثرات، بهبود کارایی و برنامه ریزی بازیابی اشاره کرد که در ۵ مقوله اصلی شناسایی، محافظت، تشخیص، پاسخ دادن و بازیابی مورد شناسایی قرار گرفتند.

در مورد دانش‌افزایی مقاله حاضر باید توجه داشت همانطور که اشاره شد مطالعات قبلی عمدتاً متمرکز بر تهدیدات‌سایبری مرکز داده بودند و مطالعه در مورد چارچوب امنیت سایبری هوشمند و یکپارچه مرکز داده در سطح ملی کمتر انجام شده است. به همین خاطر است که مطالعات قبلی بیشتر متمرکز بر ابعادی مانند تهدید، منشاء تهدید، شیوه تهدید بودند و به مواردی کلیدی مانند چرخه مستمر پایش و نظارت در این چارچوب توجه نکردند. علاوه بر این در پژوهش حاضر برخلاف مطالعات قبلی یک دسته‌بندی جامع از مولفه‌های چاچوب امنیت سایبری مرکز داده ارائه شده است.

پیشنهادات

پیشنهاد های پژوهشی زیر می تواند در ادامه کار پژوهشی فوق مورد نظر قرار گیرد:

– رویکرد جزء گرایانه و شناسایی کدهای مدیریتی چارچوب مدیریت یکپارچه و هوشمند امنیت سایبری مراکز داده.

– رویکرد کل گرایانه و ارائه چارچوب زیست بوم امنیت سایبری مراکز داده سازمانی در کشور با رویکرد مدیریت هوشمند و یکپارچه.

منابع:

- آقایی، م.، و معینی، ع.، و عرب‌سرخی، ا.، و محمدیان، ا.، و زارعی، ع. (۱۳۹۸). **ارائه مدل مفهومی ساختار تهدیدات سایبری مرا ز داده.** فصلنامه امنیت پژوهی دانشگاه فارابی.
- حسین زاده، محمد؛ حسنی آهنگر، محمدرضا. (۱۳۹۵). **اصول طراحی یک مدل امنیتی برای مراکز داده،** یازدهمین سمپوزیوم پیشرفت های علوم و تکنولوژی
- دسترنج، رویا؛ قاضی نوری، سید سپهر؛ دسـ نج، نسرین؛ شایان، علی. (۱۳۹۸). **ارزیابی اکوسیستم کلان داده در ایران با استعاره از مدل ارزیابی اکوسیستم هزاره،** فصلنامه علمی پژوهشی پژوهشگاه علوم و فناوری اطلاعات ایران
- سید علی، نیر سادات. (۱۳۹۷). **شناسایی پارامترهای موفقیت آمیز پیاده سازی انواع فناوریهای مجازی سازی در مراکز داده سازمانها،** فصلنامه مطالعات دانش شناسی دانشگاه علامه طباطبایی
- صلاحی، احمد. (۱۳۹۲). **حفاظت از زر ساخت‌های ملی در برابرحملات سایبری**
- مختاری، حمید رضا؛ مدیری، ناصر. (۱۳۹۹). **خود ارزیابی ا یت پیکر بندی سیستم های مدیریت یکپارچه تهدیدات سایبری،** چهارمین کنفرانس ملی پژوهش های کاربردی در علوم برق و کامپیوتر و مهندسی پزشکی
- مقدسی لیچاهی، امیرحسین؛ همت، حمید. (۱۳۹۷). **ارائه الگوی امنیت در فضای سایبر جمهوری اسلامی ایران با رویکرد آینده پژوهانه** ، ژورنال آینده پژوهی دفاعی

- *Abraham, R., Schneider, J., & vom Brocke, J. (2019). **A conceptual framework, structured review, and research agenda**. International Journal of Information Management, 49, 424-438.*
- *Abraham S., Nair S. (2018). **Comparative analysis and patch optimization using the cyber security analytics framework**. Journal of Defense Modeling and Simulation.*
- *Accenture Technology Vision 2019.*
- *Accenture Trend 4: Secure US to Secure ME.*
- *Ahmed M., Rama Mohan Babu G. (2019). **Cyber security framework for big data environment using support vector machine**. Journal of Advanced Research in Dynamical and Control Systems.*
- *Ahmed AlKalbani., Hepu Deng., Booi Kam., (2014). **A Conceptual Framework for Information Security in Public Organizations for E-Government Development**, 25th Australasian Conference on Information Systems, 8th -10th Dec 2014,*

Auckland, New Zealand.

- *Al-Badi, A., Tarhini, A., & Khan, A. I. (2018).* ***Exploring big data governance frameworks****. Procedia Computer Science, 141, 271-277.*
- *Alhassan, I., Sammon, D., & Daly, M. (2016).* ***Data governance activities: an analysis of the literature****. Journal of Decision Systems, 25(sup1), 64-75.*
- *Alhassan, I., Sammon, D., & Daly, M. (2019).* ***Critical success factors for data governance: a theory building approach****. Information Systems Management, 36(2), 98-110*
- *Ashtiani M., Abdollahi Azgomi M. (2014).* ***A distributed simulation framework for modeling cyber attacks and the evaluation of security measures****. SIMULATION.*
- *Al-Muhtadi J., Saleem K., Al-Rabiaah S., Imran M., Gawanmeh A., Rodrigues J.J.P.C. (2020).* ***A lightweight cyber security framework with context-awareness for pervasive computing environments****. Sustainable Cities and Society.*
- *Attard, J., Orlandi, F., & Auer, S. (2016).* ***Data driven governments: Creating value through open government data Transactions on Large-Scale Data-and Knowledge-Centered Systems*** *XXVII (pp. 84-110): Springer.*
- *Atoum I., Otoom A. (2016).* ***Effective belief network for cyber security frameworks.*** *International Journal of Security and its Applications.*
- *Atoum I., Otoom A., Ali A.A. (2014)* ***A holistic cyber security implementation framework****. Information Management and Computer Security.*
- *Australian Government. (2020).* ***Data Governance framework 2020****.*
- *American National Standards Institute/International Society of Automation (ANSI/ ISA)-62443-2-1 (99.02.01)-2009,* ***Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program****:*

https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116731

- *ANSI/ISA-62443-3-3 (99.03.03)-2013,* ***Security for Industrial Automation and Control***
- *Systems: System Security Requirements and Security Levels: https://www.isa.org/ templates/one-column.aspx?pageid=111294&productId=116785*
- *Baggott S.S., Santos J.R. (2020).* ***A Risk Analysis Framework for Cyber Security***

and Critical Infrastructure Protection of the U.S. Electric Power Grid. Risk Analysis.

- Baig Z., Zeadally S. (2019). **Cyber-security risk assessment framework for critical infrastructures**. Intelligent Automation and Soft Computing.
- Benfeldt, O., Persson, J. S., & Madsen, S. (2019). **Data governance as a collective action problem**. Information Systems Frontiers, 1-15.
- Bhardwaj A., Goundar S. (2019). ***A framework to define the relationship between cyber security and cloud performance***. Fraud and Security.
- Bonina, C., & Eaton, B. (2020). **Cultivating open government data platform ecosystems: Lessons from Buenos Aires, Mexico City and Montevideo**. Government Information Quarterly, 37(3), 101479.
- Calzada, I., & Almirall, E. (2020). **Data ecosystems for protecting European citizens' digital rights**. Transforming Government: People, Process and Policy.
- CIS Critical Security Controls for Effective Cyber Defense (CIS Controls): https://www.cisecurity.org
- Collier J. (2018). **Cyber security assemblages: *A framework for understanding the dynamic and contested nature of security provision***. Politics and Governance
- Control Objectives for Information and Related Technology (COBIT): http://www.isaca.org/COBIT/Pages/default.aspx
- Cyber Threatscape Report 2019. Accenture
- Dawes, S. S., Vidiasova, L., & Parkhimovich, O. (2016). **Planning and designing open government data programs: *An ecosystem approach.*** Government Information Quarterly, 33(1), 15-27.
- Diran, D., Hoppe, T., Ubacht, J., Slob, A., & Blok, K. (2020). ***A data ecosystem for data-driven thermal energy transition: Reflection on current practice and suggestions for re-design***. Energies, 13(2), 444.
- Efthymiopoulos M.P. (2019). ***A cyber-security framework for development, defense and innovation at NATO***. Journal of Innovation and Entrepreneurship.
- European Commission. (2020). **Data governance and data policies at the European Commission.**
- ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends, FINAL

VERSION 1.0 ETL 2018, JANUARY 2019

- Evangelou M., Adams N.M. (2020). ***An anomaly detection framework for cyber-security data.*** Computers and Security.
- Georgiadou A., Mouzakitis S., Bounas K., Askounis D. (2020). ***A Cyber-Security Culture Framework for Assessing Organization Readiness***. Journal of Computer Information Systems.
- Gupta, A., Panagiotopoulos, P., & Bowen, F. (2020). ***An orchestration approach to smart city data ecosystems.*** Technological Forecasting and Social Change, 153, 119929.
- Hadji-Janev M., Bogdanoski M. (2017). **Swarming-based cyber defence under the *framework of collective security.*** Security Journal.
- Hashim M.S., Masrek M.N., Yunos Z. (2016)**. *Elements in the cyber security framework for protecting the Critical Information Infrastructure against cyber threats.*** Information (Japan).
- Hahn A., Thomas R.K., Lozano I., Cardenas A. (2015)**. *A multi-layered and kill-chain based security analysis framework for cyber-physical systems.*** International Journal of Critical Infrastructure Protection.
- Immonen, A., & Kalaoja, J. (2019)**. Requirements of an Energy Data Ecosystem.** IEEE access, 7, 111692-111708.
- Immonen, A., Palviainen, M., & Ovaska, E. (2014)**. *Requirements of an open data based business ecosystem.*** IEEE access, 2, 88-103.
- ISO/IEC 27001, Information technology -- Security techniques -- Information security management systems -- Requirements: https://www.iso.org/standard/54534.html
- Jang, K.-a., & Kim, W.-J. (2020)**. Development of data governance components using DEMATEL and content analysis.** The Journal of Supercomputing, 1-15.
- Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., & Janowski, T. (2020)**. Data governance: Organizing data for trustworthy Artificial Intelligence.** Government Information Quarterly, 37(3), 101493.
- Jetzek, T. (2017). Innovation in the open data ecosystem: Exploring the role of real options thinking and multi-sided platforms for sustainable value generation through open data Analytics, Innovation, and Excellence-Driven Enterprise Sustainability

(pp. 137-168): Springer.

- Kapletia D., Felici M., Wainwright N. (2014). ***An integrated framework for innovation management in cyber security and privacy.*** Communications in Computer and Information Science.
- Kampars, J., Zdravkovic, J., Stirna, J., & Grabis, J. (2020). **Extending organizational capabilities with Open Data to support sustainable and dynamic business ecosystems.** Software and Systems Modeling, 19(2), 371-398.
- Kim I., Park N. (2019). ***A study on cyber security framework by life cycle for safety system based on information and communication technology.*** Journal of Advanced Research in Dynamical and Control Systems.
- Khalid A., Kirisci P., Khan Z.H., Ghrairi Z., Thoben K.-D., Pannek J. (2018). **Security framework for industrial collaborative robotic cyber-physical systems Computers in Industry.**
- Knight R., Nurse J.R.C. (2020 **. *A framework for effective corporate communication after cyber security incidents.*** Computers and Security.
- Kassen, M. (2017). Open data and e-government–related or competing ecosystems: a paradox of open government and promise of civic engagement in Estonia. Information Technology for Development, 25(3), 552-578.
- Le N.T., Hoang D.B. (2017). **Capability maturity model and metrics framework for cyber cloud security.** Scalable Computing.
- Li, S., & Yu, H. (2020). **Big data and financial information analytics ecosystem: strengthening personal information under legal regulation.** Information Systems and e-Business Management, 18(4), 891-909.
- Lillie, T., & Eybers, S. (2018). ***Identifying the constructs and agile capabilities of data governance and data management: A review of the literature.*** Paper presented at the International Development Informatics Association Conference.
- Lindman, J., Kinnari, T., & Rossi, M. (2015). **Business roles in the emerging open-data ecosystem.** IEEE Software, 33(5), 54-59.
- Lu T., Zhao J., Zhao L., Li Y., Zhang X. (2015). ***Towards a framework for assuring cyber physical system security.*** International Journal of Security and its Applications.
- Madaan, N., Ahad, M. A., & Sastry, S. M. (2018). **Data integration in IoT**

ecosystem: Information linkage as a privacy threat. *Computer law & security review*, 34(1), 125-133.

- *Mazumdar, S., Seybold, D., Kritikos, K., & Verginadis, Y.* (2019)**. *A survey on data storage and placement methodologies for cloud-big data ecosystem.*** *Journal of Big Data*, 6(1), 1-37.
- *McBride, K., Olesk, M., Kütt, A., & Shysh, D.* (2020)**. *Systemic change, open data ecosystem performance improvements, and empirical insights from Estonia: A country-level action research study.*** *Information Polity*(Preprint), 1-26.
- *Methodology of business ecosystems network analysis: A case study in Telecom Italia Future Centre, Technological Forecasting and Social Change*, Elsevier, vol. 80(6), pages 1194-1210.
- *Mendhurwar S., Mishra R.* (2019)**. *Integration of social and IoT technologies: architectural framework for digital transformation and cyber security challenges.*** *Enterprise Information Systems.*
- *Micheli, M., Ponti, M., Craglia, M., & Berti Suman, A.* (2020)**. *Emerging models of data governance in the age of datafication.*** *Big Data & Society*, 7(2), 2053951720948087.
- *Moreno, J., Fernandez, E. B., Serrano, M. A., & Fernández-Medina, E.* (2019)**. *Secure development of big data ecosystems.*** *IEEE access*, 7, 96604-96619.
- *National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity", April 16, 2018*
- *NIST SP 800-53 Rev. 4 - NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013 (including updates as of January 22, 2015). https://doi.org/10.6028/NIST.SP.800-53r4.*
- *Noorman, M.* (2017)**. *Institutions in the Data Ecosystem: Actors in the public knowledge domain and in private data companies.*** *Open Data and the Knowledge Society*, 85-103.
- *Oliveira, M. I. S., Lima, G. d. F. B., & Lóscio, B. F.* (2019)**. *Investigations into Data Ecosystems: a systematic mapping study.*** *Knowledge and Information Systems*, 1-42.
- *Otoom A., Atoum I.* (2013). *n implementation framework (IF) for the National*

Information Assurance and Cyber Security Strategy (NIACSS) of Jordan. International Arab Journal of Information Technology.

- *Panda A., Bower A.* (2020)**. Cyber security and the disaster resilience framework.** *International Journal of Disaster Resilience in the Built Environment.*
- *Pandey S., Singh R.K., Gunasekaran A., Kaushik A.* (2020)**. Cyber security risks in globalized supply chains: conceptual framework.** *Journal of Global Operations and Strategic Sourcing.*
- *Porcedda M.G.* (2018)**. Patching the patchwork: appraising the EU regulatory framework on cyber security breaches.** *Computer Law and Security Review.*
- *Rowe B., Halpern M., Lentz T.* (2012)**. Is a public health framework the cure for cyber security?.** *CrossTalk.*
- *Royalsociety.* (2020)**. The UK data governance landscape.**
- *Sandelowski, M., & Barroso, J.* (2006)**. Handbook for synthesizing qualitative research: springer publishing company.**
- *Sani A.S., Yuan D., Jin J., Gao L., Yu S., Dong Z.Y.* (2019)**. Cyber security framework for Internet of Things-based Energy Internet.** *Future Generation Computer Systems.*
- *SANS, The State of Dynamic Data Center and Cloud Security in the Modern Enterprise, A SANS Survey, Dave Shackleford, October 2015*
- *Specht, A., Guru, S., Houghton, L., Keniger, L., Driver, P., Ritchie, E. G.,... Treloar, A.* (2015)**. Data management challenges in analysis and synthesis in the ecosystem sciences.** *Science of the Total Environment, 534, 144-158.*
- *Srinivas J., Das A.K., Kumar N.* (2019)**. Government regulations in cyber security: Framework, standards and recommendations.** *Future Generation Computer Systems.*
- *Svilicic B., Kamahara J., Celic J., Bolmsten J.* (2019)**. Assessing ship cyber risks: a framework and case study of ECDIS security.** *WMU Journal of Maritime Affairs.*
- *Styrin, E., Luna-Reyes, L. F., & Harrison, T. M.* (2017)**. Open data ecosystems: an international comparison.** *Transforming Government: People, Process and Policy.*
- *Tikk-Ringas E.* (2015)**. Legal framework of cyber security.** *Intelligent Systems, Control and Automation: Science and Engineering.*

- Topal O.A., Demir M.O., Liang Z., Pusane A.E., Dartmann G., Ascheid G., Kur G.K. (2020). ***A Physical Layer Security Framework for Cognitive Cyber-Physical Systems.*** *IEEE Wireless Communications.*
- *Vaishnavi, V., Kuechler, W., and Petter, S. (Eds.) (2004/19). "Design Science Research in Information Systems" January 20, 2004 (created in 2004 and updated until 2015 by Vaishnavi, V. and Kuechler, W.); last updated (by Vaishnavi, V. and Petter, S.), June 30, 2019. URL: http://www.desrist.org/design-research-in-information-systems/.*
- *Weber, K., Otto, B., & Österle, H. (2009).* ***One size does not fit all---a contingency approach to data governance.*** *Journal of Data and Information Quality (JDIQ), 1(1), -27.*
- *Wei J. (2010).* ***Knowledge management framework for cyber security learning.*** *International Journal of Management in Education.*
- Yoon, A., & Copeland, A. (2020). ***Toward community-inclusive data ecosystems: Challenges and opportunities of open data for community-based organizations.*** *Journal of the Association for Information Science and Technology, 71(12), 1439-1454.*
- Zhai L., *Vamvoudakis K.G. (2020).* ***A data-based private learning framework for enhanced security against replay attacks in cyber-physical systems.*** *International Journal of Robust and Nonlinear Control.*
- Zimmer, L. (2006). ***Qualitative meta-synthesis: a question of dialoguing with texts.*** *Journal of advanced nursing, 53(3), 311-3*