Electronic & Cyber Defense
Vol. 13, No. 3, 2025 (Serial No. 51). pp. 5*1*- 7*0*
ISSN: 2322-4347, E-ISSN: 2980-8979

Detection and ranking of effective parameters in security evaluation of data center (Case study of the FAVA organization Rasht municipality)

Zahra Barzegar Moghaddam[1], Asadollah Shahbahrami[2]*
[1] Master's degree, Guilan University, Rasht, Iran. *z_barzegar13@yahoo.com*
[2] Professor at Guilan University, Rasht, Iran. (Correspondence: *shahbahrami@guilan.ac.ir*)

ARTICLE INFO

Article history:

Article Type: Research paper

Receive: 17 June 2025
Revise: 31 July 2025
Accept: 09 September 2025
Available online: 03 October 2025

Keywords:
Data Center
Security evaluation
FAHP

ABSTRACT

Because of gathering essential requirement for maintenance, reparation and technical support, data centers are an appropriate solution for reducing information technology cost and responsiveness to customer requirements. the data center structure must be designed and implemented in such a way that it always supplies the three essential principles of security, namely confidentiality, availability and integrity. Due to the complexity of these centers, for designing principles and supply the security, variant national documents and international standards had been prepared. In this research, by revising existence standards, effective parameters in security had been exploited in three forms of physical infrastructure security, IT infrastructure security and management issues, which can be used in the assessment security of data center. In a case study, by preparing a questionnaire, data center experts and information technology experts were asked to prioritize the parameters. Result of examinations which implemented with FAHP show that information technology infrastructure security with close weight to one is on priority, and physical infrastructure security is in the next rank. Between information technology infrastructure sub-metrics, storing and backup with 0.52 relative weight is in the first, management and information technology infrastructure monitoring with 0.28 relative weight is in the second, processing requirements with 0.20 relative weight is in the third and the rest of metrics are important in the fourth priority. And also, between physical infrastructure sub-metrics, fire protection with 0.78 relative weight is in the first, power and ground connection with 0.22 relative weight is in the second and the rest of all are important in the third priority.

Cite this article: Barzegar Moghaddam, Z., & shahbahrami, A. (2025). Detection and ranking of effective parameters in security evaluation of data center (Case study of the FAVA organization Rasht municipality). *Electronic and Cyber Defense*, *13*(3), 51-70. 2025. DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1404.13.3.2.1

Publisher: Imam Hossein University

«پدافند الکترونیکی و سایبری»
سال سیزدهم، شماره ۳، پاییز ۱۴۰۴، ص ۵۱- ۷۰
شاپا الکترونیکی: 4347 -2322 شاپا چاپی: 8979- 2980

شناسایی و رتبه‌بندی پارامترهای تأثیرگذار در ارزیابی امنیتی مراکز داده (مطالعه موردی سازمان فاوا شهرداری رشت)

زهرا برزگر مقدم [1]، اسدالله شاه بهرامی* [2]

[1] کارشناس ارشد، دانشگاه گیلان، رشت، ایران. *z_barzegar13@yahoo.com* .

[2] استاد دانشگاه گیلان، رشت، ایران. (نویسنده مسئول: *shahbahrami@guilan.ac.ir*)

چکیده

مراکز داده به دلیل تجمیع امکانات لازم برای نگهداری، تعمیرات و پشتیبانی فنی، یک راه‌حل مناسب برای کاهش هزینه‌های فناوری اطلاعات و پاسخگویی به نیازهای مشتریان است. ساختار مراکز داده باید به‌گونه‌ای طراحی و پیاده‌سازی شود که همواره سه اصل اساسی امنیت یعنی محرمانگی، دسترس‌پذیری و صحت و جامعیت تأمین شود. با توجه به پیچیدگی این مراکز، برای طراحی اصولی و تأمین امنیت، اسناد ملی و استانداردهای بین‌المللی مختلفی تدوین گردیده است. در این پژوهش با بررسی استانداردهای موجود، پارامترهای مؤثر در امنیت در قالب سه محور امنیت زیرساخت فیزیکی، امنیت زیرساخت فناوری اطلاعات و مبحث مدیریت استخراج‌شده که می‌تواند در ارزیابی امنیتی مراکز داده مورداستفاده قرار بگیرد. در یک مطالعه موردی با تهیه یک پرسش‌نامه، از صاحب‌نظران حوزه مرکز داده و کارشناسان فناوری اطلاعات خواسته شد نسبت به اولویت‌بندی پارامترها اقدام نمایند. نتیجه بررسی‌ها که با روش *FAHP* انجام شد، نشان می‌دهد امنیت زیرساخت فناوری اطلاعات با وزنی نزدیک به یک به‌طور محسوسی در اولویت قرار دارد و امنیت زیرساخت فیزیکی در رده بعدی قرار می‌گیرد. از بین زیرمعیارهای حوزه زیرساخت فناوری اطلاعات، ذخیره‌سازی و پشتیبان گیری با وزن نسبی 0/52 در اولویت اول، مدیریت و پایش زیرساخت فناوری اطلاعات با وزن نسبی 0/28 در اولویت دوم، تجهیزات پردازشی با وزن نسبی 0/20 در اولویت سوم و مابقی شاخص‌ها در اولویت چهارم اهمیت قرار دارند. در میان زیرمعیارهای حوزه زیرساخت فیزیکی نیز حفاظت در برابر آتش با وزن نسبی 0/78 در اولویت اول، برق و اتصال زمین با وزن نسبی 0/22 در اولویت دوم و مابقی شاخص‌ها در اولویت سوم اهمیت قرار دارند.

مشخصات مقاله

تاریخچه مقاله:

نوع مقاله: علمی- پژوهشی

دریافت: 27 خرداد 1404
بازنگری: 09 مرداد 1404
پذیرش: 18 شهریور 1404
ارائه آنلاین: 11 مهر 1404

کلیدواژه‌ها:

ارزیابی امنیتی
مرکز داده
تحلیل فازی

استناد: برزگر مقدم، زهرا و شاه بهرامی، اسدالله. (۱۴۰۴). شناسایی و رتبه‌بندی پارامترهای تأثیرگذار در ارزیابی امنیتی مراکز داده(مطالعه موردی سازمان فاوا شهرداری رشت) .پدافند الکترونیکی و سایبری، ۱۳(۳)، ص ۵۱-۷۰. https://dor.isc.ac/dor/20.1001.1.23224347.1404.13.3.2.1

ناشر: دانشگاه جامع امام حسین(ع).

۱. مقدمه

فناوری اطلاعات روش انجام کارها و وظایف را در سازمان‌ها متحول کرده است. قدرت پردازش سریع، دسترسی آنی به خدمات و اطلاعات، صرفه‌جویی در هزینه و افزایش بهره‌وری باعث شده استفاده از آن به‌سرعت گسترش یابد. با افزایش استفاده از این فناوری، حجم داده‌های الکترونیک رشد فزاینده‌ای یافته و وابستگی شدید سازمانی را به دنبال داشته است. گزاف نیست اگر بگوییم داده‌های الکترونیک، جزء مهم‌ترین سرمایه‌های یک سازمان به‌حساب می‌آیند که ازدست‌رفتن یا آسیب دیدن آن‌ها ضربه بزرگی ازلحاظ اعتباری و تجاری محسوب می‌شود. «طبق گزارش مؤسسه *Ponemon*، میانگین هزینه خرابی داده‌ها در انگلستان از 47 پوند در سال 2007 به 79 پوند در سال 2011 افزایش‌یافته است. این افزایش شدید نشانه افزایش چشمگیر ارزش اطلاعات سازمان‌ها است. بااین‌حال، برای برخی از انواع اطلاعات مانند پرونده پزشکی، جایی که یک تلفات تنها می‌تواند موضوع زندگی یا مرگ باشد، اهمیت آن نمی‌تواند تنها باارزش پولی سنجیده شود» [1]. لذا نیاز به نگهداری یکپارچه و امن این اطلاعات نیز افزایش‌یافته و منجر به شکل‌گیری مراکز تخصصی برای این امر به نام مراکز داده‌شده است. وجود مراکز داده باعث می‌شود ارائه خدمات به‌صورت الکترونیک، با سهولت بیشتری انجام شود و کارفرمایان به‌جای تمرکز بر نگهداری و پشتیبانی از این مراکز، توجه خود را به گسترش خدمات معطوف دارند. همه مزایای ذکرشده نیازمند مقدمه‌ای به نام امنیت است و هر چه یک مرکز داده بزرگ‌تر می‌شود، الزامات امنیتی آن نیز افزایش می‌یابد. باوجود امتیازات ویژه‌ای که یک مرکز داده دارد، اگر نتواند اطمینان مشتریان را برای نگهداری امن داده‌ها و ارائه خدمات آنی، بدون تأخیر و توقف فراهم کند، مورد اقبال قرار نخواهد گرفت.

تأمین امنیت مراکز داده در سه بعد محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات، از مسائلی است که دولت و صنعت فناوری اطلاعات با جدیت آن را دنبال می‌کنند؛ لذا تدوین یک برنامه امنیتی فراگیر و همه‌جانبه از بدیهیات و مقدمات اولیه ایجاد مراکز داده است. با توجه به پیچیدگی که در طراحی مراکز داده وجود دارد، باید مسائل مختلفی قبل، حین و بعد از ایجاد مراکز داده در نظر گرفته شود. غول‌های فناوری اطلاعات صرفاً برای انتخاب مکان مرکز داده زمان قابل‌توجهی را صرف می‌کنند که این زمان در برخی موارد تا سه سال هم به طول انجامیده است [2]. ازاین‌رو برای طراحی امن مراکز داده، اسناد و استانداردهای ملی و بین‌المللی متنوعی تاکنون ارائه‌شده است. برای اطمینان از امنیت مرکز داده نیاز است بر اساس استانداردها نسبت به ارزیابی این مراکز اقدام شود. ارزیابی، خطرات موجود را شناسایی کرده و باعث می‌شود مالکان و ذی‌نفعان مرکز داده از صحت طراحی آن مطمئن شده و نسبت به رفع نواقص و اشکالات اقدام نمایند؛ بنابراین در مرحله اول باید پارامترهای تأثیرگذار در ارزیابی امنیتی مراکز داده را شناسایی نمود. در مرحله دوم باید پارامترهای شناسایی‌شده را رتبه‌بندی کرد تا بتوان بر اساس اولویت‌های هر مرکز داده، نسبت به تأمین امنیت آن اقدامات لازم را انجام داد.

بخش‌بندی مقاله در ادامه به این شرح است:
در بخش مبانی نظری و ادبیات تحقیق، اسناد ملی و استانداردهای بین‌المللی که برای امنیت مراکز داده وجود دارد، بررسی شد و پارامترهای مؤثر بر امنیت مراکز داده استخراج گردید. در بخش پیشینه پژوهش، تحقیقات مشابهی که درباره امنیت مراکز داده انجام‌شده، موردبررسی قرار گرفت. در بخش بعدی، مدل سلسله مراتبی پژوهش بر اساس پارامترهای شناسایی‌شده در بخش مبانی نظری و ادبیات تحقیق، طراحی شد. در بخش روش پژوهش و تحلیل داده‌ها، روش‌های تصمیم‌گیری چند شاخصه بررسی شد و نحوه انجام مطالعه موردی تشریح گردید. در انتها نیز نتایج مطالعه موردی بحث و نتیجه‌گیری شد و بر اساس نتایج پژوهش، پیشنهادهای لازم برای افزایش امنیت مرکز داده سازمان فناوری اطلاعات شهرداری رشت ارائه گردید.

۲. مبانی نظری و ادبیات تحقیق

2-1. تعریف مرکز داده

تعاریف مختلفی را برای مرکز داده می‌توان به کاربرد.

«مرکز داده مکانی است با امنیت فیزیکی و الکترونیکی بالا، برخوردار از پهنای باند ارتباطی وسیع، متصل به شبکه‌های رایانه‌ای ملی یا جهانی، با خدمات تمام‌وقت و در دسترس که شامل انواع تجهیزات سخت‌افزاری (رایانه‌ها، سوئیچ‌ها، مودم‌ها و غیره) و نرم‌افزاری (پایگاه‌های داده، کامپیوترهای میزبان، سیستم‌عامل و غیره) پیشرفته بوده و از پشتیبانی و نگهداری حرفه‌ای و تمام‌وقت برخوردار است و پشتیبانی و خدمات مرتبط با اطلاعات و داده از قبیل خدمات ذخیره، نگهداری و بازیابی داده، خدمات برنامه‌ریزی منابع سازمانی[1]، میزبانی خدمات اینترنتی، میزبانی ارائه خدمات کاربردی[2]، میزبانی برون‌سپاری خدمات[3]، خدمات شبکه اختصاصی مجازی[4] و غیره را به شرکت‌های خصوصی یا دولتی ارائه می‌دهد» [3].

[1] *Enterprise Resource Planning (ERP)*
[2] *Application Service Providing (ASP)*
[3] *Out-Sourcing*
[4] *Virtual private Network (VPN)*

از دید سیسکو مرکز داده شبکه‌ای از منابع محاسباتی و ذخیره‌سازی است که امکان تحویل برنامه‌های کاربردی و داده‌های به اشتراک گذاشته‌شده را فراهم می‌کند. در دنیای فناوری اطلاعات، مرکز داده‌ها از برنامه‌های کاربردی تجاری پشتیبانی می‌کند که شامل موارد ساده‌ای چون ایمیل و اشتراک‌گذاری فایل‌ها تا مدیریت ارتباط با مشتری[1] و برنامه‌ریزی منابع سازمانی برای داده‌های بزرگ[2]، ارتباطات و خدمات همکاری است. مؤلفه‌های اصلی یک مرکز داده به شرح زیر است:

زیرساخت شبکه که کامپیوترهای میزبان (ازجمله میزبان مجازی شده) را به سرویس‌های مرکز داده، دستگاه‌های ذخیره‌سازی و اتصالات خارجی به مکان کاربر نهایی متصل می‌کند. زیرساخت ذخیره‌سازی که آرایه‌های ذخیره‌سازی را برای ذخیره سوخت مرکز داده که داده‌ها هستند، فراهم می‌کند. منابع محاسباتی که کامپیوترهای میزبان هستند و پردازش، حافظه، ذخیره‌سازی محلی و اتصال شبکه را برای موتورهای مرکز داده که برنامه‌های کاربردی هستند، فراهم می‌کنند.

«مرکز داده محلی است برای میزبانی سامانه‌های رایانه‌ای و اجزاء مرتبط با آن از قبیل سامانه‌های مخابراتی و ذخیره‌سازی» [4].

بر اساس تعاریف فوق، می‌توان این ویژگی‌ها را برای یک مرکز داده برشمرد: مرکز داده یک مکان شامل تجهیزات سخت‌افزاری و نرم‌افزاری است که به ارائه خدمات و سرویس‌های مختلف فناوری اطلاعات به اشخاص حقیقی و حقوقی می‌پردازد و نیازمند پشتیبانی تمام‌وقت و حرفه‌ای است.

در یک مرکز داده فضاها بر اساس استاندارد تقسیم می‌شوند و می‌توانند شامل موارد زیر باشند:

فضای ورودی، فضای عمومی واداری، اتاق اصلی کامپیوترهای میزبان، اتاق کنترل و پشتیبانی، نگه‌دارنده‌ها و محل‌های ورودی و خروجی داده مخابراتی، دکل ارتباطی، اتاق باطری و تجهیزات برق اضطراری، محل تجهیزات تهویه بیرونی و داخلی، محل ژنراتور، مخازن سرکوب آتش، مخزن سوخت ژنراتور (با رعایت فاصله مناسب و نکات ایمنی)، محل بارگیری تجهیزات، پارکینگ یا محوطه ورودی کامیون‌های حمل‌کننده تجهیزات.

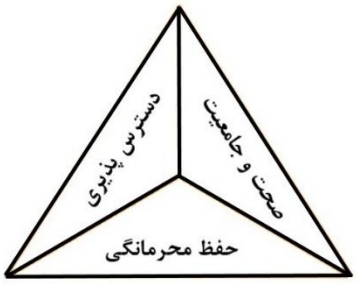
2-2. خدمات مراکز داده

خدمات مراکز داده به چهار قسمت اصلی تقسیم می‌شوند:

- اجاره فضای موردنیاز مشترک جهت نصب تجهیزات شبکه‌ای و سرویس گرها در محل مجتمع خدمات اینترنتی.
- اجاره دادن بخشی از فضای رایانه‌های موجود در مراکز داده اینترنتی[3] از قبیل میزبانی سرویس‌دهنده، میزبانی وب و اجاره فضای ذخیره‌سازی.
- ارائه برنامه‌های کاربردی به مشترکین نظیر بانک‌های اطلاعاتی، سامانه‌های اطلاعاتی جغرافیایی [4] ، برنامه‌های محاسباتی پیشرفته، اتوماسیون و غیره به‌صورت متمرکز با امکان دسترسی از راه دور به همراه خدمات نگهداری متمرکز اطلاعات برنامه‌ها.
- ارائه خدمات ارتباط با شبکه از قبیل عرضه ترافیک اینترنت به ارائه‌کنندگان خدمات اینترنتی و همچنین ایجاد شبکه‌های خصوصی محلی و داخل شهری.

2-3. مفاهیم پایه امنیت اطلاعات

امنیت اطلاعات به معنای حفظ محرمانگی[5]، دسترس‌پذیری اطلاعات[6] و صحت و جامعیت[7] است. محرمانگی به این معناست که اطلاعات صرفاً در اختیار افراد مجاز بوده و برای افراد غیرمجاز فاش نگردد. دسترس‌پذیری بدین معناست که به‌محض تقاضا، اطلاعات در اختیار افراد مجاز قرار گیرد و صحت و جامعیت نیز یعنی جلوگیری از تغییر غیرمجاز داده و تشخیص تغییر در صورت دست‌کاری آن [5]. شکل (1) ابعاد مثلث امنیت اطلاعات را نشان می‌دهد.



شکل (1). مثلث امنیت [5]

دارایی هر چیزی است که برای سازمان ارزشمند باشد و ازدست‌دادن آن باعث اختلال در امور می‌گردد، مانند اسناد اعم از کاغذی و الکترونیک، کارکنان متخصص، سخت‌افزارها، نرم‌افزارها، توپولوژی شبکه، تنظیمات مربوط به تجهیزات و غیره [5].

آسیب‌پذیری[8] یک نقص در طراحی، پیاده‌سازی یا فعالیت یک سیستم است که می‌تواند منجر به یک رخنه نرم‌افزاری یا نقص سیاست‌های امنیتی شده و مورد سوءاستفاده قرار بگیرد [5].

[1] *Customer Relationship Management (CRM)*
[2] *Big Data*
[3] *Internet Data Center (IDC)*
[4] *Geographic Information Systems (GIS)*
[5] *Confidentiality*
[6] *Availability*
[7] *Integrity*
[8] *Vulnerability*

تهدید[1] عامل بالقوه‌ای است که می‌تواند به محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات آسیب بزند [5].

خطر احتمال وقوع یک تهدید است [5].

ریسک[2] تأثیر منفی یک آسیب‌پذیری در فرایندهای سیستم با درنظرگرفتن احتمال وقوع آن است و از حاصل‌ضرب احتمال تهدید در تأثیر خرابی حاصل از آن، به دست می‌آید [5].

حمله[3] هر عملی است که امنیت سیستم را مختل کند و می‌تواند فعال یا غیرفعال باشد. در حملات فعال، محتوای اطلاعات تحت تأثیر قرار می‌گیرد و در حملات غیرفعال صرفاً اطلاعات در معرض دید قرار می‌گیرند [5].

2-4. امنیت مرکز داده

مراکز داده قلب تپنده زیرساخت‌های فناوری اطلاعات یک کشور هستند و ازاین‌رو نقش مهمی در امنیت یک کشور می‌توانند داشته باشند. با به‌خطرافتادن امنیت یک مرکز داده، سرویس‌های حیاتی مبتنی بر آن به مخاطره می‌افتند [3]. بنابراین ساختار مراکز داده باید به‌گونه‌ای طراحی و پیاده‌سازی شود که همواره سه اصل اساسی امنیت یعنی محرمانگی، دسترس‌پذیری و صحت و جامعیت تأمین شود. باید توجه داشت که هر چه سطح دسترسی بالاتر باشد، امنیت کمتر می‌شود و بالعکس هر چه امنیت بیشتر باشد، دسترسی کمتر خواهد بود. پس برای تعادل این مثلث باید اضلاع آن با لحاظ کردن مؤلفه‌های مدنظر و میزان امنیت موردنیاز، تنظیم شوند[5].

همه مراکز داده در یک درجه از اهمیت قرار ندارند. از همین رو باید مراکز داده را ازنظر اهمیت و حساسیت امنیتی طبقه‌بندی نمود؛ بنابراین اولین گام فراهم کردن امنیت برای هر سیستم، تعیین نیازهای امنیتی آن سیستم است. برنامه‌های امنیتی را می‌توان به پنج مرحله مجزا تقسیم کرد: برنامه‌ریزی برای تعیین نیازهای امنیتی، ارزیابی مخاطره و انتخاب بهترین شیوه‌ها، ایجاد سیاست‌هایی برای انعکاس نیازها، پیاده‌سازی امنیت، بررسی و واکنش به وقایع [3].

2-4-1. امنیت فیزیکی

در اینجا سعی می‌شود با بررسی کلیه جوانب از تحقق هرگونه تهدید فیزیکی یا آسیب‌های ناشی از بلایای طبیعی جلوگیری شود؛ لذا در سه مرحله تمهیدات امنیتی به اجرا درمی‌آید: مرحله قبل از ایجاد مرکز داده با انتخاب محل مناسب، هنگام ایجاد مرکز داده از طریق طراحی ایمن و پیش‌بینی کلیه شرایط، پس از ایجاد مرکز داده با مراقبت دائمی [3].

در انتخاب محل مرکز داده باید این نکته موردتوجه قرار بگیرد که محل قرار گرفتن کامپیوترهای میزبان و قفسه‌ها و دستگاه‌هایی مثل ژنراتور و تجهیزات برق اضطراری به چه مقدار فضا نیاز دارند. عدم نزدیکی محل مرکز داده به عوامل طبیعی خطرآفرین ازجمله رودخانه، معادن، آبراه یا خط ساحلی، کانال‌ها، مخازن، سدها، دشت سیلابی، نکات اولیه انتخاب محل جغرافیایی هستند. همچنین زلزله‌خیز بودن محل باید موردبررسی قرار بگیرد تا تمهیدات لازم در نظر گرفته شود. بالا بودن بیش‌ازحد دما در مناطق گرم ضمن بالابردن هزینه‌های تهویه، هزینه نگهداری تجهیزات را بالابرده و عمر تجهیزات را کاهش می‌دهد. همچنین سرمای بیش‌ازحد یا رطوبت بیش‌ازاندازه یا کمتر از مقدار لازم باعث بروز خطا در تجهیزات می‌شوند. رعایت فاصله از برخی اماکن مانند فرودگاه، راه‌آهن، مراکز نظامی، پمپ‌بنزین، خطوط فشارقوی برق، نیروگاه هسته‌ای و غیره ضروری است [6].

سایر ملاحظاتی که قبل از ایجاد مرکز داده باید به آن دقت نمود نیز به شرح ذیل است:

سیستم اعلام و اطفای حریق، دستگاه‌های تأمین‌کننده برق اضطراری یا همان *UPS*[4]، ژنراتور به‌منظور تأمین جریان برق پایدار در زمان قطعی برق، سیستم اتصال زمین، سیستم کنترل تردد، دستگاه‌های تهویه مطبوع، تعبیه آسانسورهای مناسب، طراحی مناسب درب‌های ورودی، روش‌های دسترسی مناسب به محل، امکان اتصال خطوط فیبر نوری، بررسی موانع جغرافیایی برای ارتباطات بدون سیم یا نزدیکی مراکز مخابراتی، وجود منابع انسانی متخصص در محدوده قابل سکونت و تردد آسان کارکنان به محل در تمام شرایط جوی و شب و روز و شرایط اضطراری، طراحی راهرو گرم و راهرو سرد جهت هدایت گرما و سرما [6].

2-4-2. امنیت شبکه و ارتباطات

مهم‌ترین مزیت شبکه‌های کامپیوتری، اشتراک منابع سخت‌افزاری و نرم‌افزاری و دستیابی سریع و آسان به اطلاعات است. به‌منظور ارائه این خدمات، سرویس‌ها و پروتکل‌های متعددی نصب و پیکربندی می‌شود که بعضی از آن‌ها استعداد لازم برای برخی حملات رادارند؛ لذا کنترل دستیابی و نحوه استفاده از سرویس‌ها و منابعی که به اشتراک گذاشته‌شده، از مهم‌ترین اهداف یک نظام امنیتی در شبکه است. این راهکارها باهدف تحقق موارد ذیل پیاده‌سازی می‌شوند:

- حفظ محرمانگی یعنی از افشای اطلاعات به افراد غیرمجاز

[1] *Threat*
[2] *Risk*
[3] *Attack*
[4] *Uninterruptible Power Supply*

جلوگیری شود.
- حفظ جامعیت داده؛ یعنی داده‌ها به‌درستی در مقصد دریافت شود.
- احراز هویت یعنی گیرنده از هویت فرستنده آگاه شود.
- دستیابی مجاز یعنی فقط کاربران مجاز بتوانند به داده‌ها دسترسی داشته باشند.
- عدم انکار یعنی فرستنده نتواند ارسال پیام توسط خودش را انکار کند.
- تعیین اعتبار و کنترل دسترسی یعنی دادن مجوز دسترسی به کاربران مجاز با توجه به سطوح دسترسی آن‌ها [5].

برخی اقدامات اصلی که در این راستا انجام می‌شود عبارت‌اند از: نصب دیوار آتش‌های سخت‌افزاری و نرم‌افزاری[1]، نصب سامانه‌های تشخیص نفوذ[2]، نصب سامانه‌های پیشگیری از نفوذ[3]، نصب سامانه‌های شناسایی، تعیین اعتبار و حسابرسی[4]، نصب سامانه‌های پشتیبان اطلاعات، نصب سیستم ترمیم خرابی [3].

2-4-3. امنیت خدمات

عمده تهدیدات علیه مرکز داده به شکل الکترونیکی و در قالب حملات الکترونیکی هستند و به‌ندرت اتفاق می‌افتد تعرض فیزیکی صورت گیرد. زیرا همان‌طور که بارها تأکید شده، ارزش واقعی این مراکز به اطلاعات ذخیره‌شده‌شان است؛ لذا قاعدتاً باید هدف از تهاجم به آن‌ها نیز لطمه به اطلاعات باشد. حال وقتی می‌توان از دوردست‌ترین نقاط این کره خاکی و در آرامش خاطر این مراکز را مورد تهدید جدی قرارداد، دنبال کردن تهدیدات فیزیکی عاقلانه به نظر نمی‌رسد [3].

ایمنی و پایداری خدمات و افزایش آستانه تحمل در مواجهه با تهدیدات و کاهش آسیب‌پذیری‌ها، نیازمند تأمین امنیت در حوزه نرم‌افزارهای کاربردی، سیستم‌عامل، تجهیزات سخت‌افزاری، شبکه‌های رایانه‌ای و پایگاه داده است [5].

2-5. استانداردها و معیارهای طراحی مراکز داده

با توجه به اینکه تجهیزات موجود در یک مرکز داده توسط یک سازمان خاص و یا یک سازنده خاص ارائه نمی‌شود، لازم است مدیریت واحدی باواسطه‌های استاندارد در گروه‌های مختلف برای پایش و رفع عیب ارائه گردد. بعضی از مهم‌ترین استانداردهای موجود به این شرح است:

2-5-1. استاندارد TIA[5]-942

استانداردی است که توسط انجمن علمی صنعت ارتباطات در سال 2005 برای تعیین راهکارهای عملی برای طراحی و ساخت مراکز داده مخصوصاً با نگرش تخصصی به نظام‌های کابل‌کشی و طراحی شبکه، ایجادشده است[2]. این استاندارد مباحث زیر را موردبررسی قرار می‌دهد:

- نمای کلی طراحی مرکز داده
- زیرساخت سیستم کابل‌کشی
- طراحی فضاهای مخابراتی و توپولوژی‌های مرتبط
- دستگاه‌ها و مسیرهای کابل‌کشی
- افزونگی مرکز داده

2-5-2. استاندارد BICSI[6]-002

این استاندارد، یکی از استانداردهای موجود برای طراحی، ساخت و پیاده‌سازی مراکز داده است که در سال 2010 منتشر شد و تفاوت آن با استانداردهای مؤسسه *TIA* این است که بیشتر مواردی را که در استانداردهای *TIA* لحاظ نشده یا به‌صورت کلی به آن اشاره‌شده بود، پوشش داده است. ازجمله مباحث مطرح‌شده:

- انتخاب سایت
- طراحی فضا
- ملاحظات معماری
- ملاحظات ساختاری
- سامانه‌های الکتریکی
- ملاحظات مکانیکی
- محافظت از آتش
- امنیت فیزیکی
- مدیریت مرکز داده و سامانه‌های ساختمان
- کابل‌کشی مخابرات، زیرساخت، مسیرها و فضاها
- فناوری اطلاعات
- راه‌اندازی
- تعمیر و نگهداری مرکز داده [2]

2-5-3. معیار DC100

سازمان فناوری اطلاعات ایران، اقدام به تدوین و انتشار معیار *DC100* در سال 1395 کرده است. این معیار به‌منظور ارزیابی مراکز داده تنظیم‌شده و الزامات آن پوشش‌دهنده نیازهای مراکز داده از مرحله طراحی تا مرحله بهره‌برداری است. الزامات ارزیابی مراکز داده در این معیار، به 20 حوزه تقسیم‌بندی شده‌اند:

[1] *Firewall*
[2] *Intrusion Detection System (IDS)*
[3] *Intrusion Prevention System (IPS)*
[4] *Authentication, Authorization, and Accounting (AAA)*
[5] *Telecommunications Infrastructure Association (TIA)*
[6] *Building Industry Consulting Service International*

- موقعیت جغرافیایی
- ساختمان و معماری
- حفاظت در برابر آتش
- نظارت تصویری و امنیت فیزیکی
- برق و اتصال زمین
- تهویه و مکانیک
- ارتباطات و شبکه غیرفعال
- حفاظت الکترومغناطیس
- مدیریت و پایش زیرساخت فیزیکی
- سیستم‌عامل
- نرم‌افزارها و برنامه‌های کاربردی
- ارتباطات و شبکه فعال
- تجهیزات پردازشی
- ذخیره‌سازی و پشتیبان گیری
- خدمات پایه فناوری اطلاعات
- خدمات پایگاه‌های داده
- مدیریت و پایش زیرساخت فناوری اطلاعات
- مهندسی
- راهبری و نگهداری
- خدمت

این 20 معیار به‌طورکلی در سه دسته زیر قرار می‌گیرند:

- زیرساخت فیزیکی
- زیرساخت فناوری اطلاعات
- مدیریت [6]

2-5-4. پدافند غیرعامل در طراحی مراکز داده

این سند شامل ملاحظات سازمان پدافند غیرعامل در طراحی و ساخت مراکز داده در کشور است. در این سند تهدیدات امنیتی متصور برای مراکز داده کشور با رویکرد پدافند غیرعامل بررسی گردیده است. این تهدیدات در سه دسته موردتوجه قرارگرفته است:

- تهدیدات ناشی از جنگ (سایبری و فیزیکی) و مخاصمات بین‌المللی
- تهدیدات امنیتی
- تهدیدات محیطی و طبیعی [3]

2-5-5. استانداردهای ASHRAE[1]

مجموعه استانداردهای انجمن مهندسین سرمایش، گرمایش و تهویه مطبوع آمریکاست. این انجمن در سال 1894 تأسیس‌شده است. تعدادی از استانداردهای این موسسه که در مراکز داده مورداستفاده قرار می‌گیرد، در جدول (1) ارائه‌شده است:

جدول (1). استانداردهای *ASHRAE* [2]

عنوان	شرح
ASHRAE-TC9.9	این استاندارد مربوط به تجهیزات برقی مراکز داده است و پیشنهادهایی را برای قابلیت اطمینان این تجهیزات ارائه می‌کند.
ASHRAE-62.1	این استاندارد مربوط به بهبود کیفیت هوای داخل ساختمان است.
ASHRAE-189.1	این استاندارد به الزامات ساختمان‌های سبز می‌پردازد.
ASHRAE-90.1	این استاندارد به صرفه‌جویی انرژی در ساختمان‌های تجاری مربوط می‌شود.

2-5-6. استانداردهای NFPA[2]

مجموعه استانداردهای انجمن ملی آتش‌نشانی آمریکاست. تعدادی از استانداردهای این مؤسسه که در مراکز داده مورداستفاده قرار می‌گیرد، در جدول (2) ارائه‌شده است:

جدول (2). استانداردهای *NFPA* [2]

عنوان	شرح
NFPA-12A	این استاندارد به الزامات سامانه‌های آتش‌خاموش‌کن با گاز هالون 1301 می‌پردازد.
NFPA-13	این استاندارد به دستگاه‌های آب‌پاش معلق که از آب برای خاموش کردن آتش در بخش‌های عمومی مراکز داده استفاده می‌کنند، مربوط می‌شود.
NFPA-20	این استاندارد به پمپ‌های ثابت که از آب به‌صورت مه و فوم برای خاموش کردن آتش در بخش‌های عمومی مراکز داده استفاده می‌کنند، مربوط می‌شود.
NFPA-70	این استاندارد به ایمنی برق مربوط می‌شود.
NFPA-75	این استاندارد الزامات حفاظت الکترونیکی از رایانه‌ها، تجهیزات ارتباطی، پردازشگرها و سایر تجهیزات فناوری اطلاعات را در مراکز داده بیان می‌کند.
NFPA-76	این استاندارد الزامات موردنیاز برای حفاظت از امکانات ارتباط از راه دور مانند تلفن همراه، اینترنت، تلفن اینترنتی[3] و غیره در مقابل آتش را بیان می‌کند.
NFPA-2001	این استاندارد به سامانه‌های آتش‌خاموش‌کن با پایه گاز مربوط می‌شود.
NFPA-2010	این استاندارد به سامانه‌های آتش‌خاموش‌کن با گاز آئروسل مربوط می‌شود.

2-5-7. استانداردهای IEEE[4]

مؤسسه مهندسان برق و الکترونیک، یک مؤسسه غیرانتفاعی است که به تدوین استاندارد برای صنایع برق و الکترونیک می‌پردازد. تعدادی از استانداردهای این مؤسسه که در مراکز داده مورداستفاده قرار می‌گیرد، در جدول (3) ارائه‌شده است:

[1] *American Society of Heating, Refrigerating and Air Conditioning Engineers*

[2] *American National Fire Protection Association*

[3] *Voice Over Internet Protocol*

[4] *Institute of Electrical and Electronics Engineers*

جدول (3). استانداردهای *IEEE* [2]

عنوان	شرح
IEEE-142 Green Book	این استاندارد توصیه‌هایی برای نصب و راه‌اندازی دستگاه‌های برقی، برق ژنراتور و برق اضطراری ارائه می‌کند.
IEEE-450	این استاندارد به تعمیر و نگهداری باطری می‌پردازد.
IEEE-493 Gold Book	این استاندارد طراحی صنعتی قابل‌اطمینان را برای دستگاه‌های برقی بر اساس استراتژی هزینه در مقابل اطمینان و برق 24 × 7 پایه‌ریزی می‌کند.
IEEE-1184	هدف این استاندارد ارائه الگوی بهینه برای نگهداری باطری‌های سامانه برق اضطراری است.
IEEE-1491	این استاندارد به انتخاب باطری برای تجهیزات پایش مربوط می‌شود.
IEEE-STD-299	این استاندارد برای اندازه‌گیری اثربخشی محافظ‌های الکترومغناطیسی برای کنترل سامانه‌های محاسباتی با حساسیت الکترومغناطیسی بالایی استفاده می‌شود.
IEEE-1100	این استاندارد برای تمرین اقدامات پیشنهادی برای بهبود کارایی تجهیزات برقی ارائه‌شده است.

2-5-8. استانداردهای Telcordia

مجموعه استانداردهای شرکت آمریکایی - سوئدی *Telcordia* که قبلاً بانام شرکت مخابراتی بل فعالیت می‌کرد، شامل حوزه‌های قدرت، فیزیک، زلزله، مقاومت در برابر آتش، حفاظت حرارتی، صاعقه، امواج و تداخل الکترومغناطیس و غیره است. تعدادی از استانداردهای این مؤسسه که در مراکز داده مورداستفاده قرار می‌گیرد، در جدول (4) ارائه‌شده است:

جدول (4). استانداردهای *Telcordia* [2]

عنوان	شرح
Telcordia-GR-63-CORE	شامل نیازمندی‌های عمومی برای میزان فضای موردنیاز و معیارهای زیست‌محیطی همه تجهیزات مخابراتی مورداستفاده است.
Telcordia-GR-139	شامل الزامات استفاده از کابل هم‌محور[1] است و هنگام استفاده از آن ممکن است به استانداردهای *GR-492*، *GR-1398*، *GR-63* و *GR-137* نیاز پیدا کنید.

2-6. استانداردها و معیارهای امنیت نرم‌افزار

نگرانی‌های امنیتی در حوزه شبکه و نرم‌افزار بخش عمده‌ای از نگرانی‌های سازمان‌ها را تشکیل می‌دهد. برای تأمین امنیت شبکه فعالیت‌های زیادی انجام‌شده است؛ اما بحث امنیت نرم‌افزار مغفول مانده و کمتر به آن توجه شده است. برای بررسی آسیب‌پذیری‌ها و به لحاظ حوزه‌ای با چشم‌پوشی از بعضی جزئیات می‌توان انواع حملات نفوذ را در بخش‌های ذیل دسته‌بندی نمود:

- معماری شبکه، سرویس‌ها و تجهیزات (پیکربندی سوئیچ‌ها، مسیریاب‌ها، *DNS*[2] و غیره)
- نرم‌افزارهای وب میزبان و سیستم‌عامل (*APACHE, IIS, WINDOWS, LINUX* و غیره)
- سکو وب/ فنّاوری توسعه (*PHP, Java EE,.NET* و غیره)
- کامپیوتر میزبان پایگاه داده و انباره اطلاعات (*MySQL, MS-SQL, ORACLE, SYBASE* و غیره)
- برنامه‌ها و کاربردهای وب (*Portal, Website, Web Service, Blog, Forum* و غیره)
- کاربران و سرویس‌گیرندگان (*Client App, Browser, Mobile App* و غیره)

بر اساس گزارش مؤسسه تحقیقات گارتنر، 75٪ از حملات نفوذ امنیتی به برنامه‌ها و کاربردهای وب و 25٪ مابقی روی سایر حوزه‌های ذکرشده در بالا متمرکز بوده است. این در حالی است که فقط 10% از سرمایه‌گذاری برای ایجاد امنیت در خصوص برنامه‌ها و کاربردهای وب انجام می‌شود و 90% سرمایه‌گذاری در بخش ایجاد تمهیدات امنیتی سایر حوزه‌ها به‌ویژه امنیت شبکه انجام می‌شود. ازآنجاکه یکی از خدمات عمده مراکز داده، میزبانی نرم‌افزارهای تحت وب است، امنیت نرم‌افزارها برای این مراکز اهمیت ویژه‌ای می‌یابد؛ لذا در جدول (5) مروری خواهیم داشت بر استانداردهایی که برای ارزیابی امنیت نرم‌افزارها تدوین‌شده‌اند.

2-6-1. استاندارد NIST[3] SAMATE[4]

استاندارد *SAMATE* توسط مؤسسه *NIST* تدوین‌شده است. مجموعه‌ای از روش‌ها و فرایندها برای جلوگیری، کاهش یا حذف ضعف‌ها و آسیب‌پذیری‌ها و حصول اطمینان از عملکرد صحیح نرم‌افزار است.

2-6-2. استانداردهای OWASP[5]

مؤسسه غیرانتفاعی *OWASP* یک متدولوژی در زمینه امنیت نرم‌افزارهای تحت وب ارائه کرده که متشکل از نه زیر پروژه است که هرکدام به‌صورت جداگانه در خصوص یکی از موارد مرتبط با امنیت حوزه نرم‌افزارهای تحت وب فعالیت می‌کنند. این زیر پروژه‌ها در جدول (5) ارائه‌شده است:

جدول (5). استانداردهای *OWASP*

عنوان	شرح
OWASP Application Security Verification Standard (ASVS)	طبق این استاندارد یک سری آزمون‌های امنیتی بر روی نرم‌افزار از قبیل *Cross Site Scripting* و *SQL Injection* انجام می‌شود.
OWASP XML Security Gateway (XSG)	استانداردی است که برای برقراری امنیت در ساختار *XML* استفاده می‌شود.
OWASP Development Guide	شامل یک سری نمونه کدهای کاربردی و تمثیلی از زبان‌های برنامه‌نویسی مانند *J2EE* و *ASP.NET* و *PHP* است.

[1] *Coaxial*
[2] *Domain Name System*
[3] *National Institute of Standards and Technology*
[4] *Software Assurance Metrics and Tool Evaluation*
[5] *Open Web Application Security Project*

OWASP Testing Guide	راهنمایی برای تست و آزمون گرفتن از نرم‌افزارهای کاربردی تحت وب است.
OWASP Code Review Guide	راهنمایی برای مرور کدهای نوشته‌شده و مستندسازی آن‌ها است تا برنامه‌نویس بتواند پس از نوشتن یا توسعه نرم‌افزار کاربردی وب خود، آن را آزمایش کرده و نقاط ضعف در کدهای نوشته‌شده را برطرف کند.
OWASP ZAP Project	برای انجام تست‌های نفوذ به نرم‌افزارهای کاربردی تحت وب مورداستفاده قرار می‌گیرد.
OWASP Top Ten	هدف از این پروژه اطلاع‌رسانی در خصوص مشکلات امنیتی نرم‌افزارهای تحت وب و هشدار دهی به سازمان‌ها در خصوص امنیت برنامه‌های تحت وب است.
OWASP Software Assurance Maturity Model (SAM)	این پروژه یک راهنما برای سازمان‌ها است تا بتوانند یک چارچوب درست و تحلیل امنیتی برای نرم‌افزارهای تحت وب خود ایجاد کنند.
Webgoat	این پروژه یک نرم‌افزار کاربردی تحت وب است که تمامی نقاط ضعفی که تابه‌حال توسط *OWASP* شناخته‌شده‌اند را به‌صورت مجازی و در قالب یک محیط برنامه‌نویسی شده شبیه‌سازی کرده و در اختیار برنامه‌نویسان قرار می‌دهد.

2-6-3. استاندارد ISO/IEC 12207

یک استاندارد بین‌المللی برای مهندسی نرم‌افزار است که در آن فعالیت‌های مرتبط با چرخه حیات نرم‌افزار از ابتدا تا انتها مشخص‌شده است. این استاندارد در طول حیات نرم‌افزار به بررسی خطاها و مشکلات امنیتی پرداخته و باهدف ارائه یک ساختار از بالا به پایین در هر سطح، کارها را به اجزای کوچک‌تر تقسیم می‌کند. این امر باعث آسان‌تر شدن فرایند تولید نرم‌افزار از جنبه‌های امنیتی است.

2-6-4. استاندارد CERT[1] Secure Coding Standard

این استاندارد یک سری از قوانین و پیشنهادها را برای کد نویسی امن با زبان‌های برنامه‌نویسی *C* ، *C++* و *Java* ارائه می‌دهد. هدف از این قوانین و پیشنهادها، حذف عادت‌های کد نویسی ناامن و رفتارهای تعریف‌نشده است که منجر به آسیب‌پذیری‌های قابل سوءاستفاده می‌شود [5].

2-6-5. استاندارد PCI[2] Data Security Standard

این استاندارد، استاندارد ایمنی صنعت کارت پرداخت و استاندارد امنیت اطلاعات است که برای سازمان‌هایی که با اطلاعات دارندگان کارت‌های دستگاه پایانه فروش، خودپرداز، کیف پول الکترونیک[3]، پیش‌پرداخت شده[4]، اعتباری و نقدی سروکار دارند طراحی‌شده است.

[1] *Computer Emergency Response Team*
[2] *Payment Card Industry*
[3] *E-purse*
[4] *Prepaid*

۳. پیشینه پژوهش

در پژوهشی با موضوع ارزیابی بلوغ امنیتی مراکز داده، به ارائه روشی پرداخته‌شده که بر اساس آن مهندسین امنیتی می‌توانند مسائل امنیتی را شناسایی کنند، بلوغ امنیتی را مشخص سازند و سیاست‌های جدید جهت بهبود پیکربندی‌های امنیتی مراکز داده پیشنهاد کنند. این مقاله بر روی استانداردهای بین‌المللی *ISO 27002* و *NIST SP 800-53* تمرکز کرده است. در این مقاله سطح بلوغ امنیتی مراکز داده مطابق جدول (6) دسته‌بندی‌شده است که شامل مقیاس عددی، نام‌گذاری سطح بلوغ و درصد لحاظ کردن کنترل‌های امنیتی است.

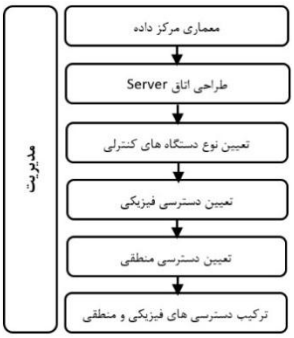
جدول (6). سطوح بلوغ امنیتی مرکز داده [7]

سطح بلوغ	درجه پیاده‌سازی	کنترل‌های موردتوجه
0	مدیریت نشده	0-19 درصد
1	مدیریت اولیه	20-39 درصد
2	مدیریت جزئی	40-59 درصد
3	مدیریت گسترده	60-79 درصد
4	مدیریت کامل	80-100 درصد

این مقاله یک روش برای ارزیابی سطح بلوغ امنیت مراکز داده را در یک زمینه کلی‌تر ارائه کرده است که شامل دورویه ارزیابی جدید است: اول تحلیل وزن‌دار که به کنترل‌های امنیتی بالاتر که هم‌زمان در استانداردهای بیشتری وجود دارند، وزن می‌دهد. دوم تحلیل زمینه‌ای که مشابه تحلیل وزن‌دار است، اما به سطح اهمیتی که سازمان به هر کنترل امنیتی تخصیص داده است، حساس است. این مقاله شامل مطالعه موردی یک شرکت برای ارزیابی مزایای متدولوژی پیشنهادی در دنیای واقعی است. سازمان بررسی‌شده یک زنجیره غذای آماده است که در 19 کشور و پنج قاره حضور دارد. ارزیابی بلوغ شامل 30 کنترل امنیتی در رابطه با امنیت سیستم‌عامل کامپیوتر میزبان از استانداردهای *ISO 27002* و *NIST 800-53* است. در تحلیل سنتی سازمان از کل 120 امتیاز، 42 امتیاز را به دست آورده است (35٪). این نشان‌دهنده سطح بلوغ یک یعنی مدیریت اولیه است. تحلیل وزن‌دار نشان‌دهنده مطابقت 39٪ با استانداردهاست که مجدداً نشان‌دهنده سطح بلوغ یک یعنی مدیریت اولیه است. افزایش سطح بلوغ زمانی مهم است که با تحلیل سنتی مقایسه می‌شود. این نتیجه نشان می‌دهد که شرکت با کنترل‌های مشترک موجود در استانداردهای امنیتی بین‌المللی مطابقت دارد. تحلیل زمینه‌ای نتایج نشان‌دهنده مقدار 40٪ است که به سطح بلوغ مشابه تحلیل وزن‌دار رسیده است. افزایش یک‌درصدی به خاطر اهمیت کنترل‌های امنیتی ازنظر شرکت است. این به معنی سطح بلوغ دو یعنی مدیریت جزئی است [7].

در پایان‌نامه‌ای درباره تأمین امنیت در دسترسی فیزیکی به مراکز داده، رویکردی برای کنترل دسترسی فیزیکی به مراکز داده با استفاده از فناوری *RFID*[1] ارائه‌شده که بر اساس تعیین سطوح امنیتی مناطق، تجهیزات شبکه و سایر پارامترهای موجود در مراکز داده، دسترسی‌های منطقی و فیزیکی را ترکیب کرده و علاوه برافزایش امنیت، تأثیر زیادی بر قابلیت اطمینان و دسترس‌پذیری مراکز داده می‌گذارد. در این پایان‌نامه با بررسی اسناد، کتب و مقاله‌های مرتبط، پارامترهای امنیتی و مسائل کلیدی در مرکز داده بر اساس سیستم *ISMS*[2] و استاندارد *ISO 27001* شناسایی‌شده و پس از بررسی و تحلیل، راهکارهایی برای افزایش امنیت در لایه زیرساخت ارائه گردیده است. همچنین رویکردی برای چگونگی احراز هویت، ردیابی و پیگیری منابع در مرکز داده با استفاده از فناوری رادیو شناسه ارائه‌شده است. در انتها رویکرد پیشنهادی با نرم‌افزار *Enterprise Dynamic* شبیه‌سازی‌شده است. این رویکرد کاهش هزینه‌ها، خودکارسازی، کاهش خطا، کنترل فرایندهای غیرقابل‌مشاهده، امکان به‌روزرسانی برچسب‌ها بدون دخالت دست و امنیت و یکپارچگی را به دنبال دارد. نتایج شبیه‌سازی رویکرد پیشنهادی نشان می‌دهد سرعت پیگیری منابع و تجهیزات در مرکز داده مدنظر حدود 15 برابر افزایش‌یافته است [8].

در مقاله‌ای با موضوع یکپارچه‌سازی دسترسی فیزیکی و منطقی در مرکز داده، برای امنیت مرکز داده دو جنبه اصلی امنیت فیزیکی و امنیت منطقی در نظر گرفته‌شده است. در این مقاله مدلی ارائه‌شده تا باعث بالا رفتن ضریب امنیتی سه پارامتر قابلیت اطمینان، دسترس‌پذیری و یکپارچگی شود. آنچه در این مدل اهمیت دارد همپوشانی سه عنصر کنترلی فیزیکی، منطقی و مدیریت آن‌هاست. تصویر مدل پیشنهادی در شکل (2) نشان داده‌شده است:



شکل (2). مدل پیشنهادی در یک پژوهش برای کنترل دسترسی به مرکز داده [9]

همان‌طور که دیده می‌شود، در این مدل دسترسی‌های فیزیکی و منطقی باهم ترکیب‌شده و کنترل‌های مدیریتی در تمام لایه‌های انجام می‌گردد. این مدل در دانشگاه آزاد اسلامی شهر مجلسی پیاده‌سازی و اثرات آن موردبررسی قرار گرفت. پیش از پیاده‌سازی، کلیه مراکز داده غیرمتمرکز دانشگاه، یکی شدند. این مدل با طراحی یک نرم‌افزار، مورد پایش و بررسی قرارگرفته است. نتایج بررسی‌ها نشان می‌دهد که پس از پیاده‌سازی این مدل میزان قطعی سامانه‌ها به 48 ساعت در سال رسید [9].

در مقاله‌ای با موضوع طراحی ساختار پشتیبان پیمانه‌ای برای مراکز داده ملی، یک ساختار برای پشتیبانی از مراکز داده ارائه‌شده که بر اساس آن چندین مرکز داده ملی، کار پشتیبانی از سایر مراکز داده کشور را انجام خواهند داد. در این ساختار اطلاعات به‌طور هم‌زمان در مراکز داده محلی و مراکز داده ملی پشتیبان ذخیره می‌شود؛ بنابراین در صورت بروز مشکل و خرابی، سرویس‌های مرکز داده از کار نخواهد افتاد. در این طرح مراکز داده ملی به‌صورت کانتینری طراحی خواهند شد. این طرح شامل پنج مرکز داده ملی پشتیبان است که در پنج منطقه مناسب جغرافیایی کشور توزیع‌شده‌اند و مراکز داده معمولی متقاضی در هر یک از این پنج منطقه توسط یکی از این مراکز داده ملی پشتیبان، پشتیبانی خواهند شد و درنهایت مراکز داده ملی پشتیبان به هم متصل خواهند شد. مدیریت کلان فنی مراکز داده ملی نیز در مرکز داده ملی مستقر در تهران صورت خواهد گرفت و دو مرکز واقع در تهران و اصفهان به‌صورت پشتیبان همدیگر عمل خواهند کرد [10].

در مقاله‌ای با موضوع رتبه‌بندی مخاطرات امنیت اطلاعات، روشی کاربردی بر اساس تلفیق دو روش تصمیم‌گیری چند شاخصه فرایند تحلیل سلسله‌مراتبی و تاپسیس[3]، در محیط فازی، ارائه‌شده که باعث بهبود رتبه‌بندی مخاطرات امنیت اطلاعات می‌گردد. مدیریت مخاطرات به مدیران کمک می‌کند تا امنیت سامانه‌ها و اطلاعات خود را کنترل کنند. در این مقاله ابتدا مخاطرات امنیتی یک سازمان با روش تصمیم‌گیری چند شاخصه فرایند سلسله‌مراتبی فازی رتبه‌بندی شده و سپس از ترکیب روش تاپسیس برای رتبه‌بندی بهتر و دقیق‌تر استفاده‌شده است. نتایج حاصل از پیاده‌سازی مدل تلفیقی فرایند تحلیل سلسله‌مراتبی فازی - تاپسیس در مقایسه با مدل فرایند تحلیل سلسله‌مراتبی فازی نشان می‌دهد که وزن‌های حاصل از مدل پیشنهادی دارای ضریب تغییرات کمتر و میانگین بیشتر نسبت به روش *FAHP* است و درنتیجه نتایج دقیق‌تر و با درصد خطای کمتر را جهت رتبه‌بندی مخاطرات ارائه می‌دهد [11].

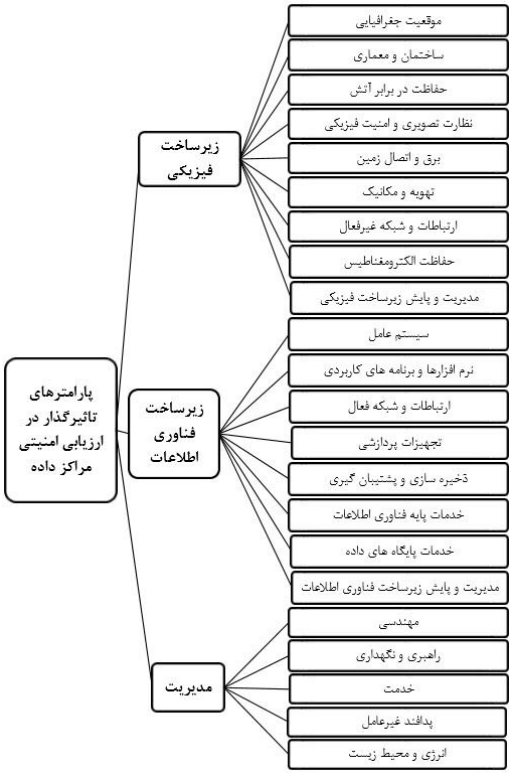
[1] *Radio-frequency identification*
[2] *Information Security Management System*
[3] *Technique for Order Performance by Similarity to Ideal Solution (TOPSIS)*

در مقاله‌ای با موضوع ارزیابی کمی مخاطره امنیتی در سامانه‌های سایبر-فیزیکی، روشی برای ارزیابی ارائه‌شده که در آن مؤلفه‌هایی چون دانش مهاجم، زمان تا خرابی سیستم، هزینه بازیابی بعد از وقوع حمله موفق، امکان حمله، امکان تشخیص حمله، خسارات وارده به دارایی‌های سیستم، هزینه‌ترمیم سامانه و نرخ آسیب‌پذیری در نظر گرفته‌شده است. نهایتاً به‌منظور نمایش کاربردپذیری، روش پیشنهادی بر یک سیستم سایبر-فیزیکی اعمال‌شده و مخاطره امنیتی ارزیابی‌شده است [12].

در مقاله‌ای با موضوع ارزیابی سلامت سیستم حفاظت از امنیت مراکز داده، امنیت این مراکز در سه لایه برنامه‌های کاربردی، لایه مجازی‌سازی و لایه زیرساخت، تجزیه‌وتحلیل شده و یک روش ارزیابی سلامت نسبتاً جامع در پنج سطح پیشنهاد می‌گردد که به بهبود مستمر قابلیت‌های حفاظت امنیتی مراکز داده کمک می‌کند [13].

۴. مدل سلسله‌مراتبی پژوهش

پس از مطالعه مقالات اجلاس‌ها، مقالات مجلات، پایان‌نامه‌های کارشناسی ارشد، استانداردهای بین‌المللی، اسناد ملی، کتاب‌ها و سایت‌های اینترنتی مرتبط، مدل مفهومی پژوهش به دست آمد که در آن شاخص‌های ارزیابی امنیتی مراکز داده جمع‌بندی شده و در شکل (3) قابل‌مشاهده است:



شکل (3). مدل سلسله‌مراتبی پژوهش

۵. روش پژوهش و تحلیل داده‌ها

تحقیق حاضر ازلحاظ هدف، تحقیقی کاربری محسوب می‌شود. ازنظر گردآوری اطلاعات، در بخش شناسایی پارامترهای تأثیرگذار در ارزیابی امنیتی مراکز داده، از نوع کتابخانه‌ای است. اما در بخش رتبه‌بندی پارامترها، از نوع تحقیقات میدانی به شمار می‌رود، چون از پرسش‌نامه برای جمع‌آوری داده‌های آن استفاده‌شده است. جامعه آماری صاحب‌نظران و کارشناسان فناوری اطلاعات شهرداری رشت هستند که به‌نوعی با مراکز داده ارتباط داشته و کارکرده‌اند. هدف نهایی، شناسایی و رتبه‌بندی پارامترهای تأثیرگذار در ارزیابی امنیتی مراکز داده است. ازآنجاکه اکثر سازمان‌ها برای بحث امنیت بودجه محدودی دارند، رتبه‌بندی شاخص‌های امنیتی کمک می‌کند بتوان بر اساس اولویت‌ها نسبت به خرید تجهیزات و پیاده‌سازی امنیت اقدام نمود.

5-1. روش‌های تصمیم‌گیری چند شاخصه

با توجه به این‌که امنیت ابعاد مختلفی دارد، برای ارزیابی آن باید از روش‌های تصمیم‌گیری چند شاخصه استفاده کرد. این روش‌ها اجازه می‌دهد طیفی از شاخص‌های وابسته به یک مبحث، امتیازدهی و وزن دهی شده و سپس رتبه‌بندی شوند و به دودسته کلی مدل غیر جبرانی و مدل جبرانی تقسیم می‌شوند. مدل غیر جبرانی شامل روش‌هایی است که مبادله بین شاخص‌ها مجاز نیست؛ یعنی نقطه‌ضعف موجود در یک شاخص توسط مزیت موجود در شاخص دیگر جبران نمی‌شود. مزیت روش‌های این مدل، سادگی آن‌هاست که با رفتار تصمیم‌گیرنده و محدود بودن اطلاعات او مطابقت دارد [11]. ازجمله این روش‌ها پرموتاسیون[۱]، لکسیکوگراف[۲]، رضایت‌بخش[۳]، ماکسی ماکس[۴]، ماکسی مین[۵]، و تسلط[۶] است. اما بیشتر مدل‌های تصمیم‌گیری چند شاخصه در دسته مدل‌های جبرانی قرار می‌گیرند. ازجمله این روش‌ها فرایند تحلیل سلسله‌مراتبی[۷]، فرایند تحلیل شبکه‌ای[۸]، روش بهترین بدترین[۹]، روش تحلیل نسبت ارزیابی وزن دهی تدریجی[۱۰]، روش شباهت به گزینه ایدئال[۱۱]، روش ویکور[۱۲]، روش

[1] *Permutation*
[2] *Lexicographic*
[3] *Satisfying method*
[4] *MaxiMax*
[5] *MaxiMin*
[6] *Dominance*
[7] *Analytical Hierarchy process (AHP)*
[8] *Analytical Network Process (ANP)*
[9] *Best-Worst Multi-criteria*
[10] *Step-Wise Weight Assessment Ratio Analysis (SWARA)*
[11] *Technique for Order Performance by Similarity to Ideal Solution (TOPSIS)*
[12] *VICOR*

وزن دهی افزایشی ساده[1] و روش انتخاب حذفی در ترجمه به واقعیت[2] است[14].

فرایند تحلیل سلسله‌مراتبی یکی از معروف‌ترین فنون تصمیم‌گیری چند شاخصه است که منعکس‌کننده رفتار طبیعی و تفکر انسانی است. این روش، مسائل پیچیده را بر اساس آثار متقابل آن‌ها موردبررسی قرار می‌دهد و آن‌ها را به شکلی ساده تبدیل کرده و به حل آن می‌پردازد. از طرفی برای رفع عدم قطعیتی که در قضاوت‌های انسانی وجود دارد، روش‌های تصمیم‌گیری چند شاخصه با منطق فازی ترکیب می‌شود. منطق فازی روشی است که با کمک آن می‌توان نتایج دقیق را با استفاده از دانش و مقادیر کلامی افراد خبره استخراج کرد. درروش فازی، خبرگان در قضاوت‌هایشان به‌جای یک عدد ثابت، یک بازه را اعلام می‌کنند. بر همین اساس در مرحله بعد برای رتبه‌بندی عوامل شناسایی‌شده، از روش فرایند تحلیل سلسله‌مراتبی فازی یا $FAHP$ استفاده شد.

5-2. مطالعه موردی

برای جمع‌آوری اطلاعات، پرسش‌نامه مقایسات زوجی در دو حوزه زیرساخت فیزیکی و زیرساخت فناوری اطلاعات تهیه‌شده و در اختیار خبرگان فناوری اطلاعات قرار گرفت. جامعه آماری این پژوهش، خبرگان حوزه فناوری اطلاعات در شهرداری رشت هستند که به‌نوعی با مراکز داده کارکرده‌اند و با چالش‌های امنیتی آن درگیر هستند. از میان کارکنان شهرداری رشت 11 نفر از خبرگان حوزه فناوری اطلاعات برای پاسخ به سؤالات انتخاب‌شده‌اند.

جدول (7) فراوانی نمونه را برحسب جنسیت آن‌ها نشان می‌دهد که 54/5 درصد مرد و 45/5 درصد آنان زن هستند.

جدول (7). توزیع فراوانی نمونه برحسب جنسیت

جنسیت	فراوانی	درصد
مرد	6	54/5
زن	5	45/5
مجموع	11	100

جدول (8). توزیع فراوانی نمونه برحسب سن

سن	فراوانی	درصد
کمتر از 25 سال	0	0
بین 26 تا 35 سال	7	63/6
بین 36 تا 45 سال	4	36/4
بیش از 46 سال	0	0
مجموع	11	100

جدول (8) نشان می‌دهد 63/6 درصد از نمونه‌ها بین سنین 26 تا 35 سال و 36/4 درصد بین 36 تا 45 سال قرار دارند.

جدول (9) نشان می‌دهد ازنظر تحصیلات 18/2 درصد نمونه‌ها لیسانس و 81/8 درصد فوق‌لیسانس و بالاتر هستند.

جدول (9). توزیع فراوانی نمونه برحسب تحصیلات

تحصیلات	فراوانی	درصد
دیپلم	0	0
فوق‌دیپلم	0	0
لیسانس	2	18/2
فوق‌لیسانس و بالاتر	9	81/8
مجموع	11	100

جدول (10) نشان می‌دهد ازنظر سابقه کار 63/6 درصد نمونه‌ها بین 6 تا 10 سال و 36/4 درصد بین 11 تا 20 سال سابقه کاردارند.

جدول (10). توزیع فراوانی نمونه برحسب سابقه کار

سابقه کار	فراوانی	درصد
کمتر از 5 سال	0	0
بین 6 تا 10 سال	7	63/6
بین 11 تا 20 سال	4	36/4
بیش از 21 سال	0	0
مجموع	11	100

5-3. پرسش‌نامه

در این پژوهش پارامترهای تأثیرگذار در ارزیابی امنیتی در سه حوزه زیرساخت فیزیکی، زیرساخت فناوری اطلاعات و مدیریت موردبررسی قرار گرفت. حوزه زیرساخت فیزیکی شامل نه شاخص موقعیت جغرافیایی، ساختمان و معماری، حفاظت در برابر آتش، نظارت تصویری و امنیت فیزیکی، برق و اتصال زمین، تهویه و مکانیک، ارتباطات و شبکه غیرفعال، حفاظت الکترومغناطیس و مدیریت و پایش زیرساخت فیزیکی است. حوزه زیرساخت فناوری اطلاعات شامل هشت شاخص سیستم‌عامل، نرم‌افزارها و برنامه‌های کاربردی، ارتباطات و شبکه فعال، تجهیزات پردازشی، ذخیره‌سازی و پشتیبان گیری، خدمات پایه فناوری اطلاعات، خدمات پایگاه‌های داده و مدیریت و پایش زیرساخت فناوری اطلاعات است. حوزه مدیریت نیز شش شاخص مهندسی، راهبری و نگهداری، خدمت، امنیت، پدافند غیرعامل و انرژی و محیط‌زیست را شامل می‌شود. برای رتبه‌بندی شاخص‌ها از ابزار پرسش‌نامه استفاده گردید. پرسش‌نامه برای دو حوزه طراحی‌شده است و در درجه اول حوزه زیرساخت فیزیکی و زیرساخت فناوری اطلاعات را اولویت‌بندی می‌کند و سپس شاخص‌های این دو حوزه را باهم مقایسه می‌نماید.

[1] *Simple Additive Weighting (SAW)*
[2] *Elimination et Choice in Translating to Reality (ELECTRE)*

5-4. روایی و پایایی پرسش‌نامه

منظور از پایایی یک پرسش‌نامه این است که اگر خصیصه موردسنجش را با همان پرسش‌نامه و در شرایط مشابه، مجدداً اندازه‌گیری کنیم، نتایج تا چه اندازه مشابه به دست می‌آید. به‌عبارت‌دیگر این پرسش‌نامه تا چه میزان، قابل‌اعتماد است و می‌توان آن را در موارد متعدد به کاربرد و نتایج یکسان گرفت. پایایی مربوط به ثبات است، یعنی حصول یک نتیجه به‌طور مکرر. درروش *FAHP*، شاخصی به نام نرخ ناسازگاری توسط نرم‌افزار محاسبه و اعلام می‌گردد که برای بررسی مفهوم پایایی استفاده می‌شود. این شاخص به‌گونه‌ای طراحی‌شده است که در صورت ناسازگار و متناقض بودن پاسخ‌های خبرگان، این مسئله خود را نشان خواهد داد و بدین ترتیب نامناسب بودن پرسش‌نامه و پاسخ‌ها مشخص می‌شود و در حالتی که ناسازگاری از حدنصاب اعلام‌شده (ده درصد) بیشتر باشد، لازم است ارزیابی‌ها مجدد انجام گردد.

روایی پرسشنامه دلالت بر این دارد که پرسش‌نامه تا چه حد گویا و واضح است و دقیقاً همان موضوع و مطلبی را که مدنظر است، اندازه‌گیری می‌نماید. با توجه به اینکه پرسش‌نامه روش *FAHP* به تأیید خبرگان موضوع می‌رسد، لذا روایی آن مورد تأیید است.

۶. نتایج و بحث

در مرحله اول فرایند *FAHP* برای دو گروه اصلی زیرساخت فیزیکی و زیرساخت فناوری اطلاعات که در مدل سلسله‌مراتبی پژوهش به شاخص‌های آن اشاره‌شده، انجام گردید تا اولویت آن‌ها نسبت به هم مشخص شود. در جدول (11)، فراوانی پاسخ‌ها بر اساس نظر خبرگان در مقایسات زوجی اولیه بر اساس اولویت‌های تعریف‌شده مشخص‌شده است که در آن معادل عبارت‌های انگلیسی عبارت‌اند از: زیرساخت فناوری اطلاعات (*A*) و زیرساخت فیزیکی (*B*).

جدول (11). ماتریس مقایسات زوجی گروه‌های اصلی

تعداد خبرگان		معیار راست با اولویت‌تر است.					معیار چپ با اولویت‌تر است.				
		اولویت کاملاً زیاد	اولویت بسیار زیاد	اولویت زیاد	اولویت متوسط	اولویت یکسان	اولویت متوسط	اولویت زیاد	اولویت بسیار زیاد	اولویت کاملاً زیاد	
11	*A*	1		1		3		1		1	*B*

باتوجه‌به اعداد ماتریس فوق، ماتریس مقایسات فازی ادغام‌شده به شرح جدول (12) خواهد بود. این جدول حاصل ادغام مقایسات زوجی بر اساس مقایسات زوجی اولیه درروش تحلیل سلسله‌مراتبی فازی با رویکرد چانگ است.

جدول (12). ماتریس مقایسات فازی ادغام‌شده

	A			*B*		
A	1	1	1	1/23	1/55	1/85
B	0/53	0/64	0/80	1	1	1

در مرحله بعد، ابتدا بایستی مجموع سطری هرکدام از سطرهای جدول فوق محاسبه شود. پس‌ازآن، معکوسِ مجموع سطرها، در هرکدام از مجموع سطرهای جدول فوق ضرب می‌شود. همچنین در این مرحله، درجه بزرگی هر معیار نسبت به معیارهای دیگر محاسبه می‌گردد. سپس درجه ارجحیت، نرمال‌سازی ارجحیت‌ها و وزن معیارها محاسبه می‌شود که جدول (13) توضیحات بالا را نشان داده است:

جدول (13). محاسبات *FAHP* برای گروه‌های اصلی

معیارها	وزن معیارها	نرمال‌سازی ارجحیت‌ها	درجه ارجحیت	درجه ارجحیت *Si* بر *Sk*	بسط مرکب فازی			جمع فازی هر سطر		
A	1	1	1	1	0/75	0/60	0/48	2/85	2/55	2/23
B	0	0	0	0	0/47	0/39	0/33	1/80	1/64	1/53

در مرحله دوم فرایند *FAHP* برای زیرمعیارهای زیرساخت فیزیکی انجام شد تا اولویت آن‌ها نسبت به هم مشخص شود. جدول (14)، فراوانی پاسخ‌ها بر اساس نظر خبرگان در مقایسات زوجی اولیه را نشان می‌دهد که در آن معادل عبارت‌های انگلیسی عبارت‌اند از: موقعیت جغرافیایی (*A*)، ساختمان و معماری (*B*)، حفاظت در برابر آتش (*C*)، نظارت تصویری و امنیت فیزیکی (*D*)، برق و اتصال زمین (*E*)، تهویه و مکانیک (*F*)، ارتباطات و شبکه غیرفعال (*G*)، حفاظت الکترومغناطیس (*H*)، مدیریت و پایش زیرساخت فیزیکی (*I*).

جدول (14). ماتریس مقایسات زوجی اولیه زیرساخت فیزیکی

تعداد خبرگان		معیار راست با اولویت‌تر است.					معیار چپ با اولویت‌تر است.				
		اولویت کاملاً زیاد	اولویت بسیار زیاد	اولویت زیاد	اولویت متوسط	اولویت یکسان	اولویت متوسط	اولویت زیاد	اولویت بسیار زیاد	اولویت کاملاً زیاد	
11	*A*	1		1	4	3	1		1		*B*
11	*A*							2		6	*C*
11	*A*	2		2	2			1		2	*D*
11	*A*			2	1	2	1	1		3	*E*
1	*A*	1		1	1			2		3	*F*

											1
G	2	3	1	1	2			1	1	*A*	**1 1**
H	1	2	3	1	4					*A*	**1 1**
I	1	3	2	1	1	1		1	1	*A*	**1 1**
C	3	2		1	1		2	1	1	*B*	**1 1**
D	1	3	1	2			1		3	*B*	**1 1**
E	3	2	1	1	1	1	1		1	*B*	**1 1**
F	1	1	4	1		1	1	1	1	*B*	**1 1**
G	3	2	1	2			2		1	*B*	**1 1**
H	1	1	4	1	1		1	2		*B*	**1 1**
I	1	3	2	2		1			2	*B*	**1 1**
D					2	1	1	1	6	*C*	**1 1**
E	1		1		3	1	3		2	*C*	**1 1**
F		1	1		2		4	2	1	*C*	**1 1**
G	2					3	1	3	2	*C*	**1 1**
H	1		1	1	1	3	2	1	1	*C*	**1 1**
I	1	1			2	2	2		3	*C*	**1 1**
E	4				3	1	1	1	1	*D*	**1 1**
F	2	1		2	1	2	1	1	1	*D*	**1 1**
G	1		3	1	1	1	2	1	1	*D*	**1 1**
H	1	1			4	3	1	1		*D*	**1 1**
I	1	2		1	4	1			2	*D*	**1 1**
F		1			3		1	2	4	*E*	**1 1**
G		1		2	1	3	2	1	1	*E*	**1 1**
H		2		1	2	3	1	1	1	*E*	**1 1**
I	1	1			3	3	1	2		*E*	**1 1**
G	1	1		2	2	1	1	2	1	*F*	**1 1**
H	1	1	1	1	2	2		3		*F*	**1 1**
I		2		4	1		2	1	1	*F*	**1 1**
H	2		1	1	2	2	1		2	*G*	**1 1**
I	2	2			1	2		3	1	*G*	**1 1**
I	1	1	1		5		1		2	*H*	**1 1**

مراحل بعدی مشابه محاسبات گروه‌های اصلی انجام شد که نتیجه نهایی به شرح جدول (15) است:

جدول (15). محاسبات *FAHP* برای زیرساخت فیزیکی

معیارها	اولویت	وزن معیارها
موقعیت جغرافیایی (*A*)	3	0/000
ساختمان و معماری (*B*)	3	0/000
حفاظت در برابر آتش (*C*)	1	0/777
نظارت تصویری و امنیت فیزیکی (*D*)	3	0/000
برق و اتصال زمین (*E*)	2	0/223
تهویه و مکانیک (*F*)	3	0/000
ارتباطات و شبکه غیرفعال (*G*)	3	0/000
حفاظت الکترومغناطیس (*H*)	3	0/000
مدیریت و پایش زیرساخت فیزیکی (*I*)	3	0/000

جدول (16). ماتریس مقایسات زوجی زیرساخت فناوری اطلاعات

		معیار راست با اولویت‌تر است.					**معیار چپ با اولویت‌تر است.**					
تعداد خبرگان		اولویت کاملاً زیاد	اولویت بسیار زیاد	اولویت زیاد	اولویت متوسط	اولویت یکسان	اولویت متوسط	اولویت زیاد	اولویت بسیار زیاد	اولویت کاملاً زیاد		
1 1	*A*	2	1		2		2		2	1	2	*B*
1 1	*A*		1	1		1		1	2	2	4	*C*
1 1	*A*		1			2			1	4	1	*D*
1 1	*A*		1		1		1		2	1	1	*E*
1 1	*A*	1	2		2		1			2	3	*F*
1 1	*A*		1	1	1	2	1	1	1	2	2	*G*
1 1	*A*		1		3	1			1	2	2	*H*
1 1	*B*	1	1	2			2	2	1	1	3	*C*
1 1	*B*		1		3	1	2		1		3	*D*
1 1	*B*		1		1		1		2		4	*E*
1 1	*B*	1	1	1		3	1	1				*F*
1 1	*B*		1	1		2	1	1	1		2	*G*
1 1	*B*		1		2	1	1		1	2	2	*H*
1 1	*C*	2			1	2	1	1			3	*D*
1 1	*C*	2		1		2	1		1	2	3	*E*
1 1	*C*	2			1	2	2		1	3	3	*F*
1 1	*C*	2	1		2	1	2	2	1	1	2	*G*
1 1	*C*	2	1		2	1	2	2	1	1	2	*H*
1 1	*C*		1		2	1	2	2	1	1	2	*I*
1 1	*D*	2	1		1	2	1	1	1	3	3	*E*
1 1	*D*		1		2	1	2	2	1	1	3	*F*
1 1	*D*		1		2	1	2	2	1	1	3	*G*
1 1	*D*		1		2	1	2	2	1	1	3	*H*
1 1	*D*		1		2	1	2	2	1	1	3	*I*
1 1	*E*		1		2	1	2	2	1	1	3	*F*
1 1	*E*		1		2	1	2	2	1	1	3	*G*
1 1	*E*		1		2	1	2	2	1	1	3	*H*
1 1	*E*		1		2	1	2	2	1	1	3	*I*
1 1	*F*		1		2	1	2	2	1	1	3	*G*
1 1	*F*		1		2	1	2	2	1	1	3	*H*
1 1	*F*		1		2	1	2	2	1	1	3	*I*
1 1	*G*		1		2	1	2	2	1	1	3	*H*
1 1	*G*		1		2	1	2	2	1	1	3	*I*
1 1	*H*		1		2	1	2	2	1	1	3	*I*

11	C	1		1				1	5	1	1	2	H
11	D	1		1	2	2			3	3		2	E
11	D	1	1	2	1		3	2		1	2	1	F
11	D	1	1	3		3		1	3	1		1	G
11	D	2	1	2	2	1		2	1	2		2	H
11	E	2	2	3			1	2		1		1	F
11	E	2	2	3			1	2	1	1		1	G
11	E	1	1	2	2	2	1	1	1	2	1	1	H
11	F			1	6			1		3			G
11	F	1	1	3	3			1	1	1	1	1	H
11	G	1		1	3	1		1		2	2	1	H

در مرحله سوم فرایند *FAHP* برای زیرمعیارهای زیرساخت فناوری اطلاعات انجام شد تا اولویت آن‌ها نسبت به هم مشخص شود. جدول (16)، فراوانی پاسخ‌ها بر اساس نظر خبرگان در مقایسات زوجی اولیه را نشان می‌دهد که در آن معادل عبارت‌های انگلیسی عبارت‌اند از. معادل عبارت‌های انگلیسی عبارت‌اند از: سیستم‌عامل (*A*)، نرم‌افزارها و برنامه‌های کاربردی (*B*)، ارتباطات و شبکه فعال (*C*)، تجهیزات پردازشی (*D*)، ذخیره‌سازی و پشتیبان گیری (*E*)، خدمات پایه فناوری اطلاعات (*F*)، خدمات پایگاه‌های داده (*G*)، مدیریت و پایش زیرساخت فناوری اطلاعات (*H*).

مراحل بعدی مشابه محاسبات گروه‌های اصلی انجام شد که نتیجه نهایی به شرح جدول (17) است:

جدول (17). محاسبات *FAHP* برای زیرساخت فناوری اطلاعات

معیارها	اولویت	وزن معیارها
سیستم‌عامل (*A*)	4	0/000
نرم‌افزارها و برنامه‌های کاربردی (*B*)	4	0/000
ارتباطات و شبکه فعال (*C*)	4	0/000
تجهیزات پردازشی (*D*)	3	0/203
ذخیره‌سازی و پشتیبان گیری (*E*)	1	0/521
خدمات پایه فناوری اطلاعات (*F*)	4	0/000
خدمات پایگاه‌های داده (*G*)	4	0/000
مدیریت و پایش زیرساخت فناوری اطلاعات (*H*)	2	0/275

۷. نتیجه‌گیری

پارامترهای مؤثر در ارزیابی امنیتی مراکز داده در سه دست زیرساخت فیزیکی، زیرساخت فناوری اطلاعات و مبحث مدیریت دسته‌بندی می‌شود. باتوجه‌به این‌که سازمان‌ها معمولاً بودجه محدودی را برای ایجاد و تأمین امنیت مراکز داده در نظر می‌گیرند، باید پیاده‌سازی امنیت را بر اساس اولویت‌ها انجام داد. از طرفی بحث امنیت به دیدگاه سازمان مربوطه نیز وابسته است و خبرگان فناوری اطلاعات اولویت‌های متفاوتی نسبت به سایر سازمان‌ها داشته باشند؛ لذا بهتر است برای پیاده‌سازی امنیت ضمن رعایت استانداردهای موجود، دغدغه‌های صاحب‌نظران فناوری اطلاعات سازمان را نیز مدنظر قرارداد. بر همین اساس در این پژوهش پس از شناسایی عوامل مؤثر در امنیت مراکز داده، این عوامل بر اساس نظر خبرگان فناوری اطلاعات شهرداری رشت رتبه‌بندی شد.

در این تحقیق از سه حوزه مطرح‌شده در بالا، دو حوزه زیرساخت فیزیکی و زیرساخت فناوری اطلاعات موردبررسی قرار گرفت و مشخص گردید میان این دو، امنیت زیرساخت فناوری اطلاعات به‌طور محسوسی نسبت به زیرساخت فیزیکی اولویت دارد و وزن آن تقریباً برابر یک است.

از بین زیرمعیارهای حوزه زیرساخت فناوری اطلاعات، ذخیره‌سازی و پشتیبان گیری با وزن نسبی 0/52 در اولویت اول، مدیریت و پایش زیرساخت فناوری اطلاعات با وزن نسبی 0/28 در اولویت دوم، تجهیزات پردازشی با وزن نسبی 0/20 در اولویت سوم و مابقی شاخص‌ها در اولویت چهارم اهمیت قرار دارند. باتوجه‌به این‌که وزن معیارها تا دو رقم اعشار محاسبه می‌شود، وزن پنج معیار از هشت معیار تقریباً برابر شده است که نشان‌دهنده میزان اهمیت یکسان آن‌ها ازنظر نمونه‌های آماری است.

در میان زیرمعیارهای حوزه زیرساخت فیزیکی نیز حفاظت در برابر آتش با وزن نسبی 0/78 در اولویت اول، برق و اتصال زمین با وزن نسبی 0/22 در اولویت دوم و مابقی شاخص‌ها در اولویت سوم اهمیت قرار دارند. باتوجه‌به این‌که وزن معیارها تا دو رقم اعشار محاسبه می‌شود، وزن هفت معیار از نه معیار تقریباً برابر شده است که نشان‌دهنده میزان اهمیت یکسان آن‌ها ازنظر نمونه‌های آماری است.

۸. پیشنهادهایی برای شهرداری رشت

بر اساس نتایج پژوهش، باتوجه‌به این‌که زیرساخت فناوری اطلاعات از اولویت زیادی برای صاحب‌نظران فناوری اطلاعات شهرداری رشت دارد، پیشنهاد می‌شود امنیت این حوزه به‌طور ویژه موردتوجه شهرداری رشت قرار گیرد. پیشنهادهایی که می‌توان بر اساس اولویت‌ها در حوزه زیرساخت فناوری اطلاعات به شهرداری رشت ارائه کرد:

- تهیه *SAN Storage*
- ایجاد نسخه‌های پشتیبان در مکان‌های مختلف و خارج از محدوده *Server Room*

- پیاده‌سازی *LUN Masking*
- پیاده‌سازی سیاست *RBAC*
- استفاده از روش‌های *Data integrity* و *Encryption*
- افزونگی در سامانه‌های ذخیره‌سازی
- پشتیبانی از فناوری استفاده از چندین سطح دیسک
- سیستم نسخ پشتیبان برای تمامی نرم‌افزارهای اصلی، سامانه‌های عامل، فایل‌ها، بانک‌های اطلاعاتی، وقایع، رویدادها و تمامی اجزای مرتبط با خدمات
- استفاده شبکه‌های محلی ذخیره‌سازی از سوئیچ برای ارتباطات و مدیریت انتقال اطلاعات
- تهیه لیست کلیه تجهیزات نصب‌شده به همراه تنظیمات آن‌ها
- ثبت وقایع سیستم مشتمل بر فعالیت‌های کاربر، استثناها، خرابی‌ها، رویدادهای امنیت اطلاعات و هر واقعه مهم دیگر
- پایش سامانه‌های فناوری اطلاعات شامل شبکه، زیرساخت و پایگاه داده توسط ابزارهای پایش
- مستندسازی گزارش‌های حاصل از پایش
- اعلام هشدار از طریق *Email* و *SMS*
- ارتقا *RAM* میزبان‌های موجود
- تهیه *RAM*، *Hard*، *CPU*، کنترل‌گر دیسک سخت، کنترل‌گر شبکه، کارت‌های *I/O*، کارت شبکه و *FAN* به‌عنوان پشتیبان تا در مواقع بروز مشکل برای تجهیزات موجود، بتوان به‌سرعت نسبت به جایگزینی آن‌ها اقدام نمود.

پیشنهادهایی که می‌توان بر اساس اولویت‌ها در حوزه زیرساخت فیزیکی به شهرداری رشت ارائه کرد:

- سیستم اعلام و اطفای حریق مبتنی بر گاز برای *Server Room*
- استفاده از پوشش‌های محافظ آتش در ساختمان
- استفاده از رنگ‌های روشن و ضد حریق در ساختمان
- عدم استفاده از مواد قابل اشتعال در *Server Room*
- استفاده از حسگرهای نمونه‌بردار در *Server Room*
- استفاده از حسگرهای دودی در سایر اتاق‌های مرکز داده
- پیاده‌سازی سیستم تأمین منبع برق و خطوط انتقال سیگنال سیستم اطفای حریق به شکل امن
- استفاده از سامانه‌های اطفای حریق مبتنی بر گاز در *Server Room*
- پایش، تعمیرات و نگهداری سیستم اعلام و اطفای حریق از طریق سامانه‌های پایش
- نصب سیستم تخلیه دود جهت تخلیه دود قبل از عملکرد سیستم اطفای گازی
- نصب سامانه‌های هشدار آتش‌سوزی در اتاق‌های حاوی تابلوی برق
- نصب سیستم حفاظت در برابر صاعقه
- سیستم روشنایی اضطراری
- دو مسیر تأمین برق مجزا باقابلیت تأمین برق کل مجموعه توسط هر یک
- حفاظت مسیرهای برق در برابر دست‌کاری و آتش‌سوزی
- استفاده از تابلو توزیع برق اختصاصی برای *Server Room*
- درنظرگرفتن خلاصی مناسب برای کابل‌های برق برای جلوگیری از کشیده شدن تصادفی
- استفاده از محافظ نوسان
- سیستم اتصال زمین و اتصال کلیه تجهیزات الکتریکی به آن
- عدم استفاده از کلیدهای محافظ جان برای پریزهای فناوری اطلاعات و کنترل‌های مرکزی
- استفاده از *UPS* مرکزی
- استفاده از *UPS* مجزا برای هر یک از خطوط تأمین برق
- جداسازی *UPS* و باتری‌ها
- اتصال سیستم تهویه اتاق *UPS* به ژنراتور برای جلوگیری از قطع برق
- عدم استفاده از باتری‌های اسیدی
- درنظرگرفتن ژنراتور مجزا برای هر یک از خطوط تأمین برق
- درنظرگرفتن منبع ذخیره سوخت برای ژنراتور با امکان سوئیچ به مخزن ذخیره به‌صورت خودکار
- آزمایش تجهیزات جدید موقع راه‌اندازی اولیه و مستندسازی نتایج

۹. محدودیت‌های پژوهش و کارهای آتی

در پژوهش‌های آتی می‌توان رتبه‌بندی معیارها را با سایر روش‌های آماری نظیر تاپسیس فازی و الکترا و غیره انجام داد و با نتایج حاصل از این پژوهش مقایسه نمود. همچنین باتوجه‌به عدم بررسی معیارهای حوزه مدیریت، می‌توان این حوزه را در تحقیق جداگانه‌ای مورد کنکاش قرارداد تا اولویت‌های آن مشخص شود.

نتایج این پژوهش مربوط به یک سازمان با شرایط مختص به خود است و در تعمیم آن به سایر سازمان‌ها باید جانب احتیاط را رعایت نمود. نکته بعدی به ذات تحقیقات پیمایشی مربوط می‌شود که ممکن است پاسخگویی به سؤالات با عدم دقت یا صداقت همراه باشد؛ لذا می‌طلبد که تحقیقات بیشتری در این مورد انجام گردد.

10. مراجع

1] A. Shameli-Sendi, R. Aghababaei-Barzegar, and M. Cheriet, “Taxonomy of information security risk assessment (ISRA),” Computers & Security, vol. 57, pp. 14–30, Mar. 2016, https://doi.org/10.1016/j.cose.2015.11.001

[2] B. Zahedi Barouq and M.J. Babaei, "Schools, Methodology, Design, Management and Maintenance of Data Centers", first edition, Tehran, Hadaf Novin Publications, 2018.(In Persian)

[3] Passive defense in the design of data centers, Research Institute of Strategic Studies and National Security, 2009.(In Persian)

[4] Requirements for data centers, Information Technology Organization of Iran, Frist edition, 2014.(In Persian)

[5] A. Shah Bahrami and R. Rafiezadeh Kasani, "Security of Information Technology Resources", first edition, Tehran, Jihad University Press, 2015.(In Persian)

[6] Requirements for creating data centers(DC100 standard), Iran Information Technology Organization, December 2014.(In Persian)

[7] M. V. M. Lima, R. M. F. Lima and F. A. A. Lins, "A multi-perspective methodology for evaluating the security maturity of data centers," 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Banff, AB, Canada, 2017, pp. 1196-1201, doi: 10.1109/SMC.2017.8122775.

[8] Z. Roknabadi, “An approach to apply security in physical access to data centers based on RFID technology”, M. Sc thesis, Payam Noor University, Tehran, 2012.(In Persian)

[9] S. Janou Sepah, N. Modiri, M. Malakouti and A. Pahlavan Tafti, “Investigating the effects of implementing a multi-layer model to integrate physical and logical access in the data center of Islamic Azad University, Majlesi branch," the third conference of electrical and electronics engineering in Iran, 2011, https://civilica.com/doc/125348.(In Persian)

[10] R. Torkashvand, S. Rahmati Asl and M. Taher Abadi, “Providing a modular support structure for the design of national data centers in Iran,” International Conference on Nonlinear Systems and Optimization of Electrical and Computer Engineering, ,2015, https://civilica.com/doc/383364..(In Persian)

[11] H. Qaraei and M. Aqa Moheidin, 2014, "Improving the ranking of information security risks using multi-criteria decision models", Signal and Data Processing Quarterly, Vol 11, Number 2, pp. 3-14 March 2013, http://jsdp.rcisp.ac.ir/article-1-161-fa.html.(In Persian)

[12] H. Sepehrzadeh, “A method for quantitative evaluation of security risk in cyber-physical systems”, Scientific Journal of Electronical & Cyber Defence, Vol. 11, No. 2, 2023, https://dorl.net/dor/20.1001.1.23224347.1402.11.2.6.9. (in Persian)

[13] R. Gao, S. Jing, M. Li, Y. Sun, G. Si and Y. Zhang, “Research on health evaluation method of data center security protection system”, Proc. SPIE 13175, International Conference on Computer Network Security and Software Engineering, 2024, https://doi.org/10.1117/12.3032059

[14] A. Habibi and S. Afaridi, "Multi-criteria decision-making models (deterministic and fuzzy)", first edition, Tehran, Narvan publications, 2022.(In Persian)

۱۱. پیوست

هوالنور

پاسخگوی گرامی

با سلام و احترام

پرسش‌نامه ذیل باهدف «رتبه‌بندی پارامترهای تأثیرگذار بر ارزیابی امنیتی مراکز داده» ازنظر خبرگان فناوری اطلاعات تهیه‌شده است. این پارامترها به دودسته اصلی زیرساخت فیزیکی و زیرساخت فناوری اطلاعات تقسیم‌شده‌اند که هر یک از آن‌ها دارای زیرمجموعه‌ای مختص به خود هستند. در مرحله اول اولویت این دودسته نسبت به هم مشخص خواهد شد و در مرحله بعد زیرمجموعه‌های هر یک از آن‌ها مورد ارزیابی قرار خواهد گرفت. جهت پاسخگویی، عناوین موجود در سمت راست و چپ جداول را باهم مقایسه کرده و اگر عنوان سمت راست اولویت بیشتری دارد، بر اساس جدول اولویت‌ها، یکی از اعداد سمت راست را که نشان‌دهنده نظر شما در مورد میزان اولویت است، با علامت × مشخص کنید. اگر عنوان سمت چپ اولویت بیشتری دارد، یکی از اعداد سمت چپ را علامت بزنید. درصورتی‌که تمایل دارید نتیجه این پژوهش را دریافت نمایید، در قسمت مشخصات فردی آدرس پست الکترونیکی خود را اعلام فرمایید. پیشاپیش از این‌که با صرف وقت و تکمیل این پرسش‌نامه، مرا در این تحقیق یاری می‌دهید، سپاسگزارم.

زهرا برزگر مقدم

دانشجوی کارشناسی ارشد مهندسی نرم‌افزار پردیس دانشگاه گیلان

اولویت	اولویت یکسان	اولویت متوسط	اولویت زیاد	اولویت بسیار زیاد	اولویت کاملاً زیاد
مقدار عددی	1	3	5	7	9

مشخصات فردی								
جنسیت	مرد	□	زن	□				
سن	20 تا 25	□	26 تا 35	□	36 تا 45	□	46 به بالا	□
مدرک تحصیلی	دیپلم	□	فوق‌دیپلم	□	کارشناسی	□	کارشناس ارشد و بالاتر	□
سابقه کار	5 سال و کمتر	□	6 تا 10 سال	□	11 تا 20 سال	□	21 سال به بالا	□
پست الکترونیک								

مقایسات زوجی گروه‌های اصلی مربوط به امنیت مرکز داده										
i	9	7	5	3	1	3	5	7	9	*j*
زیرساخت فیزیکی										زیرساخت فناوری اطلاعات

مقایسات زوجی شاخص‌های امنیتی زیرساخت فیزیکی مرکز داده										
i	9	7	5	3	1	3	5	7	9	*j*
موقعیت جغرافیایی										ساختمان و معماری
										حفاظت در برابر آتش
										نظارت تصویری و امنیت فیزیکی
										برق و اتصال زمین
										تهویه و مکانیک
										ارتباطات و شبکه غیرفعال
										حفاظت الکترومغناطیس
										مدیریت و پایش زیرساخت فیزیکی
ساختمان و معماری										حفاظت در برابر آتش
										نظارت تصویری و امنیت فیزیکی

	برق و اتصال زمین									
	تهویه و مکانیک									
	ارتباطات و شبکه غیرفعال									
	حفاظت الکترومغناطیس									
	مدیریت و پایش زیرساخت فیزیکی									
حفاظت در برابر آتش	نظارت تصویری و امنیت فیزیکی									
	برق و اتصال زمین									
	تهویه و مکانیک									
	ارتباطات و شبکه غیرفعال									
	حفاظت الکترومغناطیس									
	مدیریت و پایش زیرساخت فیزیکی									
نظارت تصویری و امنیت فیزیکی	برق و اتصال زمین									
	تهویه و مکانیک									
	ارتباطات و شبکه غیرفعال									
	حفاظت الکترومغناطیس									
	مدیریت و پایش زیرساخت فیزیکی									
برق و اتصال زمین	تهویه و مکانیک									
	ارتباطات و شبکه غیرفعال									
	حفاظت الکترومغناطیس									
	مدیریت و پایش زیرساخت فیزیکی									
تهویه و مکانیک	ارتباطات و شبکه غیرفعال									
	حفاظت الکترومغناطیس									
	مدیریت و پایش زیرساخت فیزیکی									
ارتباطات و شبکه غیرفعال	حفاظت الکترومغناطیس									
	مدیریت و پایش زیرساخت فیزیکی									
حفاظت الکترومغناطیس	مدیریت و پایش زیرساخت فیزیکی									

مقایسات زوجی شاخص‌های امنیتی زیرساخت فناوری اطلاعات مرکز داده										
i	9	7	5	3	1	3	5	7	9	*j*
سیستم‌عامل										نرم‌افزارها و برنامه‌های کاربردی
										ارتباطات و شبکه فعال
										تجهیزات پردازشی
										ذخیره‌سازی و پشتیبان گیری
										خدمات پایه فناوری اطلاعات
										خدمات پایگاه‌های داده
										مدیریت و پایش زیرساخت فناوری اطلاعات
نرم‌افزارها و برنامه‌های کاربردی										ارتباطات و شبکه فعال
										تجهیزات پردازشی
										ذخیره‌سازی و پشتیبان گیری
										خدمات پایه فناوری اطلاعات
										خدمات پایگاه‌های داده
										مدیریت و پایش زیرساخت فناوری اطلاعات
ارتباطات و شبکه فعال										تجهیزات پردازشی
										ذخیره‌سازی و پشتیبان گیری
										خدمات پایه فناوری اطلاعات
										خدمات پایگاه‌های داده
										مدیریت و پایش زیرساخت فناوری اطلاعات
تجهیزات پردازشی										ذخیره‌سازی و پشتیبان گیری
										خدمات پایه فناوری اطلاعات
										خدمات پایگاه‌های داده
										مدیریت و پایش زیرساخت فناوری اطلاعات
ذخیره‌سازی و پشتیبان گیری										خدمات پایه فناوری اطلاعات
										خدمات پایگاه‌های داده
										مدیریت و پایش زیرساخت فناوری اطلاعات
خدمات پایه فناوری اطلاعات										خدمات پایگاه‌های داده
										مدیریت و پایش زیرساخت فناوری اطلاعات
خدمات پایگاه‌های داده										مدیریت و پایش زیرساخت فناوری اطلاعات