Military Science and Tactics
AJA Command and Staff University
https://www.qjmst.ir/
Online ISSN: 4520-2676
Print ISSN: 2008-191x

Presenting the architecture framework of cyber security governance in the defense organizations of the Islamic Republic of Iran

Nima Farzamnia [1] | Behnam Abdi✉ [2]| Ali Rezaeian[3]

1. Department of Industrial Management, Central Tehran Branch, Islamic Azad University, Tehran, Iran
   E-mail: nima.farzamnia@gmail.com
2. Department of Management, Faculty of Management and Military Sciences, Imam Ali Officer University (AS), Tehran, Iran.
   E-mail: abdi220@gmail.com
3. Department of Public Administration, Central Tehran Branch, Islamic Azad University, Tehran, Iran.
   E-mail: a-rezaeian@sbu.ac.ir

Article Info

Article type:
Research Article

Article history:
Received 18 March 2022
Received in revised form 10 June 2022
Accepted 16 June 2022
Published online 25 June 2022

Keywords:
Cyber space, security, cyber security governance architecture framework, defense organizations of the Islamic Republic of Iran, organizational levels.

ABSTRACT

Objective: The current research aims to provide a framework for the architecture of cybersecurity governance in defense organizations, with a balanced approach between management and technical aspects. It considers cybersecurity not only as a set of new techniques and tools from a technical and engineering perspective but also addresses it from a management perspective.

Methodology: This is a combined research method (qualitative and quantitative), where the qualitative phase involves content analysis, and the quantitative phase is based on the findings of the qualitative phase and is conducted using questionnaire tools. The findings are then integrated into a cohesive framework.

Findings: In today's world, and consequently in organizations, assets and resources are transforming towards becoming cyber assets. Governments and organizations are well aware of the increasing role and importance of these assets and are making significant efforts in this regard. On the other hand, cyber threats are pervasive, growing, and real. Recent incidents in our country have highlighted the significance of cyber conflicts between countries and governments. This issue is even more important and serious in defense organizations.

Originality: Ultimately, a framework for the architecture of cybersecurity governance in defense organizations is proposed. This framework enables these organizations to achieve organizational security in cyberspace through a comprehensive, structured, proactive approach that goes beyond limited management, technical, and restricted perspectives. It aims to drive convergence and systematic integration in order to address the existing lack of harmony.

Cite this article: Farzamnia, N., Abdi, B., & Rezaeian, A. (2023). Presenting the architecture framework of cyber security governance in the defense organizations of the Islamic Republic of Iran. Military Science and Tactics, 19(64), 167-180.

Publisher: Command and Staff University

DOI: 10.22034/QJMST.2023.560525.1759

فصلنامه علمی علوم و فنون نظامی
شاپای چاپی: ۱۹۱۸-۲۰۰۸ شاپای الکترونیکی: ۲۶۷۶-۴۵۲۰ https://www.qjmst.ir/ دانشگاه فرماندهی و ستاد آجا

ارائه چهارچوب معماری حاکمیت امنیت سایبری در سازمان‌های دفاعی جمهوری اسلامی ایران

نیما فرزام نیا [۱] | بهنام عبدی [۲] ✉ | علی رضائیان [۳]

۱. گروه مدیریت صنعتی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران.
رایانامه: nima.farzamnia@gmail.com

۲. گروه مدیریت ، دانشکده مدیریت و علوم نظامی، دانشگاه افسری امام علی (ع)، تهران، ایران.
رایانامه: abdi220@gmail.com

۳. گروه مدیریت دولتی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران.
رایانامه: a-rezaeian@sbu.ac.ir

اطلاعات مقاله

نوع مقاله:
مقاله پژوهشی
مقالهٔ پژوهشی

تاریخ دریافت:
۱۴۰۱/۱۲/۰۱

تاریخ بازنگری:
۱۴۰۲/۰۵/۰۱

تاریخ پذیرش:
۱۴۰۲/۰۶/۰۹

تاریخ انتشار:
۱۴۰۲/۰۶/۱۳

کلیدواژه‌ها:
فضای سایبری، امنیت، چارچوب معماری حاکمیت امنیت سایبری، سازمان‌های دفاعی جمهوری اسلامی ایران، سطوح سازمانی.

چکیده

هدف: پژوهش حاضر به دنبال چارچوبی برای معماری حاکمیت امنیت سایبری در سازمان‌های دفاعی و با نگاهی متوازن مدیریتی و فنی است که امنیت سایبری را نه فقط یک‌مجموعه از تکنیک‌ها و ابزارهای جدید دیدگاه فنی و مهندسی می‌داند و نه صرفا با دیدگاه مدیریتی به امنیت سایبری می‌پردازد.

روش: روش تحقیق ترکیبی (کیفی و کمی) است که فاز کیفی آن به وسیله تحلیل محتوا و فاز کمی آن بر مبنای یافته‌های فاز کیفی و با ابزار پرسشنامه انجام شده است و یافته‌ها در یک چارچوب زکمن قرار می‌گیرند.

یافته‌ها: در جهان امروز و به تبع آن در سازمان‌ها؛ سرمایه‌ها، دارایی‌ها و منابع سازمان‌ها، در حال تبدیل و تغییر ماهیت به سمت سرمایه‌های سایبری است، لذا دولت‌ها و سازمان‌ها به نقش و اهمیت روزافزون این سرمایه‌ها به خوبی واقف شده و تلاش قابل توجهی در این رابطه دارند. از سوی دیگر تهدیدهای سایبری فراگیر، رو به رشد و واقعی هستند و همانطور که اخیرا در کشور ما نیز مصداق‌هایی مشاهده شد، مناقشات سایبری در بین کشورها و دولت‌ها در حال گسترش و بسیار تعیین کننده است. این مهم در سازمان‌های دفاعی اهمیت بسیار بیشتر و جدی‌تری دارد.

نتیجه‌گیری: در نهایت یک چارچوب معماری حاکمیت امنیت سایبری در سازمان‌های دفاعی ارائه می‌گردد تا این سازمان‌ها بتوانند با نگاهی جامع و ساختاری و پیش‌کنش‌گرانه و فراتر از دیدگاه‌های مدیریتی، فنی و محدود، به برقراری امنیت سازمان در فضای سایبری دست یابند و عدم همگرایی موجود را به سمت یکپارچگی و نظام‌مندی سوق دهند.

استناد: فرزام نیا، نیما، عبدی، بهنام و رضائیان، علی. (۱۴۰۲). ارائه چهارچوب معماری حاکمیت امنیت سایبری در سازمان‌های دفاعی جمهوری اسلامی ایران. علوم و فنون نظامی، ۱۹(۶۴)، ۱۶۷-۱۸۰.
doi: 10.22034/qjmst.2023.560525.1759

ناشر: دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

۱. مقدمه

یکی از مباحث و چالش‌های اساسی در بهره‌مندی از ظرفیت‌های فضای سایبر، امنیت سایبری است. امنیت سایبری مجموعه‌ای از ابزارها، سیاست‌ها، مفاهیم امنیتی، دستورالعمل‌ها، رویکردهای مدیریت ریسک، اقدامات، آموزش، بهترین شیوه‌ها، اطمینان و فن‌آوری هایی است که می‌تواند برای محافظت از محیط زیست سازمان و دارایی‌های سایبری آن استفاده شود. از سوی دیگر با توجه به نفوذ همه جانبه ابزارهای فناوری اطلاعات و ارتباطات در زندگی بشر، فضای سایبری در سازمان‌های دفاعی هم وسعت بسیار زیادی یافته است از سوی دیگر ماده حیاتی و خونی که در رگ‌های فضای مجازی و سایبری وجود دارد اطلاعات است و این محیط‌ها براساس پردازش، ذخیره و انتقال اطلاعات پایه گذاری می‌شوند و به عبارتی شالوده این محیط‌ها عملیات روی اطلاعات است. نکته حائز اهمیت اینجاست که بی‌تردید اطلاعات، پردازش اطلاعات و شبکه‌های ارتباطی هسته تمامی فعالیت‌های نظامی و اطلاعاتی بشمار می‌آیند و در طول تاریخ فرماندهان نظامی به برتری اطلاعاتی همواره به عنوان یکی از عوامل موثر در کسب پیروزی نگریسته‌اند. با این همه انقلاب در فناوری اطلاعات نه تنها در حال ایجاد تغییرات کمی در محیط‌های اطلاعاتی است، بلکه باعث تغییرات کیفی در این محیط‌ها نیز گردیده است به طوری که امروزه شاهد تغییرات ژرفی در عملیات‌های دفاعی، نظامی و استراتژیک هستیم که خود تبدیل به شیوه‌های جدیدی ازعملیات‌ها وجنگ‌های استراتژیک شده‌اند که مهم‌ترین آن‌ها جنگ‌های سایبری است. بدین ترتیب حفاظت از مرزهای مجازی که عمده اطلاعات این عامل نیروبخش و حیاتی را در درون خود جای داده‌اند به اندازه حفاظت از مرزهای فیزیکی برای هر کشوری دارای اهمیت است.

باتوجه به روند حرکت سریع جنگ‌های سایبری و دکترین سایبری تهاجمی که کشورهای دشمن دارند و همچنین عملیات و ضربات سایبری اخیرکه علیه شبکه‌ها و سایت‌های رایانه‌ای سازمان‌های دولتی و حتی علیه منافع ملی صورت گرفته است (همچون حمله به شبکه توزیع سوخت، راه آهن و وبگاه‌های دولت و...)، طبیعی است که در جهت جلوگیری از غافلگیری در جنگ راهبردی و یا عملیاتی سایبری دشمن باید توجه ویژه‌ای به چارچوب معماری حاکمیت امنیت سایبری در سازمان‌های دفاعی و تقویت ساختار سازمانی سایبری در نیروهای مسلح براساس این معماری شود

به همین ترتیب این مهم است که در طراحی ساختار عملیات دفاعی این سازمان‌ها باید توانایی‌های سایبری دشمنان را در نظر بگیریم، زیرا در زمان حمله هوایی، زمینی و یا موشکی دشمن، ممکن است همراه با عملیات نفوذ یا ضربه سایبری علیه ساختار سایبری عملیاتی و

ارتباطی و یا ضد سیستم‌های بحرانی و حیاتی کشور مانند: شبکه آب عمومی، شبکه برق، مخابرات کشوری و یا رادیو و تلویزیون باشدکه تقریبا همه جنبه‌های زندگی مردم را در بر می‌گیرد، این اقدام می‌تواند باعث فلج نمودن جامعه و تضعیف روحیه افکار عمومی شده و جنگ را به نفع دشمن خاتمه یافته جلوه دهد. البته شایان ذکر است که در سازمان‌های دفاعی اقدامات مفید و مطلوبی نیز صورت گرفته است که از مهم‌ترین آن‌ها می‌توان به تشکیل اداره امنیت سایبری، تدوین آئین‌نامه جامع امنیت فناوری اطلاعات و یا اقدامات مشابه دیگری اشاره نمود البته مساله مهم اینجاست که این تلاش‌ها و اقدامات در سازمان‌ها،بخش ها، نیروها و ادارات دفاعی انجام شده است که هرکدام به صورت نگاه‌های برهه‌ای و جزیره‌ای و با توجه به درکشان محدودشان از موضوع، اعتبار، منابع و امکانات محدود در اختیارشان بوده است (فرزام نیا، ۱۳۹۷: ۲۸).

این‌ها را می‌توان پله‌هایی از مراحل رشد سازمانی دانست که تاکنون در تامین امنیت فضای سایبری و بهداشت سایبری سازمان‌های دفاعی انجام شده است، اما با وضعیت موجود و حرکات سریع و جبهه‌های جدیدی فضای سایبری در دنیا که دشمنان ما می‌توانند علیه ما اختیار کنند هم‌خوانی ندارد و نکته مهم دیگری که در سازمان‌ها در برخورد با این فضا وجود دارد نگرش متفاوت به این فضاست چرا که جنگ سایبری را نباید فقط یک مجموعه از تکنیک‌های عملیاتی جدید به شمار آورد و با دیدگاه فنی و مهندسی به آن نگاه کرد و یا به همین ترتیب نمی‌توان فقط با دیدگاه مدیریتی به آن پرداخت، بلکه باید آن را سبک نوینی از جنگ دانست که امنیت در این فضا مستلزم ارائه رهیافت‌ها، راهکارها، و راهبردهای نو در زمینه معماری و سازماندهی در سازمان‌های دفاعی می باشد (Peter Trim **et. al,2022: 196**). از اینروست که نیاز به طراحی یک چارچوب معماری حاکمیت امنیت سایبری در سازمان‌های دفاعی می‌باشد تا بتوانند با نگاهی فراتر از دیدگاه‌های مدیریتی، فنی و محدود به برقراری امنیت سازمان در فضای سایبری دستیافت و این عدم همگرایی موجود را به سمت یکپارچگی و نظام‌مندی سوق داد.

برای درک بهتر مساله، رتبه‌بندی منطقه آسیا و اقیانوسیه در فهرست جهانی امنیت سایبری دنیا که توسط سازمان ITU در سال ۲۰۲۰ منتشر شده است در جدول زیر قابل توجه است:

جدول (۱) رتبه‌بندی امنیت سایبری در آسیا و اقیانوسیه سال ۲۰۲۰ (Global Cybersecurity Index ,2020)

کشور	نمره	رتبه در منطقه	رتبه جهانی
عربستان	۵۴.۹۹	۱	۳
جمهوری کره	۵۲.۹۸	۲	۴
سنگاپور	۵۲.۹۸	۲	۴

کشور	نمره	رتبه در منطقه	رتبه جهانی
امارات متحده عربی	۰۶ .۹۸	۳	۵
مالزی	۰۶ .۹۸	۳	۵
ژاپن	۸۲ .۹۷	۴	۷
هند	۵ .۹۷	۵	۱۰
استرالیا	۴۷ .۹۷	۶	۱۲
عمان	۰۴ .۹۶	۷	۲۱
اندونزی	۸۸ .۹۴	۸	۲۴
ویتنام	۵۹ .۹۴	۹	۲۵
قطر	۵ .۹۴	۱۰	۲۷
ایران	۰۷ .۸۱	۱۴	۵۴

ایران در رتبه ۵۴ دنیا و چهاردهم آسیا و اقیانوسیه قرار دارد و مطابق این گزارش ایران اختلاف فاحشی با کشور رتبه نخست منطقه یعنی عربستان و رتبه اول دنیا یعنی کشور آمریکا دارد. به همین ترتیب مطابق گزارش سازمان جهانی ITU سهم خاورمیانه در این استاندارد در سال ۲۰۱۳ تنها ۲ درصد بوده است و با توجه به جایگاه ایران در میان کشورهای منطقه، می‌توان نتیجه گرفت حوزه امنیت سایبری در ایران، جایگاهی بسیار پایین در میان کشورهای پیشرفته جهان است. نکات حائز اهمیت این است که کشورهای منطقه مانند ترکیه با رتبه ۱۱ جهانی، عربستان رتیه سوم جهانی، روسیه و امارات عربی با رتبه پنجم جهانی در رتبه‌های خوب دنیا هستند.

بنابراین بسیار مهم است که تمام صنایع، نهادهای دولتی، سازمان‌ها و مردم از بهترین روش‌های امنیتی مناسب برای محافظت از حملات سایبری استفاده کنند که این مهم نیاز به یک چارچوب معماری درست و کامل برای مدیریت امنیت سایبری سازمان خود دارد تا براساس آن بتواند روند برقراری امنیت را در فضای سایبری به درستی طی نماید. معماری حاکمیت امنیت سایبری سازمان، سیستم امنیت سایبری را از جنبه‌های گوناگون معماری مورد بررسی قرار می‌دهد. چارچوبی را معرفی می‌نماید که بر پایه معماری سازمانی شکل گرفته است. یک سازمان نیاز دارد به نحو مناسبی ساختارهای امنیتی خود را طراحی نماید تا توسط آن بتواند در محیط به شدت رقابتی امروزی، فعالیت نماید و وضعیت امنیت سایبری دفاعی کشور را در سطح بین المللی ارتقا دهد. (Schoenfield,2020: 24)

۲. ادبیات و پیشینه پژوهش

۱.۲. فضای سایبری

مفهوم فضای سایبر قابل تغییر و تحول و بسیار بحث‌انگیز است و تعاریف متعددی برای این فضا وجود دارد. به عنوان مثال درگذشته، پنتاگون حداقل دوازده تعریف متفاوت از فضای سایبر ارائه کرده است. آخرین بار در سال ۲۰۰۸ میلادی، پنتاگون گروهی از متخصصان را گرد هم آورد تا ظرف مدت یک سال بر روی تعریف جامع از فضای سایبر توافق کنند. این بار آن‌ها چنین تعریفی ارائه کردند: «دامنه‌ای جهانی درونِ محیطی اطلاعاتی، تشکیل یافته از شبکه‌های به هم پیوسته در بستری از فناوری اطلاعات شامل اینترنت، شبکه‌های ارتباطاتی، سیستم‌های رایانه‌ای، پردازشگرهای نهفته و دستگاه‌های کنترلی». در ادامه به تعریفی جامع که منطبق با خصوصیات امروزۀ آن است اشاره می‌کنیم.

به شبکه‌های وابسته به یکدیگر، از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه‌های رایانه‌ای، پردازنده‌های تعبیه شده، کنترل‌کننده‌های صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین این محیط‌ها و انسان به منظور تولید، پردازش، ذخیره‌سازی، مبادله، بازیابی و بهره‌برداری از اطلاعات، فضای سایبری اطلاق می‌شود. (فرزام نیا و همکاران، ۵: ۱۳۹۳)

این تعریف قرار نیست تعریفی جامع و مانع باشد. حتی در آینده می‌توان رایانه‌هایی را تصور کرد که بر پایه DNA باشند نه الکترونیک (Jocelyn O. Padallan,2020: 146).

گسترۀ این فضا بسیار بیشتر از آن است که تصور می‌شود به عنوان مثال از فضای تبادل اطلاعات در شبکۀ اینترنت تا سیستم‌ها و سامانه‌های کنترل وزارت نیرو که کل شبکۀ برق و آب یک کشور را کنترل می‌کند و یا سیستم‌های ارتباطی سامانه‌های موشکی وحتی سامانه‌های اطلاعاتی کنترل ترافیک شهری و موارد مشابه زیاد دیگر را می‌توان در این فضا نام برد. برای شناخت بهتر فضای سایبری این فضا را در سه لایه زیر تعریف می‌کنند:

۱. لایۀ فیزیکی

تمام سیستم‌های اطلاعاتی روی یک لایۀ فیزیکی که متشکل از چندین جعبۀ و برد الکترونیکی و گاهی چندین سیم یا امواج الکترونیکی قرار گرفته است. با حذف لایۀ فیزیکی، کل این سیستم محو می‌شود. بنابراین اجزاء سخت‌افزاری دستگاه‌های الکترونیکی و رایانه‌ها را می‌توان به عنوان مثال‌هایی از این لایه نام برد.

۲. لایهٔ ساختاری

لایهٔ ساختاری شامل دستورالعمل‌هایی است که طراحان و کاربران برای تجهیزات و شیوهٔ تبادل اطلاعات در آن‌ها تعریف می‌کنند و از طریق این دستورالعمل‌ها، دستگاه‌ها با هم تعامل دارند و شامل شناخت طرح، تنظیم اطلاعات، آدرس‌دهی، مسیریابی، قالب‌بندی مستندات، مدیریت پایگاه داده‌ها و غیره است. این همان لایه‌ای است که در آن عملیات هک صورت می‌گیرد به عنوان مثال برنامه‌های نوشته شده توسط برنامه‌نویسان و یا سایت‌های طراحی شده توسط طراحان یا پروتکل‌های ارتباطی شبکه و الگوریتم‌های رمزنگاری استفاده شده را می‌توان جزء این لایه دانست.

۳. لایهٔ معنایی(اطلاعات)

لایهٔ معنایی که بالاترین لایه است، شامل اطلاعات دستگاه است. همان چیزی که کامپیوتر را در جایگاه اول اهمیت قرار داده است و به عبارتی طراحی دولایهٔ دیگر برای پردازش، سازماندهی، تجزیه و تحلیل و ذخیره و بازیابی محتوای این لایه بوده و به زبان ساده دولایهٔ دیگر به این لایه خدمات ارائه می‌دهند. معمولاً حمله و نفوذ در فضای سایبری ممکن است در هر لایه‌ای صورت پذیرد؛ ولی در نهایت با هدف دسترسی، تغییرات، انهدام و یا ساخت اطلاعات در این لایه می‌باشد. (F. Schreier,2015: 11)

۲. ۲. جنگ سایبری و حملهٔ سایبری

جنگ سایبری، تحریف یا اختلال عمدی توسط یک کشور یا مهاجمان در سیستمی در فضای سایبری است که کشوری دیگر از آن بهره می‌برد. کشور اول را مهاجم و کشور دوم را هدف می‌نامند. در برخی مواقع، هدف ممکن است مقابله به مثل نماید. جنگ سایبری می‌تواند به طور مستقل انجام شده یا در کنار جنگ زمینی، دریایی و یا هوایی صورت پذیرد.. (Stanislav Abaimov, Maurizio Martellini,2020: 15). به هرگونه اقدام غیرمجاز، که با هدف نقض سیاست امنیتی یک سرمایهٔ سایبری و ایجاد خرابی یا اختلال در عملکرد یا از کاراندازی خدمات و دستیابی به اطلاعات سرمایهٔ سایبری مذکور انجام می‌گیرد، تهاجم (حمله) سایبری اطلاق می‌گردد. (Dan Shoemaker et all,2017: 78)

۱. ۲. ۲. انواع جنگ‌های سایبری

جنگهای سایبری را از نظر شیوهٔ عملکرد و نحوهٔ به کارگیری می‌توان به دو دستهٔ زیر تقسیم نمود:

۱-۲۲-۲-جنگ سایبری عملیاتی

جنگ سایبری عملیاتی عبارتست از حملات سایبری که علیه اهداف نظامی یا اهداف غیرنظامی که مرتبط با کاربردهای نظامی هستند، صورت می‌گیرد.

۲-۲۲-۲- جنگ سایبری راهبردی

مجموعهٔ عملیات سایبری که توسط یک کشور یا نهاد مستقل علیه یک کشور و مردم آن اجرا شده و عموماً به منظور ایجاد تغییر در رفتار کشور هدف در فضای سیاسی و استراتژیک صورت می‌پذیرد را جنگ سایبری راهبردی می‌خوانند. فرض در جنگ‌های سایبری راهبردی بر این است که متوسل شدن کشورها به جنگ سایبری بدان معناست که ابزارهای حقوقی، دیپلماتیک و اقتصادی برای وادار کردن کشور هدف به در پیش گرفتن رفتار مطلوب مؤثر واقع نشده و یا ناکافی فرض شده است و به ناچار دو کشور جهت دستیابی به اهداف مورد نظر خود یا به عنوان اقدامی تلافی‌جویانه به این نوع از نبرد سایبری یا مقابله با آن دست می‌یابند. (C. LIBICKI,2009: 117). به عنوان مثال زمانی که آمریکا و رژیم صهیونیستی در فشارهای استراتژیک برای متوقف کردن روند پیشرفت انرژی هسته‌ای ایران راه به جایی نبردند، اقدام به طراحی نرم‌افزار استاکس نت نمودند تا بتوانند از طریق فضای سایبری روند رشد انرژی هسته‌ای را مختل کنند که موفق نشدند.

۳. ۲. دفاع سایبری

شامل تمام اقداماتی است که مانع موفقیت حمله‌کنندگان و سود بردن آن‌ها از تلاش‌هایشان شود. به عبارت دیگر در زمان حملهٔ سایبری اقدامات دفاعی در جهت جلوگیری از دسترسی به منابع سایبری مورد نظر متخاصم و یا عمل متقابل در جهت ممانعت از ادامهٔ عملیات توسط متخاصم صورت می‌پذیرد که البته نوع دفاع (ممانعت یا عمل متقابل) وابسته به استراتژی ملی دفاعی یک کشور است تا با توجه به تهدیدات و حملاتی که در دنیای فناوری اطلاعات هر روزه جلوه‌های جدیدتری را به نمایش می‌گذارد تجربه کسب نموده و از حملات انجام شده و تهدیدهای روز را رصد کرده و به وسیلهٔ بازخورد سیستم دفاع را بروز کنند (ANDRESS et. al,2014: 203).

۴. ۲. حکمرانی[1]

مبنای اساسی طرح این مفهوم، این واقعیت است که اداره صحیح کشور، اساسا معطوف به هدایت اقتصاد و جامعه است و مدیران باید طیفی از الزامات و اقدامات را برای این هدایت در نظر بگیرند. در همین امتداد، ارتباط بین‌بخش های دولتی و خصوصی در قالب مفهوم حکمرانی مطرح می‌شود(Pierre & Peters, 2000) . اساسی‌ترین مفهوم قابل درک از واژه حکمرانی، آن

[1] Governance

است که دیگر نمی‌توان دولت را تنها کنشگر مستقل و دارای قدرت در جامعه (در یک زمان خاص) دانست، بلکه امروزه‌بخش عمومی وبخش خصوصی، به شیوه‌های گوناگون، به هم وابسته بوده، سهم قابل توجهی از خط‌مشی‌های‌بخش عمومی بر اساس مراوده‌بخش دولتی وبخش خصوصی، توسعه یافته و اجرا می‌شود. تغییر به سمت مفهوم حکمرانی برای اهداف جمعی، ملاحظات ناظر بر خط مشی قابل توجهی درباره نقش مدیریت دارد. این تغییر نگاه به سمت حکمرانی، به این معناست که دولت باید به حالتی فراتر از یک جایگاه ساختاری دارای اختیارات و سلسله مراتب حرکت کند (Hall, 2002).

۱. ۴. ۲. حکمرانی(حاکمیت) امنیت سایبری

«حکمرانی امنیت سایبری»عبارتی است که در دو سطحِ کلان و خرد به کار می‌رود. در سطح کلان، این عبارت مفهومی سیاسی است که در حوزه‌ی روابط بین الملل و حکمرانی اینترنت به کار می‌رود. در سطح خرد (که عمده‌ی ادبیات در حول و حول این سطح از واژه طرح شده است)، حکمرانی امنیت سایبری مفهومی مدیریتی و فنی است که بخشی از مباحث مرتبط با حکمرانیِ سازمان‌ها پیرامون آن شکل گرفته است. در واقع، قلمروِ حکمرانی امنیت سایبری در معنای خرد، به سطح یک سازمان بزرگ یا کوچک دولتی یا خصوصی محدود می‌شود بر اساس تعریفِ مُجمل، حکمرانی امنیت سایبری ناظر به فعالیت‌های تصمیم‌سازی، تصمیم گیری و نیز توزیع اختیارات در مسائل مرتبط با امنیت فضای سایبری است. بر اساس تعریفِ مبسوط، حکمرانی امنیت سایبری، سیستمی متشکل از فرآیندهای تصمیم‌گیری و پاسخگویی با استفاده از فرآیندهای مرتبط با اطلاعات است که مشخص می‌کند چه کسی می‌تواند چه اقداماتی را با چه عملیاتی در چه زمانی، تحت چه شرایط و مقتضیاتی و با استفاده از چه روشی در فضای سایبری با هدف حفظ امنیت سایبری انجام دهد.

۲. ۴. ۲. معماری امنیت سایبری

معماری امنیت سایبری سازمانی، مجموعه‌ای از فعالیت‌های به کارگیری روش‌های جامع برای تشریح ساختار و رفتار فرآیندهای امنیتی سازمانی، سیستم‌های امنیتی سایبری و زیربخش های شخصی و سازمانی در حوزه سایبری است، به گونه‌ای که با اهداف مرکزی و جهت‌های استراتژیک سازمانی هم راستا شوند.

۵. ۲. چارچوب‌های معماری سازمانی[۲]

[2] Enterprise Architecture Framework

از دیدگاه معماری، چارچوب ابزاری است که کمک می‌کند تا معمار سازماندهی شده بیاندیشد. این ابزار برای معماری سازمانی عبارت است از یک ساختار منطقی برای دسته‌بندی و سازمان‌دهی مدل‌های توصیفی سازمان که برای مدیریت سازمان و به همان اندازه برای توسعه سیستم‌های سازمان دارای اهمیت هستند. جالب اینجاست که بسیاری معماری را تنها از طریق چارچوب تعریف می‌کنند و شاید هم چنین تعریفی اشتباه نباشد، چرا که معماری بدون چارچوب ممکن است به اهداف نهایی خود نرسد. در عوض استفاده از چارچوب تضمین دهنده یکنواختی و استاندارد در زمان گذار و یکپارچه‌سازی سیستم‌های اطلاعاتی است.

۱. ۵. ۲. چارچوب معماری سازمانی زکمن

چارچوب معماری سازمانی زکمن (Zachman 1987) را جان زکمن در سال ۱۹۸۷ برای صنعت و تجارت ارائه کرده است. وی در ابتدا این کار را با ارئه یک الگوی جامع در زمینه معماری اطلاعات شروع نمود و چون معتقد به تحلیل سازمان با استفاده از چارچوب معماری بود جنبه‌های مختلف طراحی یک سیستم از نظر محتوا، مفهوم، منطق، فیزیک و توصیف‌های دقیق غیر محتوائی را به صورت مجموعه سوالاتی از نقطه نظر داده، وظیفه، شبکه، افراد، زمان و انگیزه در یک جدول ارائه کرد و در طی فرآیند تکمیل آن، معماری انجام شده با پاسخ به سوالات چه چیز، چطور، کجا، چه کسی، چه زمانی و چرا توصیف می‌شود:

جدول (۲) فرمت کلی چارچوب معماری سازمانی جان زکمن

دیدگاه/جنبه	چه چیز	چطور	کجا	چه کسی	چه وقت	چرا
محتوایی						
مفهومی						
منطقی						
فیزیکی						
غیرفیزکی						

بدیهی است در پژوهش حاضر به نگاه خاص مهندسی (فنی) و مدیریتی، به دنبال تعریف سطرها، ستون‌ها و تکمیل خانه‌های ماتریس حاصل و ارائه چارچوب پیشنهادی معماری حاکمیت امنیت سایبری دربخش دفاع هستیم.

روش‌شناسی پژوهش

با توجه به عدم بررسی چارچوب معماری حاکمیت امنیت سایبری، این تحقیق اکتشافی و به دنبال درک بهتر از پدیده‌ی مورد نظر می باشد. بر این اساس، اجرای این تحقیق به منظور پاسخ به سوالات زیر می‌باشد:

۱: ابعاد و سطوح معماری حاکمیت امنیت سایبری براساس چارچوب معماری سازمانی کدامند؟

۲: ابعاد و سطوح معماری حاکمیت امنیت سایبری چه ارتباطاتی با یکدیگر دارند؟

۳: چارچوب معماری امنیت سایبری براساس چارچوب معماری سازمانی چگونه می‌باشد؟

پژوهش، ترکیبی (کیفی و کمی) بوده و در فاز اول پژوهش با توجه به نوع پژوهش، ترکیبی از مطالعات کتابخانه‌ای به منظور تحلیل محتوای اسناد و مدارک موجود و مطالعات میدانی با مصاحبه مورد توجه قرارگرفت. بنابراین از روش‌ها و ابزارهای: ۱)منابع کتابخانه‌ای و اینترنتی شامل، کتب، مقالات ۲) مصاحبه اکتشافی با خبرگان متخصص در حوزه مربوط و مدیران و کارشناسان خبره خارجی ۳) پرسشنامه جهت جمع‌آوری اطلاعات استفاده شد. و درفاز دوم پژوهش پس از به دست آوردن ابعاد در زمینه چارچوب معماری حاکمیت امنیت سایبری در سازمان‌های دفاعی به منظور بررسی و تایید یافته‌ها، پرسشنامه‌ای تهیه و توزیع گردید و پرسشنامه‌ها به منظور تحلیل داده‌ها در اختیار خبرگان قرار گرفت. پرسشنامه دارای دو قسمت است: اول)اطلاعات مربوط به پاسخ‌دهندگان. دوم) ابعاد و مفاهیم نهایی حاصل از فاز کیفی در این قسمت قرارداده شده و میزان اهمیت هر یک از گزاره‌ها (ابعاد) در چارچوب معماری حاکمیت امنیت سایبری در سازمان‌های دفاعی بر اساس طیف لیکرت پنج گزینه‌ای سنجیده می‌شود.

خبرگان و متخصصان در دسترس سازمان‌های دفاعی که قبلا در فاز کیفی به آن‌ها مراجعه کرده بودیم برای این‌بخش انتخاب شدند. در این مطالعه به نوعی از نمونه‌گیری را هدفمند استفاده شده و جامعه آماری کلیه خبرگان و متخصصان سازمان‌های دفاعی در حوزه مرتبط با موضوع و نمونه آماری خبرگان و متخصصان در دسترس جامعه آماری دارای تحصیلات مرتبط می‌باشند. نمونه آماری با توجه به اینکه پژوهش کیفی و اکتشافی است، نمونه گیری به روش گلوله برفی و تا زمان اشباع نظری ادامه یافت. نمونه از بین افراد در دسترس جامعه انتخاب شد. برای تحلیل داده‌های فاز اول، داده‌های ابعاد و مولفه‌های قابل توجه در معماری حاکمیت امنیت سایبری به صورت عمومی که از مطالعات کتابخانه‌ای و تحقیقات میدانی احصا شد و به منظور تحلیل محتوای اسناد و مدارک موجود و مطالعات میدانی و همچنین احصا ابعاد و مولفه‌های بومی سازمان‌های دفاعی با مصاحبه اکتشافی با خبرگان متخصص در حوزه مربوط و

مدیران و کارشناسان خبره سازمان‌های دفاعی ابعاد ومولفه‌های نهایی استخراج شد. **در فاز دوم** پرسشنامه دارای دو قسمت تنظیم شد، قسمت اول، اطلاعات مربوط به پاسخ‌دهندگان و قسمت دوم، ابعاد و مفاهیم نهایی حاصل از فاز کیفی در این قسمت قرارداده شده و میزان اهمیت هر یک از گزاره‌ها (ابعاد) در چارچوب معماری حاکمیت امنیت سایبری در سازمان‌های دفاعی بر اساس طیف لیکرت پنج گزینه‌ای سنجیده شد.

برای تایید روایی پرسشنامه ضمن بررسی دقیق مبانی نظری موجود، جمع‌آوری و تحلیل داده‌ها از منابع مختلف و انجام مصاحبه‌ها، پرسشنامه نهایی قبل از توزیع، در اختیار خبرگان حوزه قرار داده شد و برای محاسبه روایی از تحلیل عاملی تاییدی استفاده گردید. و با توجه به خروجی بدست آمده اشتراک تمامی متغیرها بیشتر از ۰/۴ شد بنابر این تمامی سئوالات از روایی مناسبی برخوردار بودند

پس از تایید روایی نوبت به محاسبه پایایی می‌رسد. بر اساس سئوالات فرایندها و با استفاده از ضریب آلفای کرونباخ میزان پایایی فعالیت هر کدام از فرایندها بدست آمده است و از آنجا که ضریب آلفای کرونباخ در آن‌ها از ۰. ۶۶۷ بزرگتر است بنابراین ابزار پژوهش، پرسشنامه، از پایایی قابل قبولی برخوردار است.

جدول(۳)ضریب آلفای کرونباخ فرآیندها

فرآیند	تعداد فعالیتها	ضریب آلفای کرونباخ
شناخت	۲۴	۸۹۰ .۰
محافظت	۳۵	۹۳۹ .۰
تشخیص	۱۸	۹۵۸ .۰
واکنش	۱۵	۹۴۲ .۰
بازیابی	۶	۸۹۲ .۰

۳. تحلیل داده ها

روش‌های تجزیه و تحلیل اطلاعات

برای تجزیه و تحلیل داده‌ها در این پژوهش، در فاز اول، تحلیل محتوای متون و اسناد موجود و مصاحبه‌ها انجام شده است. در فاز دوم تحقیق از پرسشنامه و طیف لیکرت استفاده شده و برای بررسی روایی پرسشنامه از طریق مصاحبه و نظر نخبگان و برای بررسی پایایی پرسشنامه از طریق ثبات درونی روش آلفای کرونباخ است. که توسط نرم افزار SPSS این کار ممکن است. پس از تایید پایایی و روایی پرسشنامه و هم چنین ابعاد و مولفه‌های بدست آمده میزان اهمیت هر یک از ابعاد و مولفه‌ها از طریق آزمون تی تک نمونه‌ای استخراج می‌گردد و در نهایت درجهت ایجاد معماری حاکمیت امنیت سایبری و تلفیق دیدگاه‌های مدیریتی و فنی در یک

چارچوب از چارچوب معماری زکمن استفاده می‌گردد به طوریکه ابعاد فرآیندها و مولفه‌های بدست آمده در سطوح مدیریتی سازمان قرار گرفته و چارچوب معماری حاکمیت امنیت سایبری ایجاد می‌شود.

آمار توصیفی

نمونه آماری و حجم نمونه

در این پژوهش (همانند آنچه در پژوهش‌های کیفی رخ می‌دهد) به جای نمونه‌گیری احتمالی از نمونه‌گیری هدفمند استفاده شده است، بطوریکه در این پژوهش از خبرگان سازمان‌های دفاعی که هم سابقه کاری مرتبط و تحصیلات آکادمیک در این حوزه داشتند استفاده شد که به شرح زیر ارائه می‌گردد:

جداول(۴) اطلاعات جمعیت شناختی پاسخ دهندگان

ردیف	مقطع تحصیلی	رشته تحصیلی	سن	سابقه
۱	دکتری	مدیریت فناوری اطلاعات	۴۰	۲۳
۲	دکتری	مدیریت فناوری اطلاعات	۴۹	۲۵
۳	دکتری	سایبر	۴۳	۲۹
۴	دکتری	سایبر	۴۳	۲۸
۵	دکتری	مهندسی کامپیوتر- نرم افزار	۳۹	۲۳
۶	دکتری	مهندسی کامپیوتر- نرم افزار	۴۶	۳۰
۷	دکتری	امنیت اطلاعات	۳۹	۲۱
۸	دانشجوی دکتری	مدیریت فناوری اطلاعات	۴۰	۲۳
۹	دانشجوی دکتری	مدیریت فناوری اطلاعات	۳۸	۲۵
۱۰	دانشجوی دکتری	مدیریت فناوری اطلاعات	۳۹	۲۶
۱۱	کارشناسی ارشد	مدیریت فناوری اطلاعات	۴۴	۲۹
۱۲	کارشناسی ارشد	مدیریت فناوری اطلاعات	۳۹	۲۵
۱۳	کارشناسی ارشد	مهندسی کامپیوتر- نرم افزار	۳۸	۲۴
۱۴	کارشناسی ارشد	مهندسی کامپیوتر- نرم افزار	۳۷	۲۳
۱۵	کارشناسی ارشد	امنیت اطلاعات	۳۹	۲۶

فاز دوم

پس از به دست آوردن ابعاد و مولفه‌ها در زمینه چارچوب معماری حاکمیت امنیت سایبری در سازمان‌های دفاعی به منظور بررسی و تایید یافته‌ها، پرسشنامه‌ای تهیه و توزیع گردید و پرسشنامه‌ها به منظور تحلیل داده‌ها در اختیار خبرگان قرار گرفت. در جهت تایید نهایی فرآیندها و فعالیت‌ها و همچنین میزان اهمیت هر فعالیت خبرگان و متخصصان در دسترس

سازمان‌های دفاعی که قبلا در فاز کیفی به آن‌ها مراجعه کرده بودیم برای فاز کمی نیز انتخاب شدند که به تعداد ۱۵ نفر خبره رسید.

آمار استنباطی

فاز اول

پس از مطالعه ادبیات موضوع در مقالات، کتب، استانداردهای موجود و... به‌صورت نظام‌مند سرفصل‌های اصلی قابل توجه ابعاد و مولفه‌ها در معماری امنیت سایبری به‌صورت عمومی احصاء شد و در گام بعدی به وسیله مصاحبه با خبرگان متخصص در سازمان‌های دفاعی که تخصص آکادمیک و تجربه کاری در حوزه امنیت سایبری داشتند نظرات تخصصی آنان در جهت بومی‌سازی ابعاد و مولفه‌های یافته شده در کشور و سازمان‌های دفاعی صورت پذیرفت.

جدول (۵) فرآیندها، ابعاد و مفاهیم حاکمیت امنیت سایبری استخراج شده از فاز اول پژوهش

(فرآیندها)	ابعاد (گروه فعالیت)	مفاهیم (فعالیت‌ها)
شناخت	۱. مدیریت دارایی‌ها	۱-۱. دستگاه‌های فیزیکی و سیستم‌های موجود در سازمان لیست می‌شوند.
		۱-۲. پلت فرم‌های نرم‌افزاری و برنامه‌های کاربردی درون سازمان ثبت می‌شوند.
		۱-۳. ارتباطات سازمانی و جریان داده‌ها ترسیم می‌شوند.
		۱-۴. سیستم‌های اطلاعاتی خارجی دسته‌بندی می‌شوند.
		۱-۵. منابع بر اساس طبقه‌بندی، حساسیت و ارزش تجاری آن‌ها اولویت‌بندی می‌شوند.
		۱-۶. نقش‌ها و مسئولیت‌های سایبری در کل نیروی کار و ذینفعان ثالث ایجاد می‌شود.
	۲. محیط سازمان	۲-۱. نقش سازمان در زنجیره تأمین، شناسایی و ابلاغ می‌گردد.
		۲-۲. جایگاه سازمان در زیرساخت‌های حیاتی وبخش صنعت آن شناسایی و ابلاغ می‌گردد.
		۲-۳. اولویت مأموریت‌ها، اهداف و فعالیت‌های سازمان مشخص شده و ابلاغ می‌گردد.
		۲-۴. وابستگی‌ها و کاربردهای حیاتی برای فراهم آوردن خدمات حیاتی ایجاد و ابلاغ می‌شوند.
		۲-۵. نیازمندی‌های مقاومت برای پشتیبانی از سرویس‌های حیاتی ایجاد می‌شوند.
	۳. حاکمیت	۳-۱. سیاست‌های امنیتی اطلاعات سازمان ایجاد می‌گردند.
		۳-۲. نقش‌های امنیتی اطلاعات و مسئولیت‌ها با همکاران درونی و بیرونی هماهنگ و منطبق می‌شوند.
		۳-۳. نیازمندی‌های قانونی و تنظیمی در زمینه امنیت سایبری، ازجمله وظایف در جهت آزادی‌های شخصی و اجتماعی تفهیم شده و مدیریت می‌شوند.
		۳-۴. فرآیندهای اجرایی و مدیریت ریسک، خطرات امنیت سایبری را بررسی می‌کنند.
	۴. ارزیابی	۴-۱. آسیب‌پذیری‌های دارایی‌ها شناسایی و مستند می‌شوند.

(فرآیندها)	ابعاد (گروه فعالیت)	مفاهیم (فعالیت‌ها)
	ریسک	۴-۲هوشیاری‌های تهدید سایبری از انجمن‌ها و منابع به اشتراک‌گذاری اطلاعات دریافت می‌شود.
		۴-۳. تهدیدات، داخلی و خارجی، شناسایی و مستند می‌شوند.
		۴-۴. اثرات و احتمالات تجاری بالقوه شناسایی می‌شود.
		۴-۵. تهدید، آسیب‌پذیری، احتمال و تأثیرات برای تعیین خطر استفاده می‌شود.
		۴-۶. پاسخ به خطرات شناسایی و اولویت‌بندی می‌شوند.
	۵. استراتژی مدیریت ریسک	۵-۱. فرآیندهای مدیریت ریسک ایجاد شده، مدیریت شده و با ذینفعان سازمانی توافق می‌شود.
		۵-۲. تحمل ریسک سازمانی مشخص و بطور واضح بیان می‌شود.
		۵-۳. بوسیله‌بخش تجزیه و تحلیل ریسک، میزان تحمل ریسک سازمان و نقش آن در زیرساختهای حیاتی تعیین می‌شود.
محافظت	۱. کنترل دسترسی	۱-۱. هویت‌ها و میزان اعتبار برای دستگاه‌ها، کاربران و فرآیندهای مجاز صادر، مدیریت و حسابرسی می‌شوند.
		۱-۲. دسترسی فیزیکی به دارایی‌ها مدیریت شده و از آن محافظت می‌شود.
		۱-۳. دسترسی از راه دور مدیریت می‌شود.
		۱-۴. مجوزهای دسترسی، که شامل اصول کمترین امتیاز و تفکیک وظایف است مدیریت می‌شوند
		۱-۵. یکپارچگی شبکه محافظت می‌شود و درصورت لزوم جداسازی شبکه نیز به کار گرفته می‌شود.
	۲. آگاه‌سازی و مهارت‌آموزی	۲-۱. به همه کابران اطلاع رسانی انجام شود و تحت آموزش قرار می‌گیرند.
		۲-۲. کاربران خاص، نقش و مسئولیت‌ها را می‌آموزند.
		۲-۳. ذینفعان ثالث (به‌عنوان مثال، تأمین کنندگان، مشتریان، شرکا) نسبت به نقش‌ها و مسئولیت‌هایشان آگاه می‌شوند.
		۲-۴. مدیران ارشد نقش‌ها و مسئولیت‌ها را فرا می‌آموزند.
		۲-۵. پرسنل امنیت فیزیکی و اطلاعاتی نقش‌ها و مسئولیت‌ها را می‌آموزند.
	۳. امنیت اطلاعات	۳-۱. اطلاعات ساکن محافظت می‌شود.
		۳-۲. داده در حال حمل و نقل محافظت می‌شود.
		۳-۳. دارایی‌ها به‌طور رسمی در طول حذف، انتقال و توزیع مدیریت می‌شود.
		۳-۴. ظرفیت مناسب برای اطمینان از دردسترس بودن حفظ می‌شود.
		۳-۵. حفاظت در برابر نشت اطلاعات اجرا می‌شود.

(فرآیندها)	ابعاد (گروه فعالیت)	مفاهیم (فعالیت‌ها)
		۳-۶. مکانیسم‌های بررسی یکپارچگی برای تأیید نرم‌افزارها، ثابت افزارها[۳] و صحت اطلاعات استفاده می‌شود.
		۳-۷. محیط‌های توسعه و آزمایش جدا از محیط تولید باشد.
	۴. فرآیندها و رویه‌های حفاظت از اطلاعات	۴-۱. پیکربندی پایه‌ای سیستم‌های اطلاعاتی، فناوری اطلاعات و سیستم‌های صنعتی ایجاد و حفظ می‌شود.
		۴-۲. یک چرخه‌ای عمر توسعه سیستم برای مدیریت سیستم‌ها پیاده‌سازی شود
		۴-۳. فرآیندهای کنترل پیکربندی در جای خود قرار می‌گیرند.
		۴-۴. پشتیبان‌گیری از اطلاعات انجام، حفظ و به‌صورت دوره‌ای آزمایش می‌شود.
		۴-۵. سیاست و مقررات مربوط به محیط عملیاتی فیزیکی برای دارایی‌های سازمانی اجرا می‌شود.
		۴-۶. داده‌ها طبق سیاست‌گذاری‌ها امحا می‌شوند.
		۴-۷. فرآیندهای حفاظت به طور مداوم بهبود می‌یابد.
		۴-۸. اثربخشی فن‌آوری های حفاظت با اشخاص مناسب به اشتراک گذاشته می‌شود.
		۴-۹. طرح‌های واکنش (واکنش حادثه و تداوم کسب و کار) و برنامه‌های بهبود (بازیابی حادثه و فاجعه) در جای خود قرارگرفته و مدیریت می‌شود.
		۴-۱۰. برنامه‌های پاسخ و بازیابی آزمایش می‌شوند.
		۴-۱۱. امنیت سایبری در کارهای منابع انسانی (از جمله برنامه نویسی، کنترل دسترسی پرسنل).
		۴-۱۲. یک برنامه مدیریت آسیب ذیری توسعه داده شده و اجرا می‌شود.
	۵. نگهداری	۵-۱. تعمیر و نگهداری و حفاظت از دارایی‌های سازمانی به صورت مرتب با ابزارهای تأیید شده و کنترل شده انجام می‌شود.
		۵-۲. نگهداری از راه دور دارایی‌های سازمانی اجرا شده وبا ابزار مورد تایید و کنترل شده به موقع ثبت می‌شوند.
	۶. فناوری‌های محافظت	۶-۱. سوابق ممیزی، جمع‌آوری، مستندسازی، پیاده‌سازی و مطابق با قوانین بررسی می‌شود.
		۶-۲. رسانه‌های قابل حمل محافظت شده و استفاده از آن‌ها بر اساس قوانین محدود می‌شود.
		۶-۳. دسترسی به سیستم‌ها و دارایی‌ها کنترل می‌شود و اصل داشتن حداقل کارکرد به کار گرفته می‌شود.
		۶-۴. شبکه‌های ارتباطات و کنترل محافظت می‌شوند.
تشخیص	۱. وقایع و ناهنجاری‌ها	۱-۱. یک زیرساخت از عملیات‌های شبکه و جریان داده مورد انتظار برای کاربران و سیستم‌ها ایجاد و مدیریت می‌شود.

[۳] برنامه‌های تقریباً ثابت و نسبتاً کوچک یا ساختمان‌های داده های که درون سخت‌افزار انواع دستگاه‌های الکترونیک است

(فرآیندها)	ابعاد (گروه فعالیت)	مفاهیم (فعالیت‌ها)
		۲-۱. رویدادهای شناسایی شده برای فهمیدن اهداف و روش‌های حمله تجزیه وتحلیل می‌شوند.
		۳-۱. داده‌های رویدادها جمع می‌شوند و ازطریق منابع مختلف و حسگرها بهم مرتبط می‌شوند.
		۴-۱. تأثیر رویدادها تعیین می‌شود.
		۵-۱. آستانه هشدار حوادث مشخص می‌شود.
	۲. مانیتورینگ و نظارت امنیتی پیوسته	۱-۲. شبکه برای شناسایی رویدادهای امنیتی احتمالی سایبری نظارت می‌شود.
		۲-۲. محیط فیزیکی برای شناسایی رویدادهای امنیتی احتمالی سایبری نظارت می‌شود.
		۳-۲. فعالیت‌های کارکنان برای شناسایی رویدادهای امنیتی احتمالی سایبری نظارت می‌شود.
		۴-۲. کدهای مخرب شناسایی می‌شود.
		۵-۲. کدهای تلفن همراه و شماره تلفن‌های غیرمجاز شناسایی می‌شود
		۶-۲. فعالیت‌های خدمات دهندگان خارجی برای شناسایی رویدادهای احتمالی سایبری نظارت می‌شود.
		۷-۲. نظارت بر کارکنان، اتصالات، دستگاه‌ها و نرم‌افزاری غیر مجاز انجام می‌شود.
		۸-۲. اسکن آسیب‌پذیری‌ها انجام می‌شود.
	۳. فرآیندهای تشخیص	۱-۳. نقش‌ها و مسئولیت‌های تشخیص به خوبی تعریف شده است تا مسئولیت‌پذیری را تضمین کند.
		۲-۳. فعالیت‌های تشخیص مطابق با تمام الزامات قابل اجرا می‌شود.
		۳-۳. فرآیندهای تشخیص آزمایش می‌شوند.
		۴-۳. اطلاعات تشخیص رویداد به طرف احزاب مناسب ارسال می‌شود.
		۵-۳. فرآیندهای تشخیص به طور مداوم بهبود می‌یابد.
واکنش	۱. برنامه‌ریزی پاسخ	۱-۱. طرح واکنش در زمان انجام یک رخداد یا پس از رویداد اجرا می‌شود.
	۲. تعاملات	۱-۲. پرسنل نقش‌ها و ترتیب فرآیندها را زمانی که عکس‌العملی نیاز است می‌دانند.
		۲-۲. رویدادها مطابق با معیارهای مشخص شده گزارش می‌شود.
		۳-۲. اطلاعات بر اساس نقشه‌های پاسخگویی به اشتراک گذاشته می‌شود.
		۴-۲. هماهنگی با ذینفعان مطابق با نقشه‌های پاسخگویی صورت می‌گیرد.
		۵-۲. به اشتراک‌گذاری داوطلبانه اطلاعات با ذینفعان خارجی برای دستیابی به آگاهی بیشتر در زمینه وضعیت امنیتی سایبری صورت می‌گیرد.
	۳. تحلیل	۱-۳. اطلاعیه‌ها از سیستم‌های تشخیص مورد بررسی قرار می‌گیرند.
		۲-۳. تأثیر حادثه آموخته می‌شود.
		۳-۳. دادرسی قانونی انجام می‌شود.

(فرآیندها)	ابعاد (گروه فعالیت)	مفاهیم (فعالیت‌ها)
		۴-۳. رخدادها در راستای نقشه‌های عملکرد دسته‌بندی می‌شوند.
	۴. کاهش آسیب‌پذیری‌ها	۴-۱. رخدادها مهار می‌شوند.
		۴-۲. حوادث کاهش می‌یابد.
		۴-۳. آسیب‌پذیری‌های شناسایی شده جدید، کاهش یابند یا به‌عنوان خطرات پذیرفته شده مستند می‌گردند.
	۵. بهینه‌سازی	۵-۱. درس‌های آموخته شده در طرح‌های واکنش اعمال گردد.
		۵-۲. استراتژی‌های پاسخ به‌روزرسانی می‌شود
بازیابی	۱. برنامه‌ریزی بازیابی	۱-۱. برنامه بازیابی در حین یا پس از یک رویداد اجراء می‌شود.
	۲. بهبودسازی‌ها	۲-۱. با توجه به درس‌های آموخته شده، طرح‌های بازیابی را بهبود می‌بخشند.
		۲-۲. استراتژی بازیابی به‌روز می‌شود.
	۱. روابط سازمانی و ارتباطات	۳-۱. روابط عمومی مدیریت می‌شوند.
		۳-۲. اعتبار سازمان پس از رویداد بازسازی می‌شود.
		۳-۳. فعالیت‌های بازیابی به ذینفعان داخلی و خارجی و همچنین تیم‌های اجرایی و مدیریتی ابلاغ می‌شود

۴-۳-۲- فازدوم

بر اساس مضامین، ابعاد و مفاهیم بدست آمده دربخش کیفی (جدول ۵)، پرسشنامه‌ای تنظیم شد و از طریق ارائه به خبرگان شناسایی شده این مضامین، ابعاد و مفاهیم نهایی شده و سطح معنی‌داری هر کدام مشخص شد.

۴-۴- روش‌های تجزیه و تحلیل اطلاعات

بعد از تایید پایایی و روایی پرسشنامه و هم چنین ابعاد و مفاهیم به‌دست آمده سطح معناداری هر یک از مفاهیم از طریق آزمون تی تک نمونه‌ای استخراج گردید. تصمیم‌گیری در خصوص وضعیت مناسب مفاهیم تحقیق، بستگی به سطح معنی داری آزمون تی تک نمونه‌ای دارد. اگر سطح معنی‌داری (sig) بالاتر از ۰. ۰۵ باشد، وضعیت آن متغیر مناسب نیست و اگر کمتر از این مقدار باشد قابل قبول است. همانطور که در خروجی مشاهده می‌گردد سطح معنی داری سوالات ۸، ۱۱، ۲۱، ۷۵، ۸۰، ۸۲ بالاتر از پنج صدم است، یعنی شش مفهوم از جدول ابعاد و مفاهیم بدست آمده اولیه در فاز کیفی حذف می‌گردد.

یافته‌های پژوهش: ارائه چارچوب پیشنهادی چارچوب معماری حاکمیت امنیت سایبری در سازمان‌های دفاعی جمهوری اسلامی ایران

به منظور ارائه چارچوب پیشنهادی چارچوب معماری حاکمیت امنیت سایبری در سازمان‌های دفاعی جمهوری اسلامی ایران بر مبنای چارچوب معماری سازمانی زکمن، تمامی فرآیندها و فعالیت‌ها حاکمیت امنیت سایبری را در سه سطح سازمانی در یک ماتریس زکمن قرار داده تا در نهایت به یک چارچوب معماری حاکمیت امنیت سایبری در سازمان‌های دفاعی دست یابیم که بتواند هر دو دیدگاه مدیریتی و فنی را پوشش دهد. در این ماتریس، سطرها نشان دهنده منظرهای مختلف سطوح سازمانی است و ستون‌ها بیانگر فعالیت‌های مختلف در پنج فرآیند مورد نیاز معماری حاکمیت امنیت سایبری است.

المان‌های کلیدی امنیت اطلاعات (ستون‌های چارچوب)

با بررسی چارچوب‌های مختلف امنیت سایبری و استفاده از نظر خبرگان سازمان‌های دفاع و در نهایت تحلیل کیفی و کمی در سازمان‌های دفاعی و همینطور سایر صنایع، فرآیندهای ذیل در بحث معماری امنیت سایبری با نگاهی جامع گرایانه استخراج شد:

۱. شناخت[4]: درک سازمانی را برای مدیریت خطر امنیت سایبری برای سیستم‌ها، افراد، دارایی‌ها، داده‌ها و قابلیت‌ها ایجاد می‌کند.
۲. محافظت[5]: اقدامات پیشگیرانه مناسب برای اطمینان از ارائه خدمات مهم ایجاد و پیاده‌سازی می‌شود.
۳. تشخیص[6]: فعالیت‌های مناسب برای شناسایی وقوع یک رویداد امنیت سایبری توسعه و اجرا می‌کند.
۴. واکنش[7]: فعالیت‌های مناسب را برای انجام اقدامات در پاسخ به یک حادثه سایبری شناسایی شده، توسعه داده و پیاده‌سازی می‌کند.
۵. بازیابی[8]: توسعه و پیاده‌سازی فعالیت‌های مناسب برای نگهداری از تاب‌آوری و بازیابی هرگونه قابلیت و یا خدماتی که به دلیل امنیت سایبری مختل شده‌اند

با توجه به المان‌های فوق می‌توان گفت چارچوب پیشنهادی باید به گونه‌ای طراحی شود که المان‌های فوق را پوشش دهد. بنابراین میان هر یک از ستون‌های چارچوب زکمن و المان‌های

[4] Identify
[5] Protect
[6] Detect
[7] Respond
[8] Recover

فوق تناظر برقرار شده است. جدول۷ نشان دهنده ارتباط میان المان‌ها و ستون‌های چارچوب زکمن است:

جدول(۷)فرآیندهای معماری حاکمیت امنیت سایبری در ستون‌های چارچوب زکمن در چارچوب پیشنهادی

فرآیندهای امنیت سایبری در سازمان	شناسایی	محافظت	تشخیص	واکنش	بازیابی

فعالیتهای مرتبط با امنیت اطلاعات: سطرهای چارچوب

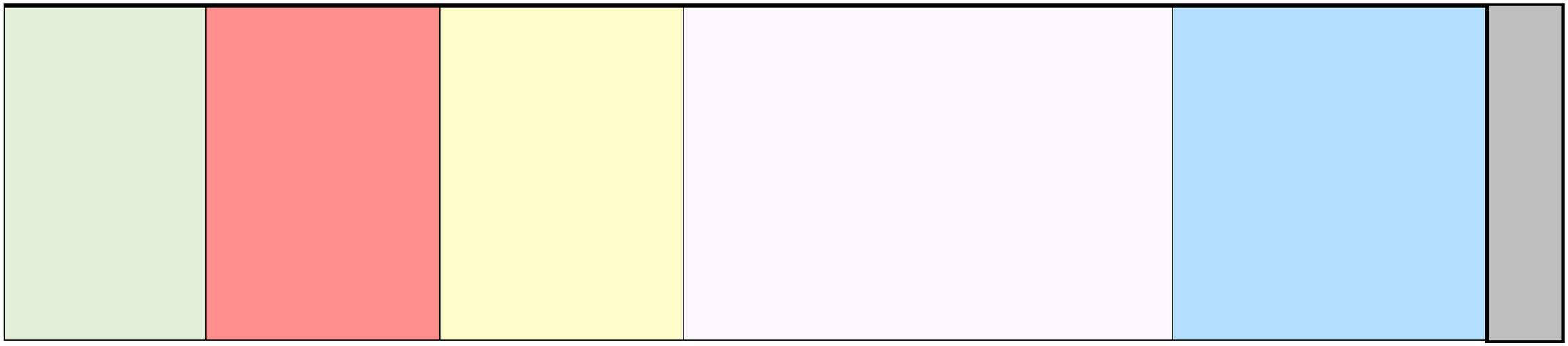
به منظور ارائه چارچوب، پنج ستون ماتریس زکمن فرآیندهای معماری حاکمیت امنیت سایبری قرار گرفت. و فعالیت‌هایی که برای اجرای هرکدام از این فرآیندها لازم است مشخص شد و در قالب ردیف‌های ماتریس و هر کدام از منظر سطوح سازمانی در نظر گرفته شد، به‌طوریکه درهر سطح سازمانی مشخص می‌نماید که چه فعالیت‌هایی در خصوص فرآیندهای دستیابی به حاکمیت امنیت سایبری را باید انجام دهند بنابراین. بالاترین لایه، منظر راهبردی، که مربوط به مدیران سطح بالا و استراتژیک سازمان می‌باشند. سطر دوم منظر تاکتیکی است که به فعالیت‌هایی اشاره دارد که می‌بایست توسط مدیران میانی مد نظر قرار گیرد و هدایت و کنترل شود. و در سطح سوم منظر عملیاتی است، که استانداردهایی را برای چگونگی وظایف اجرایی از استانداردهای معروف امنیت سایبری یافته و تعیین نموده‌ایم.

جدول(۸) چارچوب پیشنهادی معماری حاکمیت امنیت سایبری در سازمان‌های دفاعی برمبنای چارچوب زکمن

	شناسایی	محافظت	تشخیص	واکنش	بازیابی
سطح استراتژیک	۱. مدیریت دارایی‌ها ۲. محیط سازمان ۳. حاکمیت ۴. ارزیابی ریسک ۵. استراتژی مدیریت ریسک	۱. سیاستهای کنترل دسترسی ۲. آگاه‌سازی و مهارت‌آموزی ۳. امنیت اطلاعات ۴. فرآیندها و مراحل حفاظت از اطلاعات ۵. نگهداری ۶. فناوری‌های محافظت	۱. رویدادها و ناهنجاری‌ها ۲. مانیتورینگ امنیتی پیوسته ۳. فرآیندهای تشخیص	۱. برنامه‌ریزی پاسخ ۲. تعاملات ۳. تحلیل ۴. کاهش آسیب‌پذیری‌ها ۵. بهینه‌سازی	۱. برنامه‌ریزی بازیابی ۲. بهبودسازی‌ها ۳. ارتباطات
سطح میانی	۱-۱. دستگاه‌های فیزیکی و سیستم‌های موجود در سازمان لیست می‌شوند. ۱-۲. پلت فرم‌های نرم‌افزاری و برنامه‌های کاربردی درون سازمان ثبت می‌شوند. ۱-۳. ارتباطات سازمانی و جریان داده‌ها ترسیم می‌شوند. ۱-۴. سیستم‌های اطلاعاتی خارجی دسته‌بندی می‌شوند. ۱-۵. منابع (به‌عنوان مثال، سخت افزار، دستگاه‌ها، داده‌ها و نرم افزار) بر اساس طبقه‌بندی، حساسیت و ارزش تجاری آن‌ها اولویت‌بندی می‌شوند. ۱-۶. نقش‌ها و مسئولیت‌های سایبری در کل نیروی کار و ذینفعان ثالث (به‌عنوان مثال، تأمین‌کنندگان، مشتریان، شرکا) ایجاد می‌شود. ۲-۱. نقش سازمان در زنجیره تأمین، شناسایی و ابلاغ می‌گردد. ۲-۲. اولویت مأموریت‌ها، اهداف و فعالیت‌های سازمان مشخص شده و ابلاغ می‌گردد. ۲-۳. وابستگی‌ها و کاربردهای حیاتی برای فراهم آوردن خدمات حیاتی ایجاد شده و ابلاغ می‌شوند. ۳-۱. سیاست‌های امنیتی اطلاعات سازمان ایجاد می‌گردند. ۳-۲. نقش‌های امنیتی اطلاعات و مسئولیت‌ها با همکاران درونی و بیرونی هماهنگ و منطبق می‌شوند. ۳-۳. نیازمندی‌های قانونی و تنظیمی در زمینه امنیت سایبری، ازجمله وظایف در جهت آزادی‌های شخصی و اجتماعی تفهیم شده و مدیریت می‌شوند. ۳-۴. فرایندهای اجرایی و مدیریت ریسک، خطرات امنیت سایبری را بررسی می‌کنند. ۴-۱. آسیب‌پذیری‌های دارایی‌ها شناسایی و مستند می‌شوند. ۴-۲. اطلاعات آسیب‌پذیری تهدید از انجمن‌ها و منابع به اشتراک‌گذاری اطلاعات دریافت می‌شود. ۴-۳. تهدیدات، داخلی و خارجی، شناسایی و مستند می‌شوند. ۴-۴. اثرات و احتمالات تجاری بالقوه شناسایی می‌شود. ۴-۵. تهدید، آسیب‌پذیری، احتمال و تأثیرات برای تعیین خطر استفاده می‌شود. ۵-۱. فرایندهای مدیریت ریسک ایجاد شده، مدیریت شده و با ذینفعان سازمانی توافق می‌شود. ۵-۲. تحمل ریسک سازمانی مشخص و بطور واضح بیان می‌شود. ۵-۳. تصمیمات سازمان در مورد تحمل خطر توسط نقش آن در زیرساخت‌های بحرانی و تجزیه و تحلیل خطرات مشخص معین می‌شود.	۱-۱. هویت و اعتبارهای دستگاه‌ها و کاربران مجاز و مدیریت می‌شوند. ۱-۲. دسترسی فیزیکی به دارایی‌ها مدیریت شده و از آن محافظت می‌شود. ۱-۳. دسترسی از راه دور مدیریت می‌شود. ۱-۴. مجوزهای دسترسی مدیریت شده و اصول حداقل امتیاز تفکیک وظایف را به کار می‌گیرند. ۱-۵. یکپارچگی شبکه محافظت می‌شود و درصورت لزوم جداسازی شبکه نیز به کار گرفته می‌شود. ۲-۱. به همه کابران اطلاع رسانی شده و تحت آموزش قرار می‌گیرند. ۲-۲. کاربران صاحب امتیاز، نقش و مسئولیت‌ها را می‌آموزند. ۲-۳. ذینفعان ثالث (به‌عنوان مثال، تأمین کنندگان، مشتریان، شرکا) نقش و مسئولیت‌ها را می‌آموزند. ۲-۴. مدیران ارشد نقش‌ها و مسئولیت‌ها را فرا می‌آموزند. ۲-۵. پرسنل امنیتی فیزیکی و اطلاعاتی نقش و مسئولیت را می‌آموزند. ۳-۱. اطلاعات ساکن محافظت می‌شود. ۳-۲. داده در حال حمل و نقل محافظت می‌شود. ۳-۳. دارایی‌ها به‌طور رسمی در طول حذف، انتقال و توزیع مدیریت می‌شود. ۳-۴. ظرفیت مناسب برای اطمینان از در دسترس بودن حفظ می‌شود. ۳-۵. حفاظت در برابر درز شدن داده‌ها اجرا می‌شود. ۳-۶. مکانیسم‌های بررسی یکپارچگی برای تأیید نرم‌افزار، سفت افزار و صحت اطلاعات استفاده می‌شود. ۳-۷. محیط‌های توسعه و آزمایش جدا از محیط تولید است. ۴-۱. پیکربندی پایه‌ای سیستم‌های اطلاعاتی فناوری اطلاعات و سیستم‌های صنعتی ایجاد و حفظ می‌شود. ۴-۲. چرخه‌ای از زندگی برای توسعه سیستم‌ها به کار گرفته می‌شود. ۴-۳. فرایندهای کنترل پیکربندی در جای خود قرار می‌گیرند. ۴-۴. پشتیبان‌گیری از اطلاعات انجام، حفظ و به‌صورت دوره‌ای آزمایش می‌شود. ۴-۵. سیاست و مقررات مربوط به محیط عملیاتی فیزیکی برای دارایی‌های سازمانی برآورده می‌شود. ۴-۶. داده‌ها طبق سیاست‌گذاری‌ها تخریب می‌شوند. ۴-۷. فرآیندهای حفاظت به طور مداوم بهبود می‌یابد. ۴-۸. اثربخشی فن‌آوری های حفاظت با اشخاص مناسب به اشتراک گذاشته می‌شود. ۴-۹. طرح‌های واکنش (واکنش حادثه و تداوم کسب و کار) و برنامه‌های بهبود (بازیابی حادثه و فاجعه) در جای خود قرارگرفته و مدیریت می‌شود. ۴-۱۰. برنامه‌های پاسخ و بازیابی آزمایش می‌شوند. ۴-۱۱. امنیت سایبری در کارهای منابع انسانی (از جمله برنامه نویسی، بازرسی پرسنل). ۴-۱۲. یک برنامه مدیریت آسیب‌پذیری توسعه داده شده و اجرا می‌شود. ۵-۱. تعمیر و نگهداری و حفاظت از دارایی‌های سازمانی به صورت مرتب با ابزارهای تأیید شده و کنترل شده انجام می‌شود. ۵-۲. نگهداری از راه دور دارایی‌های سازمانی اجرا شده وبا ابزار مورد تایید و کنترل شده به موقع ثبت می‌شوند. ۶-۱. سوابق ممیزی، جمع‌آوری، مستندسازی، پیاده‌سازی و مطابق با قوانین بررسی می‌شود. ۶-۲. رسانه‌های قابل حمل محافظت شده و استفاده از آنها بر اساس قوانین محدود می‌شود. ۶-۳. دسترسی به سیستم‌ها و دارایی‌ها کنترل می‌شود و اصل داشتن حداقل کارکرد به کار گرفته می‌شود. ۶-۴. شبکه‌های ارتباطات و کنترل محافظت می‌شوند.	۱-۱. خط مبنایی از عملیات شبکه و جریان داده مورد انتظار برای کاربران و سیستم‌ها ایجاد و مدیریت می‌شود. ۱-۲. حوادث مشخص شده برای درک اهداف و روش‌های حمله تحلیل می‌شوند. ۱-۳. داده‌های رویدادها جمع می‌شوند و ازطریق منابع مختلف و حسگرها همبسته می‌شوند. ۱-۴. تأثیر رویدادها تعیین می‌شود. ۱-۵. آستانه هشدار حوادث ایجاد می‌شود. ۲-۱. شبکه برای شناسایی رویدادهای امنیتی احتمالی سایبری نظارت می‌شود. ۲-۲. محیط فیزیکی برای شناسایی رویدادهای امنیتی احتمالی سایبری نظارت می‌شود. ۲-۳. فعالیت‌های کارکنان برای شناسایی رویدادهای امنیتی احتمالی سایبری نظارت می‌شود. ۲-۴. کد مخرب شناسایی می‌شود. ۲-۵. کد تلفن غیر مجاز شناسایی می‌شود. ۲-۶. فعالیت‌های ارائه‌دهنده خدمات خارجی برای شناسایی رویدادهای احتمالی سایبری نظارت می‌شود. ۲-۷. نظارت بر کارکنان غیر مجاز، اتصالات، دستگاه‌ها و نرم‌افزار انجام می‌شود. ۲-۸. اسکن آسیب‌پذیری انجام می‌شود. ۳-۱. نقش و مسئولیت شناسایی به خوبی تعریف شده است تا مسئولیت‌پذیری را تضمین کند. ۳-۲. فعالیت‌های تشخیص مطابق با تمام الزامات قابل اجرا است. ۳-۳. فرایندهای تشخیص آزمایش می‌شوند. ۳-۴. فرآیندهای تشخیص به طور مداوم بهبود می‌یابد.	طرح واکنش در طی یا پس از یک رویداد اجرا می‌شود. ۲-۱. پرسنل نقش‌ها و ترتیب فرآیندها را زمانی که عکس‌العملی نیاز است می‌دانند. ۲-۲. رویدادها مطابق با معیارهای مشخص شده گزارش می‌شود. ۲-۳. هماهنگی با ذینفعان مطابق با نقشه‌های پاسخگویی صورت می‌گیرد. ۳-۱. اطلاعیه‌ها از سیستم‌های تشخیص مورد بررسی قرار می‌گیرند. ۳-۲. تأثیر حادثه آموخته می‌شود. ۳-۳. دادرسی قانونی انجام می‌شود. ۳-۴. رخدادها در راستای نقشه‌های عملکرد دسته‌بندی می‌شوند. ۴-۱. رخدادها مهار می‌شوند. ۴-۲. حوادث کاهش می‌یابد. ۴-۳. آسیب‌پذیری‌های شناسایی شده جدید، کاهش یابند یا به‌عنوان خطرات پذیرفته شده مستند گردند. ۵-۱. درس‌های آموخته شده در طرح‌های واکنش اعمال گردد. ۵-۲. استراتژی‌های پاسخ به‌روزرسانی می‌شود.	۱-۱. برنامه بازیابی در حین یا پس از یک رویداد اجراء می‌شود. ۱-۲. با توجه به درس‌های آموخته شده، طرح‌های بازیابی را بهبود می‌بخشند. ۲-۲. استراتژی بازیابی به‌روز می‌شود. ۳-۱. روابط عمومی مدیریت می‌شوند. ۳-۲. اعتبار پس از زمانی که یک رویداد بازسازی شده است. ۳-۳. فعالیت‌های بازیابی به ذینفعان داخلی و تیم‌های اجرایی و مدیریتی مخابره می‌شوند.

سطح اجرایی (استانداردهای اجرایی)	۱-۱. CCS CSC 1 COBIT 5 BAI09. 01, BAI09. 02 ISA 62443-2-1: 2009 4. 2. 3. 4 ISA 62443-3-3: 2013 SR 7. 8 ISO/IEC 27001: 2013 A. 8. 1. 1, A. 8. 1. 2 NIST SP 800-53 Rev. 4 CM-8 ۱-۲. CCS CSC 2 COBIT 5 BAI09. 01, BAI09. 02, BAI09. 05 ISA 62443-2-1: 2009 4. 2. 3. 4 ISA 62443-3-3: 2013 SR 7. 8 ISO/IEC 27001: 2013 A. 8. 1. 1, A. 8. 1. 2 NIST SP 800-53 Rev. 4 CM-8 ۱-۳. CCS CSC 1 COBIT 5 DSS05. 02 ISA 62443-2-1: 2009 4. 2. 3. 4 ISO/IEC 27001: 2013 A. 13. 2. 1 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8 ۱-۴. COBIT 5 APO02. 02 ISO/IEC 27001: 2013 A. 11. 2. 6 NIST SP 800-53 Rev. 4 AC-20, SA-9 ۱-۵. COBIT 5 APO03. 03, APO03. 04, BAI09. 02 ISA 62443-2-1: 2009 4. 2. 3. 6 ISO/IEC 27001: 2013 A. 8. 2. 1 NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14 ۱-۶. COBIT 5 APO01. 02, DSS06. 03 ISA 62443-2-1: 2009 4. 3. 2. 3. 3 ISO/IEC 27001: 2013 A. 6. 1. 1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11 ۲-۱. COBIT 5 APO08. 04, APO08. 05, APO10. 03, APO10. 04, APO10. 05 ISO/IEC 27001: 2013 A. 15. 1. 3, A. 15. 2. 1, A. 15. 2. 2 NIST SP 800-53 Rev. 4 CP-2, SA-12 ۲-۲. COBIT 5 APO02. 01, APO02. 06, APO03. 01 ISA 62443-2-1: 2009 4. 2. 2. 1, 4. 2. 3. 6 NIST SP 800-53 Rev. 4 PM-11, SA-14 ۲-۳. ISO/IEC 27001: 2013 A. 11. 2. 2, A. 11. 2. 3, A. 12. 1. 3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14 ۳-۱. COBIT 5 APO01. 03, EDM01. 01, EDM01. 02 ISA 62443-2-1: 2009 4. 3. 2. 6 ISO/IEC 27001: 2013 A. 5. 1. 1 NIST SP 800-53 Rev. 4 -1 controls from all families ۳-۲. COBIT 5 APO13. 12 ISA 62443-2-1: 2009 4. 3. 2. 3. 3 ISO/IEC 27001: 2013 A. 6. 1. 1, A. 7. 2. 1 NIST SP 800-53 Rev. 4 PM-1, PS-7 ۳-۳. COBIT 5 MEA03. 01, MEA03. 04 ISA 62443-2-1: 2009 4. 4. 3. 7 ISO/IEC 27001: 2013 A. 18. 1 NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1) ۳-۴. COBIT 5 DSS04. 02 ISA 62443-2-1: 2009 4. 2. 3. 1, 4. 2. 3. 3, 4. 2. 3. 8, 4. 2. 3. 9, 4. 2. 3. 11, 4. 3. 2. 4. 3, 4. 3. 2. 6. 3 NIST SP 800-53 Rev. 4 PM-9, PM-11 ۴-۱. CCS CSC 4 COBIT 5 APO12. 01, APO12. 02, APO12. 03, APO12. 04 ISA 62443-2-1: 2009 4. 2. 3, 4. 2. 3. 7, 4. 2. 3. 9, 4. 2. 3. 12 ISO/IEC 27001: 2013 A. 12. 6. 1, A. 18. 2. 3 NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 ۴-۲. ISA 62443-2-1: 2009 4. 2. 3, 4. 2. 3. 9, 4. 2. 3. 12 ISO/IEC 27001: 2013 A. 6. 1. 4 NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5 ۴-۳. COBIT 5 APO12. 01, APO12. 02, APO12. 03, APO12. 04 ISA 62443-2-1: 2009 4. 2. 3, 4. 2. 3. 9, 4. 2. 3. 12 NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16	۱-۱. CCS CSC 16 COBIT 5 DSS05. 04, DSS06. 03 ISA 62443-2-1: 2009 4. 3. 3. 5. 1 ISA 62443-3-3: 2013 SR 1. 1, SR 1. 2, SR 1. 3, SR 1. 4, SR 1. 5, SR 1. 7, SR 1. 8, SR 1. 9 ISO/IEC 27001: 2013 A. 9. 2. 1, A. 9. 2. 2, A. 9. 2. 4, A. 9. 3. 1, A. 9. 4. 2, A. 9. 4. 3 NIST SP 800-53 Rev. 4 AC-2, IA Family ۱-۲. COBIT 5 DSS01. 04, DSS05. 05 ISA 62443-2-1: 2009 4. 3. 3. 3. 2, 4. 3. 3. 3. 8 ISO/IEC 27001: 2013 A. 11. 1. 1, A. 11. 1. 2, A. 11. 1. 4, A. 11. 1. 6, A. 11. 2. 3 NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9 ۱-۳. COBIT 5 APO13. 01, DSS01. 04, DSS05. 03 ISA 62443-2-1: 2009 4. 3. 3. 6. 6 ISA 62443-3-3: 2013 SR 1. 13, SR 2. 6 ISO/IEC 27001: 2013 A. 6. 2. 2, A. 13. 1. 1, A. 13. 2. 1 NIST SP 800-53 Rev. 4 AC- 17, AC-19, AC-20 ۱-۴. CCS CSC 12, 15 ISA 62443-2-1: 2009 4. 3. 3. 7. 3 ISA 62443-3-3: 2013 SR 2. 1 ISO/IEC 27001: 2013 A. 6. 1. 2, A. 9. 1. 2, A. 9. 2. 3, A. 9. 4. 1, A. 9. 4. 4 NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16 ۱-۵. ISA 62443-2-1: 2009 4. 3. 3. 4 ISA 62443-3-3: 2013 SR 3. 1, SR 3. 8 ISO/IEC 27001: 2013 A. 13. 1. 1, A. 13. 1. 3, A. 13. 2. 1 NIST SP 800-53 Rev. 4 AC-4, SC-7 ۲-۱. CCS CSC 9 COBIT 5 APO07. 03, BAI05. 07 ISA 62443-2-1: 2009 4. 3. 2. 4. 2 ISO/IEC 27001: 2013 A. 7. 2. 2 NIST SP 800-53 Rev. 4 AT-2, PM-13 ۲-۲. CCS CSC 9 COBIT 5 APO07. 02, DSS06. 03 ISA 62443-2-1: 2009 4. 3. 2. 4. 2, 4. 3. 2. 4. 3 ISO/IEC 27001: 2013 A. 6. 1. 1, A. 7. 2. 2 NIST SP 800-53 Rev. 4 AT-3, PM-13 ۲-۳. CCS CSC 9 COBIT 5 APO07. 03, APO10. 04, APO10. 05 ISA 62443-2-1: 2009 4. 3. 2. 4. 2 ISO/IEC 27001: 2013 A. 6. 1. 1, A. 7. 2. 2 NIST SP 800-53 Rev. 4 PS-7, SA-9 ۲-۴. CCS CSC 9 COBIT 5 APO07. 03 ISA 62443-2-1: 2009 4. 3. 2. 4. 2 ISO/IEC 27001: 2013 A. 6. 1. 1, A. 7. 2. 2, NIST SP 800-53 Rev. 4 AT-3, PM-13 ۲-۵. CCS CSC 9 COBIT 5 APO07. 03 ISA 62443-2-1: 2009 4. 3. 2. 4. 2 ISO/IEC 27001: 2013 A. 6. 1. 1, A. 7. 2. 2, NIST SP 800-53 Rev. 4 AT-3, PM-13 ۳-۱. CCS CSC 17 COBIT 5 APO01. 06, BAI02. 01, BAI06. 01, DSS06. 06 ISA 62443-3-3: 2013 SR 3. 4, SR 4. 1 ISO/IEC 27001: 2013 A. 8. 2. 3 NIST SP 800-53 Rev. 4 SC-28 ۳-۲. CCS CSC 17 COBIT 5 APO01. 06, DSS06. 06 ISA 62443-3-3: 2013 SR 3. 1, SR 3. 8, SR 4. 1, SR 4. 2 ISO/IEC 27001: 2013 A. 8. 2. 3, A. 13. 1. 1, A. 13. 2. 1, A. 13. 2. 3, A. 14. 1. 2, A. 14. 1. 3 NIST SP 800-53 Rev. 4 SC-8 ۳-۳. COBIT 5 BAI09. 03 ISA 62443-2-1: 2009 4. 4. 3. 3. 3. 9, 4. 3. 4. 4. 1 ISA 62443-3-3: 2013 SR 4. 2 ISO/IEC 27001: 2013 A. 8. 2. 3, A. 8. 3. 1, A. 8. 3. 2, A. 8. 3. 3, A. 11. 2. 7 NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16 ۳-۴. COBIT 5 APO13. 01 ISA 62443-3-3: 2013 SR 7. 1, SR 7. 2 ISO/IEC 27001: 2013 A. 12. 3. 1 NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5 ۳-۵. CCS CSC 17 COBIT 5 APO01. 06 ISA 62443-3-3: 2013 SR 5. 2 ISO/IEC 27001: 2013 A. 6. 1. 2, A. 7. 1. 1, A. 7. 1. 2, A. 7. 3. 1, A. 8. 2. 2, A. 8. 2. 3, A. 9. 1. 1, A. 9. 1. 2, A. 9. 2. 3, A. 9. 4. 1, A. 9. 4. 4, A. 9. 4. 5, A. 13. 1. 3, A. 13. 2. 1, A. 13. 2. 3, A. 13. 2. 4, A. 14. 1. 2, A. 14. 1. 3 NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 ۳-۶. ISA 62443-3-3: 2013 SR 3. 1, SR 3. 3, SR 3. 4, SR 3. 8 ISO/IEC 27001: 2013 A. 12. 2. 1, A. 12. 5. 1, A. 14. 1. 2, A. 14. 1. 3 NIST SP 800-53 Rev. 4 SI-7 ۳-۷. COBIT 5 BAI07. 04 ISO/IEC 27001: 2013 A. 12. 1. 4 NIST SP 800-53 Rev. 4 CM-2	۱-۱. COBIT 5 DSS03. 01 ISA 62443-2-1: 2009 4. 4. 3. 3 NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4 ۱-۲. ISA 62443-2-1: 2009 4. 3. 4. 5. 6, 4. 3. 4. 5. 7, 4. 3. 4. 5. 8 ISA 62443-3-3: 2013 SR 2. 8, SR 2. 9, SR 2. 10, SR 2. 11, SR 2. 12, SR 3. 9, SR 6. 1, SR 6. 2 ISO/IEC 27001: 2013 A. 16. 1. 1, A. 16. 1. 4 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4 ۱-۳. ISA 62443-3-3: 2013 SR 6. 1 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4 ۱-۴. COBIT 5 APO12. 06 NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI -4 ۱-۵. COBIT 5 APO12. 06 ISA 62443-2-1: 2009 4. 2. 3. 10 NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8 ۲-۱. CCS CSC 14, 16 COBIT 5 DSS05. 07 ISA 62443-3-3: 2013 SR 6. 2 NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4 ۲-۲. ISA 62443-2-1: 2009 4. 3. 3. 3. 8 NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20 ۲-۳. ISA 62443-3-3: 2013 SR 6. 2 ISO/IEC 27001: 2013 A. 12. 4. 1 NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11 ۲-۴. CCS CSC 5 COBIT 5 DSS05. 01 ISA 62443-2-1: 2009 4. 3. 4. 3. 8 ISA 62443-3-3: 2013 SR 3. 2 ISO/IEC 27001: 2013 A. 12. 2. 1 NIST SP 800-53 Rev. 4 SI-3 ۲-۵. ISA 62443-3-3: 2013 SR 2. 4 ISO/IEC 27001: 2013 A. 12. 5. 1 NIST SP 800-53 Rev. 4 SC-18, SI-4. SC-44 ۲-۶. COBIT 5 APO07. 06 ISO/IEC 27001: 2013 A. 14. 2. 7, A. 15. 2. 1 NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4 ۲-۷. NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4 ۲-۸. COBIT 5 BAI03. 10 ISA 62443-2-1: 2009 4. 2. 3. 1, 4. 2. 3. 7 ISO/IEC 27001: 2013 A. 12. 6. 1 NIST SP 800-53 Rev. 4 RA-5 ۳-۱. CCS CSC 5 COBIT 5 DSS05. 01 ISA 62443-2-1: 2009 4. 4. 3. 1 ISO/IEC 27001: 2013 A. 6. 1. 1	۱-۱. COBIT 5 BAI01. 10 CCS CSC 18 ISA 62443-2-1: 2009 4. 3. 4. 5. 1 ISO/IEC 27001: 2013 A. 16. 1. 5 NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8 ۲-۱. ISA 62443-2-1: 2009 4. 3. 4. 5. 2, 4. 3. 4. 5. 3, 4. 3. 4. 5. 4 ISO/IEC 27001: 2013 A. 6. 1. 1, A. 16. 1. 1 NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8 ۲-۲. ISA 62443-2-1: 2009 4. 3. 4. 5. 5 ISO/IEC 27001: 2013 A. 6. 1. 3, A. 16. 1. 2 NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8 ۲-۳. ISA 62443-2-1: ISA 62443-2-1: 2009 4. 3. 4. 5. 5 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 ۳-۱. COBIT 5 DSS02. 07 ISA 62443-2-1: 2009 4. 3. 4. 5. 6, 4. 3. 4. 5. 7, 4. 3. 4. 5. 8 ISA 62443-3-3: 2013 SR 6. 1 ISO/IEC 27001: 2013 A. 12. 4. 1, A. 12. 4. 3, A. 16. 1. 5 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4 ۳-۲. ISA 62443-2-1: 2009 4. 3. 4. 5. 6, 4. 3. 4. 5. 7, 4. 3. 4. 5. 8 ISO/IEC 27001: 2013 A. 16. 1. 6 NIST SP 800-53 Rev. 4 CP-2, IR-4 ۳-۳. ISA 62443-3-3: 2013 SR 2. 8, SR 2. 9, SR 2. 10, SR 2. 11, SR 2. 12, SR 3. 9, SR 6. 1 ISO/IEC 27001: 2013 A. 16. 1. 7 NIST SP 800-53 Rev. 4 AU-7, IR-4 ۳-۴. ISA 62443-2-1: 2009 4. 3. 4. 5. 6 ISO/IEC 27001: 2013 A. 16. 1. 4 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8 ۴-۱. ISA 62443-2-1: 2009 4. 3. 4. 5. 6 ISA 62443-3-3: 2013 SR 5. 1, SR 5. 2, SR 5. 4 ISO/IEC 27001: 2013 A. 16. 1. 5 NIST SP 800-53 Rev. 4 IR-4 ۴-۲. ISA 62443-2-1: 2009 4. 3. 4. 5. 6, 4. 3. 4. 5. 10 ISO/IEC 27001: 2013 A. 12. 2. 1, A. 16. 1. 5 NIST SP 800-53 Rev. 4 IR-4 ۴-۳. ISO/IEC 27001: 2013 A. 12. 6. 1 NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5 ۵-۱. COBIT 5 BAI01. 13 ISA 62443-2-1: 2009 4. 3. 4. 5. 10, 4. 4. 3. 4 ISO/IEC 27001: 2013 A. 16. 1. 6 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 ۵-۲. NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8	۱-۱. CCS CSC 8 COBIT 5 DSS02. 05, DSS03. 04 ISO/IEC 27001: 2013 A. 16. 1. 5 NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8 ۲-۱. COBIT 5 BAI05. 07 ISA 62443-2-1 4. 4. 3. 4 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 ۲-۲. COBIT 5 BAI07. 08 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 ۳-۱. COBIT 5 EDM03. 02 ۳-۲. COBIT 5 MEA03. 02 ۳-۳. NIST SP 800-53 Rev. 4 CP-2, IR-4

	۴-۴. COBIT 5 DSS04. 02 ISA 62443-2-1: 2009 4. 2. 3, 4. 2. 3. 9, 4. 2. 3. 12 NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14 ۴-۵. COBIT 5 APO12. 02 ISO/IEC 27001: 2013 A. 12. 6. 1 NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16 ۵-۱. COBIT 5 APO12. 04, APO12. 05, APO13. 02, BAI02. 03, BAI04. 02 ISA 62443-2-1: 2009 4. 3. 4. 2 NIST SP 800-53 Rev. 4 PM-9 ۵-۲. COBIT 5 APO12. 06 ISA 62443-2-1: 2009 4. 3. 2. 6. 5 NIST SP 800-53 Rev. 4 PM-9 ۵-۳. NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14	۴-۱. CCS CSC 3, 10 COBIT 5 BAI10. 01, BAI10. 02, BAI10. 03, BAI10. 05 ISA 62443-2-1: 2009 4. 3. 4. 3. 2, 4. 3. 4. 3. 3 ISA 62443-3-3: 2013 SR 7. 6 ISO/IEC 27001: 2013 A. 12. 1. 2, A. 12. 5. 1, A. 12. 6. 2, A. 14. 2. 2, A. 14. 2. 3, A. 14. 2. 4 NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10 ۴-۲. COBIT 5 APO13. 01 ISA 62443-2-1: 2009 4. 3. 4. 3. 3 ISO/IEC 27001: 2013 A. 6. 1. 5, A. 14. 1. 1, A. 14. 2. 1, A. 14. 2. 5 NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8 ۴-۳. COBIT 5 BAI06. 01, BAI01. 06 ISA 62443-2-1: 2009 4. 3. 4. 3. 2, 4. 3. 4. 3. 3 ISA 62443-3-3: 2013 SR 7. 6 ISO/IEC 27001: 2013 A. 12. 1. 2, A. 12. 5. 1, A. 12. 6. 2, A. 14. 2. 2, A. 14. 2. 3, A. 14. 2. 4 NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10 ۴-۴. COBIT 5 APO13. 01 ISA 62443-2-1: 2009 4. 3. 4. 3. 9 ISA 62443-3-3: 2013 SR 7. 3, SR 7. 4 ISO/IEC 27001: 2013 A. 12. 3. 1, A. 17. 1. 2A. 17. 1. 3, A. 18. 1. 3 NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9 ۴-۵. COBIT 5 DSS01. 04, DSS05. 05 ISA 62443-2-1: 2009 4. 3. 3. 3. 1 4. 3. 3. 3. 2, 4. 3. 3. 3. 3, 4. 3. 3. 3. 5, 4. 3. 3. 3. 6 ISO/IEC 27001: 2013 A. 11. 1. 4, A. 11. 2. 1, A. 11. 2. 2, A. 11. 2. 3 NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18 ۴-۶. COBIT 5 BAI09. 03 ISA 62443-2-1: 2009 4. 3. 4. 4. 4 ISA 62443-3-3: 2013 SR 4. 2 ISO/IEC 27001: 2013 A. 8. 2. 3, A. 8. 3. 1, A. 8. 3. 2, A. 11. 2. 7 NIST SP 800-53 Rev. 4 MP-6 ۴-۷. COBIT 5 APO11. 06, DSS04. 05 ISA 62443-2-1: 2009 4. 4. 3. 1, 4. 4. 3. 2, 4. 4. 3. 3, 4. 4. 3. 4, 4. 4. 3. 5, 4. 4. 3. 6, 4. 4. 3. 7, 4. 4. 3. 8 NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6 ۴-۸. ISO/IEC 27001: 2013 A. 16. 1. 6 NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4 ۴-۹. COBIT 5 DSS04. 03 ISA 62443-2-1: 2009 4. 3. 2. 5. 3, 4. 3. 4. 5. 1 ISO/IEC 27001: 2013 A. 16. 1. 1, A. 17. 1. 1, A. 17. 1. 2 NIST SP 800-53 Rev. 4 CP-2, IR-8 ۴-۱۰. ISA 62443-2-1: 2009 4. 3. 2. 5. 7, 4. 3. 4. 5. 11 ISA 62443-3-3: 2013 SR 3. 3 ISO/IEC 27001: 2013 A. 17. 1. 3 NIST SP 800-53 Rev. 4 CP-4, IR-3, PM-14 ۴-۱۱. COBIT 5 APO07. 01, APO07. 02, APO07. 03, APO07. 04, APO07. 05 ISA 62443-2-1: 2009 4. 3. 3. 2. 1, 4. 3. 3. 2. 2, 4. 3. 3. 2. 3 ISO/IEC 27001: 2013 A. 7. 1. 1, A. 7. 3. 1, A. 8. 1. 4 NIST SP 800-53 Rev. 4 PS Family ۴-۱۲. ISO/IEC 27001: 2013 A. 12. 6. 1, A. 18. 2. 2 NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2 ۵-۱. COBIT 5 BAI09. 03 ISA 62443-2-1: 2009 4. 3. 3. 3. 7 ISO/IEC 27001: 2013 A. 11. 1. 2, A. 11. 2. 4, A. 11. 2. 5 NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5 ۵-۲. COBIT 5 DSS05. 04 ISA 62443-2-1: 2009 4. 3. 3. 6. 5, 4. 3. 3. 6. 6, 4. 3. 3. 6. 7, 4. 4. 4. 6. 8 ISO/IEC 27001: 2013 A. 11. 2. 4, A. 15. 1. 1, A. 15. 2. 1 NIST SP 800-53 Rev. 4 MA-4 ۶-۱. CCS CSC 14 COBIT 5 APO11. 04 ISA 62443-2-1: 2009 4. 3. 3. 3. 9, 4. 3. 3. 5. 8, 4. 3. 4. 4. 7, 4. 4. 2. 1, 4. 4. 2. 2, 4. 4. 2. 4 ISA 62443-3-3: 2013 SR 2. 8, SR 2. 9, SR 2. 10, SR 2. 11, SR 2. 12 ISO/IEC 27001: 2013 A. 12. 4. 1, A. 12. 4. 2, A. 12. 4. 3, A. 12. 4. 4, A. 12. 7. 1 NIST SP 800-53 Rev. 4 AU Family ۶-۲. COBIT 5 DSS05. 02, APO13. 01 ISA 62443-3-3: 2013 SR 2. 3 ISO/IEC 27001: 2013 A. 8. 2. 2, A. 8. 2. 3, A. 8. 3. 1, A. 8. 3. 3, A. 11. 2. 9 NIST SP 800-53 Rev. 4 MP-2, MP-4, MP-5, MP-7 ۶-۳. COBIT 5 DSS05. 02 ISA 62443-2-1: 2009 4. 3. 3. 5. 1, 4. 3. 3. 5. 2, 4. 3. 3. 5. 3, 4. 3. 3. 5. 4, 4. 3. 3. 5. 5, 4. 3. 3. 5. 6, 4. 3. 3. 5. 7, 4. 3. 3. 5. 8, 4. 3. 3. 6. 1, 4. 3. 3. 6. 2, 4. 3. 3. 6. 3, 4. 3. 3. 6. 4, 4. 3. 3. 6. 5, 4. 3. 3. 6. 6, 4. 3. 3. 6. 7, 4. 3. 3. 6. 8, 4. 3. 3. 6. 9, 4. 3. 3. 7. 1, 4. 3. 3. 7. 2, 4. 3. 3. 7. 3, 4. 3. 3. 7. 4 ISA 62443-3-3: 2013 SR 1. 1, SR 1. 2, SR 1. 3, SR 1. 4, SR 1. 5, SR 1. 6, SR 1. 7, SR 1. 8, SR 1. 9, SR 1. 10, SR 1. 11, SR 1. 12, SR 1. 13, SR 2. 1, SR 2. 2, SR 2. 3, SR 2. 4, SR 2. 5, SR 2. 6, SR 2. 7 ISO/IEC 27001: 2013 A. 9. 1. 2 NIST SP 800-53 Rev. 4 AC-3, CM-7 ۶-۴. CCS CSC 7 COBIT 5 DSS05. 02, APO13. 01 ISA 62443-3-3: 2013 SR 3. 1, SR 3. 5, SR 3. 8, SR 4. 1, SR 4. 3, SR 5. 1, SR 5. 2, SR 5. 3, SR 7. 1, SR 7. 6 ISO/IEC 27001: 2013 A. 13. 1. 1, A. 13. 2. 1 NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7	NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14 ۳-۲. ISA 62443-2-1: 2009 4. 4. 3. 2 ISO/IEC 27001: 2013 A. 18. 1. 4 NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4 ۳-۳. COBIT 5 APO13. 02 ISA 62443-2-1: 2009 4. 4. 3. 2 ISA 62443-3-3: 2013 SR 3. 3 ISO/IEC 27001: 2013 A. 14. 2. 8 NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4 ۳-۴. COBIT 5 APO11. 06, DSS04. 05 ISA 62443-2-1: 2009 4. 4. 3. 4 ISO/IEC 27001: 2013 A. 16. 1. 6 NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14		



نتیجه‌گیری

در این پژوهش یک چارچوب کاربردی برای پیاده‌سازی حاکمیت امنیت سایبری در سازمان‌های دفاعی ارائه گردید بطوریکه در این چارچوب یک دیدگاه جامع ارائه گردید که دو منظر فنی و مدیریتی در سازمان را بطور توامان در نظر گرفته و تلفیق نموده است و سازمان‌ها می‌توانند براساس این چهار چوب در سطوح مختلف سازمانی این سیاستها لحاظ نموده و برنامه‌ها اجرایی و استانداردهای عملیاتی لازم را در پنج فرآیند عملیاتی کلی در جهت تضمین امنیت سایبری استفاده نمایند و بدین ترتیب امکان دستیابی به حاکمیت سایبری در سازمان‌های دفاعی محقق می‌گردد. پیشنهاد می‌گردد برای تکامل و ادامه این پژوهش بهتر است در کارهای آینده به تدوین مراحل بلوغ سازمانی در معماری امنیت سایبری پرداخته شود تا بتوان پس از اجرای چارچوب بدست آمده در یک سازمان دفاعی این سازمان را از نظر بلوغ امنیت سایبری ارزیابی و رتبه‌بندی نمود و بُعد سومی را به این چارچوب افزود.

قدردانی

در پایان نویسندگان مقاله حاضر از تمامی خبرگانی که ما را در فرایند انجام پژوهش حاضر یاری رساندند کمال تشکر و قدردانی را دارند.

منابع

- جباررشیدی، علی، و شکیبازاد، محمد. (۱۳۹۶). مدل‌سازی و شبیه‌سازی صحنه نبرد سایبری. *مدیریت فناوری اطلاعات*، ۹(۴): ۸۰۹-۸۲۸.
- نیما فرزام نیا. (۱۳۹۵). *جنگ و دفاع سایبری مفاهیم، راهبردها و راهکارها*، تهران: انتشارات دانشگاه امام علی (ع).
- شورای عالی پدافند غیر عامل کشور، ۱۳۹۴/۲/۲۹، سند راهبردی پدافند سایبری کشور
- سازمان پدافند غیرعامل. (۱۳۹۲). *سیاست‌های کلی ابلاغ شده از سوی مقام معظم رهبری در امور خودکفایی دفاعی و امنیتی*، تهران: مرکز پدافند سایبری کشور.
- سازمان پدافند غیرعامل. (۱۳۹۱). *سند راهبردی پدافند سایبری کشور*، تهران: مرکز پدافند سایبری کشور.
- سازمان پدافند غیرعامل. (۱۳۹۱)، *پدافند غیرعامل در برنامه ۵ ساله پنجم توسعه کشور*، تهران: مرکز پدافند سایبری کشور.
- سازمان پدافند غیرعامل. (۱۳۹۱). *تهدیدات سایبری*، تهران: مرکز پدافند سایبری کشور.
- سازمان پدافند غیرعامل. (۱۳۹۲). *دستورالعمل آمادگی دستگاه‌ها/استان‌ها/ مناطق ویژه، به منظور مقابله با تهدیدات سایبری دشمن*، تهران: مرکز پدافند سایبری کشور.

- دفتر مطالعات و نوآوری ایز ایران. (۱۳۹۴). بررسی قدرت سایبری در ایران و جهان، تهران: انستیتو ایزایران.
- فرزام نیا، نیما. (۱۳۹۳). *بررسی چالش‌های جنگ‌های سایبری در نیروهای مسلح*، تهران: دومین کنفرانس ملی دفاع سایبری، دانشگاه جامع امام حسین(ع).
- گرکی، مارکو. (۱۳۸۹)، *جرایم سایبری: راهنمایی برای کشورهای در حال توسعه*، مترجم: مرتضی اکبری، تهران: پلیس امنیت فضای تولید و تبادل اطلاعات ناجا.
- خالقی، محمود. (۱۳۹۱). *راهنمای پیاده‌سازی سیستم مدیریت امنیت اطلاعات*، تهران، دبیرخانه شورای عالی امنیت فضای تبادل اطلاعات کشور(مرکز فناوری اطلاعات ریاست جمهوری).
- هاسپین، ادوارد. (۱۳۸۹)، *جنگ سایبری، جنگ اینترنتی و انقلاب در امور نظامی*، ترجمه: روح‌اله طالبی آرانی، تهران: دفتر مطالعات سیاسی مرکز پژوهش‌های مجلس شورای اسلامی.
- شین پی، کوریل. (۱۳۸۸)، نیروی هوایی و مأموریت فضای مجازی (سایبر): دفاع از شبکه رایانه‌ای نیروی هوایی در آینده، ترجمه: مسعود منزوی، تهران، مؤسسه آموزشی و تحقیقاتی صنایع دفاعی مرکز آینده پژوهی علوم و فناوری دفاعی.
- کیلکرس، جورجیا. (۱۳۹۰). *مدل سازمانی برای تیم‌های پاسخگو به حوادث رایانه‌ای*، ترجمه: رضا انتظار شبستری، حسن‌زاده جعفر اسدی، امیر صمدی، تهران: انستیتو ایزایران.
- اخوان نیاکی، انوشیروان. (۱۳۹۰)، مقایسه فرآروش‌های ایجاد و توسعهٔ سامانه‌های اطلاعاتی، تهران: انستیتو ایز ایران.
- نیما فرزام نیا، عماد اصلانی مناره بازاری. (۱۳۹۵). بررسی تاثیرگذاری فضای سایبری بر مولفه‌های توان رزمی داعش با رویکرد تحلیل محتوا، *فصلنامه امنیت پژوهی*، ۱۵(۵۳)، ۱۱۹.
- مرکز پژوهش‌های مجلس شورای اسلامی(معاونت پژوهش‌های اجتماعی فرهنگی). (۱۳۹۸). ستراتژی سایبری ملی ایالات متحده آمریکا، ایران، تهران.
- محمد مهدی رضاپور. (۱۳۹۸). *حکمرانی فضای مجازی در کشور روسیه*، تهران: پژوهشگاه فضای مجازی- گروه علوم و فناوری‌های نوین.
- محمد مهدی رضاپور. (۱۳۹۸). *حکمرانی فضای مجازی در کشور چین*، تهران: پژوهشگاه فضای مجازی- گروه علوم و فناوری‌های نوین.
- اختری، محمد؛ کرامتی، محمدعلی و موسوی، سیدعبداله امین. (۱۴۰۲). ارائه مدل مفهومی بلوغ امنیت سایبری برای زیرساخت‌های حیاتی کشور. آینده‌پژوهی دفاعی، ۸(۲۹): ۱۰۱-۱۳۴.

- فرهنگ، سجاد و آروند، حمید. (۱۴۰۲). تأثیر کاربرد فناوری‌های شبیه‌سازی دیجیتال بر یادگیری شناختی اجتماعی رفتار اخلاقی در سازمان‌های نظامی. آینده‌پژوهی دفاعی، ۸(۲۹): ۱۶۰-۱۳۵.
- Fischerkeller, M. P., Goldman, E. O., & Harknett, R. J. (2022). *Cyber persistence theory: Redefining national security in cyberspace*. Oxford University Press.
- Trim, P., & Lee, Y. I. (2022). *Strategic cyber security management*. Taylor & Francis.
- Siegel, C. A., & Sweeney, M. (2020). *Cyber strategy: risk-driven security and resiliency*. CRC Press.
- Martellini, M. (2019). Cyber Arms Security in Cyberspace.
- Jocelyn O. Padallan. (2020)," Cyber Security ", Canada, Arcler Press. Brook S. E. Schoenfield. (2020)," Secrets of a Cyber Security Architect", NEWYORK, Taylor & Francis Group
- Kohnke, A., Sigler, K., & Shoemaker, D. (2017). *Implementing cybersecurity: A guide to the national institute of standards and technology risk management framework*. CRC Press.
- Kohnke, A., Sigler, K., & Shoemaker, D. (2017). *Implementing cybersecurity: A guide to the national institute of standards and technology risk management framework*. CRC Press.
- Index, G. C. , & Profiles, C. (2017). International Telecommunication Union (ITU). URL: https: //www. itu. int/epublications/publication/global-cybersecurityindex-2020/en/(дата звернення: 24. 06. 2021).
- Connell, M. , & Vogler, S. (2017). Russia's approach to cyber warfare (1rev). No. DOP-2016-U-014231-1Rev (Center for Naval Analyses Arlington United States, 2017), https: //apps. dtic. mil/dtic/tr/fulltext/u2/1019062. pdf.
- Kohnke, A., Sigler, K., & Shoemaker, D. (2017). *Implementing cybersecurity: A guide to the national institute of standards and technology risk management framework*. CRC Press.
- Fred Schreier, (2015), On Cyberwarfare, DCAF HORIZON 2015 WORKING PAPER No. 7.
- Singer, P. W. , & Friedman, A. (2014). Cybersecurity: What everyone needs to know. oup usa.
- Andress, J. , & Winterfeld, S. (2013). Cyber warfare: techniques, tactics and tools for security practitioners. Elsevier.
- Krepinevich, A. F. (2012). Cyber warfare. Center for Strategic and Budgetary Assessments.
- House of Commons Defence Committee. (2012)," Defence and Cyber-Security", London, House of Commons.
- Geers, K. (2011). Strategic cyber security. Kenneth Geers.

- DEFENSEDEPARTMENT CYBER EFFORTS (2011), "DOD Faces Challenges In Its Cyber Activities" , United States ,United States Government Accountability Office.
- Colbaugh, R., & Glass, K. (2011, July). Proactive defense for evolving cyber threats. In *Proceedings of 2011 IEEE International Conference on Intelligence and Security Informatics* (pp. 125-130). IEEE.
- Richardson, J. (2011). Stuxnet as cyberwarfare: applying the law of war to the virtual battlefield. *J. Marshall J. Computer & Info. L.*, *29*, 1.
- Borah, C. K. (2015). Cyber war: the next threat to national security and what to do about it? by Richard A. Clarke and Robert K. Knake.
- Libicki, M. C. (2009). Cyberdeterrence and cyberwar. RAND corporation.
- Billo, C. , & Chang, W. (2004). Cyber warfare. An Analysis of the means and motivations of selected nation states. Dartmouth, ISTS.
- United states, arcyberthe next bottlefield(2018). Us. Army cyber, command.
- Hall, J. S. (2002). Reconsidering the connection between capacity and governance. Public Organization Review, 2, 23-43.
- Rhodes, R. A. W. (1996). The new governance: governing without government. Political studies, 44(4), 652-667.
- Pierre, J., & Peters, B. G. (2000). Governance, the state and public policy.
- Rajab, M., & Eydgahi, A. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers & Security*, *80*, 211-223.
- Pettai, V., & Illing, E. (2004). Governance and good governance. *Journal of Humanities and Social Sciences*, *8*(4), 347-351.
- Hufty, M. (2011). Investigating policy processes: the governance analytical framework (GAF). *Research for sustainable development: Foundations, experiences, and perspectives*, 403-424.
- Bevir, M. (2012). *Governance: A very short introduction*. OUP Oxford.