فصلنامه علمی پژوهشی مطالعات بین‌رشته‌ای دانش راهبردی
سال هشتم، شماره ۳۱، تابستان ۱۳۹۷، صفحات ۲۸۱-۲۵۳

تدوین راهبردهای امنیت سایبری سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی کشور

ابراهیم محمودزاده[۱]؛ حمیدرضا حسنی‌اصل[۲]؛ محمدمهدی قوچانی[۳]؛ علی نیک‌نفس[۴]

تاریخ دریافت: ۱۳۹۶/۰۵/۱۰ تاریخ پذیرش: ۱۳۹۶/۱۲/۲۰

چکیده

زیرساخت‌ها بسترهای مهم حیات، رشد و پویایی صنایع و جوامع به‌شمار می‌روند. در این میان برخی از زیرساخت‌ها نقشی حیاتی در منافع ملی دارند و اختلال هرچند کوتاه‌مدت در عملکرد آن‌ها می‌تواند منجر به آسیب جدی در اقتصاد، امنیت یا ایمنی جامعه شود. بر همین اساس و با توجه به اهمیت بالایی که امنیت فضای سایبر در تداوم خدمات زیرساخت‌های حیاتی دارد، در این مقاله به احصاء و ارائه راهبردهای تأمین امنیت سایبری سامانه‌های کنترل صنعتی زیرساخت‌های حیاتی بر اساس مطالعات کتابخانه‌ای و جلسات خبرگی و رتبه‌بندی آن‌ها با استفاده از آزمون فریدمن، با نظر خبرگان حوزه سایبر پرداخته شده است و درنهایت سه راهبرد "سازمان‌دهی تیم‌های مدیریت کشف و پاسخگویی به حوادث سایبری و تعامل با سازمان‌های مشابه منطقه‌ای و بین‌المللی"، "رصد فضای سایبر زیرساخت‌های حیاتی به‌منظور کشف و مواجهه فعال و پیش‌کنشگر با تهدیدات سایبری" و "ایجاد فرایندهای نظارت و ممیزی امنیت سایبری زیرساخت‌های حیاتی" بالاترین اهمیت را به خود اختصاص داده‌اند.

کلیدواژه‌ها: زیرساخت‌های حیاتی، امنیت، سامانه کنترل صنعتی، فضای سایبر، راهبرد.

۱- دانشیار دانشگاه صنعتی مالک اشتر

۲- دانشجوی دکتری رشته مدیریت راهبردی فضای سایبرگرایش امنیت سایبر دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی (رایانامه:hassaniasl.h@nisoc.ir)

۳- دانشجوی دکتری رشته مدیریت دولتی دانشگاه علامه طباطبایی

٤- دانشجوی دکتری رشته مدیریت راهبردی فضای سایبرگرایش امنیت سایبر دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی.

مقدمه

زیرساخت‌های حیاتی نقش مهمی در ثبات نظام‌های سیاسی، اقتصادی و اجتماعی کشورها دارند. زیرساخت‌های حیاتی زیرساخت‌هایی هستند که انهدام کل یا قسمتی از آن‌ها موجب بروز بحران، آسیب و صدمات قابل‌توجه در نظام سیاسی، هدایت، کنترل و فرماندهی، تولیدی و اقتصادی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی و دفاعی با سطح تأثیرگذاری در سراسر کشور می‌شود (نشریه پدافند غیرعامل،۱۳۸۸).

هم‌زمان با پیشرفت و توسعه سریع فناوری‌ها، شدت وابستگی متقابل بین زیرساخت‌ها در طول زمان افزایش‌یافته و توسعه فضای سایبر در این پدیده بیشترین نقش را داشته است. توجه به وابستگی شدید زیرساخت‌های حیاتی به فضای سایبر به‌عنوان مغز مدیریت و راهبری پیکره زیرساخت‌های حیاتی از اهمیت ویژه‌ای برخوردار است. زیرساخت‌ها و سامانه‌های حیاتی و حساس کشور، یا خود، بخشی از فضای سایبری کشور را تشکیل می‌دهند و یا از طریق این فضا، کنترل، مدیریت و بهره‌برداری می‌شوند. سامانه‌های کنترل صنعتی[1] به‌عنوان مرکز راهبری و بخش جدایی‌ناپذیر این زیرساخت‌ها اهمیت و اولویت بسیار زیادی دارند. سامانه کنترل یک اصطلاح کلی است که دربرگیرندهٔ انواع مختلفی از سیستم‌های کنترلی ازجمله سیستم‌های کنترل نظارت و اکتساب داده‌ها[2]، سیستم‌های کنترل توزیع‌شده[3] و کنترل‌کننده‌های منطقی برنامه پذیر[4] است (ستوفر، پیلیتری، لیتمان، آبرامس و هاهن، ۲۰۱۵).

سامانه‌های کنترل صنعتی، کنترل و نظارت بر گستره وسیعی از فرایندها و صنایع را برعهده دارند که صنایع عظیم زیرساختی نظیر صنعت نفت، گاز، تولید انرژی الکتریکی و آب و نیز صنایع و فرآیندهای تولیدی نظیر صنایع دارویی، صنایع غذایی و تولید محصولات شیمیایی از آن دسته می‌باشند؛ این سامانه‌ها در معرض چالش‌ها، آسیب‌ها و تهدیدهای گوناگونی نظیر ارتکاب جرائم سازمان‌یافته، تخریب بانک‌های اطلاعاتی، حملات مختل‌کنندهٔ خدمات، جاسوسی، خرابکاری، نقض حریم خصوصی و نقض حقوق مالکیت معنوی قرار دارند.

با توجه به گستردگی حوزه عملکرد سامانه‌های کنترل صنعتی، تـأمین‌کننـدگان بـه‌طـور فزاینـده‌ای دسترسی از راه دور مبتنی‌بر وب را به‌منظور تسهیل عملیات نظارت و کنترل در محصـولات خـود

[1] Industrial Control Systems (ICS)
[2] Supervisory Control and Data Acquisition (SCADA)
[3] Distributed Control System (DCS)
[4] Programmable Logic Controller (PLC)

جایگذاری کرده‌اند. دسترسی آنلاین به اطلاعات برای تصمیم‌گیرندگان مزایایی از قبیل: پیاده‌سازی الگوهای کارآمدتر کنترل، افزایش ایمنی کارکنان و واحد صنعتی، کاهش هزینه‌های تولید و نهایتاً افزایش بهره‌وری به‌همراه داشته است (ستوفر، پیلیتری، لیتمان، آبرامس و هاهن، ۲۰۱۵). اتصال روزافزون این ابزارها به فضای سایبر به‌صورت مستمر مسیرهای تهدید و ناامنی بیشتری را بر ضد این زیرساخت‌ها فراهم می‌سازد.

مروری بر وقایع و حوادث سال‌های اخیر در جهان و کشور، مؤید این واقعیت است که بخش عمده‌ای از تهدیدهای موجود علیه کشور، به‌ویژه در زیرساخت‌های حیاتی یا مستقیماً از فضای سایبر این زیرساخت‌ها یعنی سامانه‌های کنترل صنعتی نشأت می‌گیرند و یا این فضا را هدف تهدید مستقیم خود قرار می‌دهند. در زیر چند نمونه از آخرین حملات سایبری به زیرساخت‌های حیاتی در نقاط مختلف جهان اشاره شده است

- مارس ۱۹۹۷ حمله به ترافیک ارتباطات هوایی در ماساچوست.
- ژوئن ۱۹۹۹ حمله به خط لوله بنزین واشنگتن.
- ژانویه ۲۰۰۰ میلادی حمله به سامانه کنترل فاضلاب Maroochy در کوئینزلند استرالیا.
- سال ۲۰۰۰ حمله به خط لوله گاز روسیه.
- ژانویه ۲۰۰۳ حمله به نیروگاه هسته‌ای Ohio توسط کرم Slammer.
- اوت ۲۰۰۳ حمله به نیروگاه برق و خاموشی شمال شرق ایالات‌متحده آمریکا و کانادا.
- اوت ۲۰۰۵ حمله به کارخانه‌های ماشین‌سازی کاترپیلار و هواپیماسازی بوئینگ توسط کرم Zotob.
- مارس ۲۰۰۸ خاموش‌شدن نیروگاه انرژی هسته‌ای Hatch در گرجستان.
- ژوئن ۲۰۱۰ حمله کرم کامپیوتری Stuxnet به مراکز هسته‌ای ایران.
- اکتبر ۲۰۱۳ میلادی حمله سایبری بسیار بزرگ «خاموشی آمریکایی»[1] به سامانه‌های کنترل صنعتی شبکه برق آمریکا (میلر و روه، ۲۰۱۲).

در این شرایط نگرانی‌ها از احتمال وقوع تهدیدات تروریستی پیچیده و هدفمند با استفاده از تسلیحات سایبری[2] علیه این زیرساخت‌ها عمیقاً گسترش‌یافته است. فضای سایبر پنجمین عرصه جنگ بعد از زمین، دریا، هوا و فضا محسوب می‌شود و این مسئله نشان می‌دهد که فضای سایبر،

[1] Docudrama
[2] Cyber Weapons

یک فضای جنگ و درگیری است که در استراتژی‌های دشمنان به‌وضوح دیده می‌شود (جلالی، ۱۳۹۰). اختلال در کارکرد فضای سایبر به معنی اختلال در زیرساخت‌های حیاتی و درنتیجه تسری آن به جامعه و سایر زیرساخت‌های مرتبط و وابسته خواهد بود و تداوم این روند به مختل‌سازی فعالیت‌های اجتماعی و شکل‌گیری تهدیدها در سطح امنیت ملی منجر خواهد شد (روبلس و پارک، ۲۰۱۱).

با توجه به نوپا بودن مفهوم امنیت سامانه‌های کنترل صنعتی و میزان تأثیرگذاری آن بر امنیت ملی، تدوین سیاست‌ها و راهبردهای مؤثر در جهت حفاظت از زیرساخت‌های حیاتی و تداوم فعالیت‌ها و ارائه خدمات توسط آن‌ها به‌عنوان یک ضرورت و اولویت کشور تلقی می‌شود. لذا دغدغه اصلی تحقیق حاضر فقدان راهبردهای مناسب جهت تأمین امنیت سایبری سامانه‌های کنترل صنعتی مورداستفاده در زیرساخت‌های حیاتی است و به دنبال پاسخ به این سؤال است که اولویت هر یک از گزینه‌های راهبردی احصاء شده در این زمینه نسبت به هم چگونه است؟

مبانی نظری و پیشینه‌شناسی تحقیق

زیرساخت

برای واژه زیرساخت تعاریف متنوعی وجود دارد. دانشنامه وبستر این واژه را چنین تعریف می‌کند: «سامانه‌ای از تأسیسات عمومی یک کشور، ایالت یا منطقه»، «منابع پرسنلی، ساختمانی یا تجهیزات موردنیاز برای انجام یک فعالیت» و نیز «شالوده اساسی و چارچوب بنیادی یک سامانه یا سازمان».

کمیسیون حفاظت از زیرساخت‌های بحرانی آمریکا نیز زیرساخت را چنین تعریف می‌کند: «شبکه‌ای از سامانه‌ها و فرایندهای مستقل، اغلب در مالکیت بخش خصوصی و ساخته دست بشر که به‌صورت مشارکتی و هم‌افزا برای تولید و توزیع جریان پیوسته‌ای از کالا و خدمات ضروری عمل می‌کنند».

زیرساخت‌ها به‌عنوان اساسی‌ترین پایه‌های پیشرفت برای یک کشور محسوب می‌شوند. در شرایطی که رقابت جهانی در حوزه اقتصادی و سیاسی از گذشته تابه‌حال به‌شدت حساس و بسیار فشرده‌تر شده، با نگاهی اجمالی یکی از مهم‌ترین عواملی که تأثیرات شگرفی بر روی این رقابت جهانی می‌گذارد را می‌توان زیرساخت‌های حیاتی یک کشور دانست (تابانسکی، ۲۰۱۱).

زیرساخت حیاتی

تعاریف متعددی برای زیرساخت حیاتی ارائه‌شده است. به دو تعریف که از طرف اتحادیه اروپا و آمریکا ارائه‌شده است اشاره می‌شود:

طبق تعریف آژانس امنیت ملی آمریکا[1]، زیرساخت حیاتی به دارائی‌های فیزیکی یا معنوی، سامانه‌ها و شبکه‌هایی اطلاق می‌شود که از چنان اهمیتی برخوردارند که هرگونه اختلال و یا تخریب آن‌ها اثرات مخرب بر امنیت، اقتصاد، سلامت و ایمنی عمومی جامعه یا ترکیبی از این موارد را در پی خواهد داشت.

از دیدگاه اتحادیه اروپا زیرساخت حیاتی، دارایی‌ها، سامانه یا قسمتی از یک سامانه است که برای تداوم عملکردهای حیاتی جامعه، سلامت، ایمنی، امنیت، اقتصاد یا سلامت اجتماعی مردم ضروری باشد و اختلال یا نابودی هرکدام از این زیرساخت‌ها تأثیر مخربی بر عملکرد این بخش‌ها داشته یا کنترل و اداره این مراکز را غیرممکن سازد اطلاق می‌گردد (آنجلینی و همکاران، ۲۰۱۳).

در این خصوص باید به این نکته توجه کرد که در تمامی تعاریفی که از زیرساخت‌های حیاتی ارائه‌شده یک وجه مشترک وجود دارد و آن این است که اگر در یک زیرساخت اختلالی ایجاد شود حداقل یکی از بخش‌های مهم کشور ازنظر سیاسی، اقتصادی، اجتماعی و یا امنیتی به خطر می‌افتد. اهمیت زیرساخت‌های حیاتی در عصر رقابت در عرصهٔ اینترنت و اطلاعات بر کسی پوشیده نیست، اما آنچه در حال رخ دادن است و اهمیت روزافزونی پیداکرده، حفاظت از آن‌ها است. یکی از مهم‌ترین انواع حفاظت‌ها که با رشد اینترنت و استفاده از آن و ظهور پدیده‌ای به نام فضای سایبر[2] احساس می‌شود، حفاظت سایبری از این زیرساخت‌های حیاتی است (تابانسکی، ۲۰۱۱).

انواع زیرساخت‌های حیاتی

واژه زیرساخت‌های حیاتی معمولاً از سوی دولت‌ها برای توصیف دارایی‌هایی استفاده می‌شود که مدیریت و عملیات ساختارهای اساسی جامعه را ممکن می‌سازد. زیرساخت‌های حیاتی و منابع کلیدی در ۱۸ بخش مختلف توسط مؤسسه استاندارد و فناوری آمریکا شناسایی و معرفی‌شده است. این بخش‌های اساسی عبارت‌اند از: کشاورزی و غذا، بانکداری و امور مالی، شیمیایی و مواد، امکانات تجاری، ارتباطات، کارخانه‌های حیاتی، سدها، صنایع دفاعی، خدمات اضطراری، انرژی، امکانات دولتی، بهداشت و درمان، فناوری اطلاعات، نمادها و آثار ملی، راکتورهای هسته و

[1] Department of Homeland Security (DHS)
[2] Cyber space

ضایعات آن‌ها، پست و حمل‌ونقل مرسوله، سامانه‌های حمل‌ونقل و آب.

با توجه به تعاریف متعدد زیرساخت و نقش هر یک از بخش‌های کشور در پیشبرد اهداف دولت، اساسی‌ترین و مهم‌ترین زیرساخت‌های حیاتی که در بین همهٔ کشورها مشترک هستند در یک دسته‌بندی دیگر در جدول شماره ۱ ارائه شده است:

جدول ۱. مهم‌ترین زیرساخت‌های حیاتی

انرژی	اطلاعات و ارتباطات	حمل‌ونقل	سلامت	آب	پول و بیمه	دولت و مراکز اداری دولت	غذا و کشاورزی	رسانه و دارایی‌های فرهنگی
الکتریسیته گاز بنزین	ارتباطات راه دور دستگاه‌های اطلاعات جمعی: رادیو- تلویزیون	کشتیرانی هوانوردی حمل‌ونقل ریلی حمل‌ونقل جاده‌ای حمل‌ونقل نظامی	دارو داروخانه‌ها شرکت‌های ساخت دارو	سدها ذخایر آبی شبکه آب‌رسانی	بانک‌ها بهابازار شرکت‌های بیمه	دولت مجلس مؤسسات دولتی	تجارت غذا کشاورزی	رادیو انتشارات بناهای تاریخی و باستانی

منبع: (*OSCE*, 2013)

تهدیدات در زیرساخت‌های حیاتی

تهدیدهای متعددی علیه زیرساخت‌های حیاتی از سوی کارمندان ناراضی در داخل، سارقان اطلاعات، تبهکاران سازمان‌یافته، جاسوسان صنعتی و به‌طور فزاینده‌ای سازمان‌های اطلاعاتی و ارتش‌های سایبری وجود دارد که مدام نیز برشدت آن‌ها افزوده می‌شود .این تهدیدها همچنین می‌توانند ناشی از یک انحراف ساختاری یا کارکردی در درون خود زیرساخت نیز باشند. به‌عبارت‌دیگر، تهدیدهای متوجه زیرساخت‌ها در قالب حملات تروریستی فیزیکی یا سایبری، تهدید مصنوعی، بلایای طبیعی (مانند سیل، زلزله، طوفان و غیره)، اختلال‌های فناورانه، سوانح، حوادث و غیره دسته‌بندی می‌شوند.

وابستگی زیرساخت‌های حیاتی به فضای سایبر

همان‌گونه که گفته شد؛ زیرساخت حیاتی به دارائی‌های فیزیکی یا مجازی، سامانه‌ها و شبکه‌هایی اطلاق می‌شود که از چنان اهمیتی برخوردارند که هرگونه اختلال و یا تخریب آن‌ها اثرات مخرب بر امنیت، اقتصاد، سلامت و ایمنی جامعه داشته باشد. اصولاً زیرساخت‌ها بر اساس ماهیت و عملکرد به یکدیگر وابسته هستند. در یک طبقه‌بندی، وابستگی متقابل زیرساخت‌ها به چهار نوع تقسیم‌شده است که عبارت‌اند از" وابستگی فیزیکی، وابستگی جغرافیائی، وابستگی منطقی و وابستگی سایبری (رینالدی، پرنبوم و کلی، ۲۰۰۱). با توجه به ساختار زیرساخت‌های مدرن امروزی وابستگی سایبری وجه مشترک وابستگی در همه زیرساخت‌های حیاتی به‌شمار می‌رود. وابستگی سایبری عبارت است از حالت یک سامانه که وابسته است به اطلاعاتی که از یک زیرساخت اطلاعاتی تأمین می‌شود (رینالدی و همکاران، ۲۰۰۱)

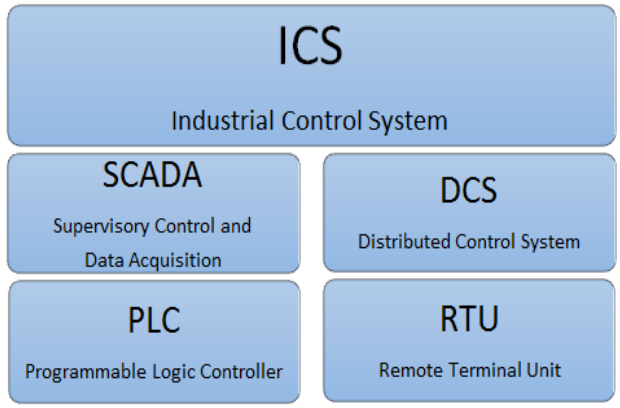
بنابراین زیرساخت‌های حیاتی و حساس کشور، یا خود، بخشی از فضای سایبر کشور را تشکیل می‌دهند و یا در چرخهٔ فرایندهای تولید، توزیع و ذخیره‌سازی این زیرساخت‌های حیاتی، فضای سایبر، نقش کلیدی داشته و به‌ویژه بخش‌های کنترلی و سامانه‌های مدیریتی آن‌ها را دربرمی‌گیرد. بر این اساس، تهدیدهای فضای سایبر کشور، مستقیماً تهدید علیه زیرساخت‌های حیاتی کشور محسوب شده و قادر به ایجاد مخاطره (تا سرحد تخریب و نابودی) در این زیرساخت‌ها را خواهند داشت.

فضای سایبر و سامانه‌های کنترل صنعتی

منظور از فضای سایبر عبارت است از شبکه‌های وابسته به یکدیگر، یعنی زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه‌های رایانه‌ای، پردازنده‌های تعبیه‌شده (جاگذاری شده)، کنترلرهای صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین این محیط و انسان به‌منظور تولید، پردازش، ذخیره‌سازی، مبادله، بازیابی و بهره‌برداری از اطلاعات. این فضا، ممکن است در ارتباط مستقیم و مداوم با سامانه‌های فناوری اطلاعات و شبکه‌های ارتباطی اعم از شبکه اینترنت باشد و یا تنها قابلیت اتصال به محیط پیرامونی در آن تعبیه‌شده باشد. همچنین در تعریف دیگری آمده است که؛ فضای سایبر فضایی فیزیکی و عینی شامل تجهیزات سخت‌افزاری و ملزومات فناوری اطلاعات و ارتباطات که دربردارنده ابعاد غیرفیزیکی از جمله اطلاعات، نرم‌افزارها، پردازش و خدمات مرتبط با اطلاعات است که به‌منظور همبستگی متقابل بین عوامل انسانی از طریق فضای مجازی متکی به شبکه‌های اینترنتی و تجهیزات مخابراتی به‌وجود آمده است. (گروه

مطالعاتی دانشجویان دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، ۱۳۹۲).

سامانه‌های کنترل صنعتی[1] به‌عنوان هسته اصلی فضای سایبر زیرساخت‌های حیاتی و یکی از مهم‌ترین اجزاء آن، اهمیت و اولویت بسیار زیادی دارند. سامانه کنترل یک اصطلاح کلی است که دربرگیرندهٔ انواع مختلفی از سیستم‌های کنترلی از جمله سیستم‌های کنترل، نظارت و اکتساب داده‌ها[2]، سیستم‌های کنترل توزیع‌شده[3] و سیستم‌های کنترلی کوچک‌تر مانند کنترل‌کننده‌های منطقی برنامه پذیر[4] و واحد پایانه راه دور[5] به شکل (۱) است (ستوفر و همکاران،۲۰۱۵).



شکل ۱. خانواده تجهیزات کنترل صنعتی

الف) سیستم کنترل نظارتی و کسب داده‌ها

این سامانه‌ها بخش مهمی از زیرساخت حیاتی بسیاری از کشورها را پشتیبانی می‌کنند. خطوط لوله نفت و گاز، سیستم‌های جمع‌آوری فاضلاب، شبکه توزیع برق، حمل‌ونقل ریلی و طیف گسترده‌ای از فعالیت‌های صنعتی که در سرتاسر یک منطقه گسترده جغرافیایی پراکنده شده‌اند، توسط این سیستم‌ها کنترل می‌شوند. طبق تعریف "اسکادا، فناوری است که کاربر را قادر می‌سازد داده‌ها را از یک یا تعدادی تأسیسات راه‌دور جمع‌آوری کرده و/یا دستورالعمل‌های محدود کنترلی را به آن تأسیسات ارسال نماید" (ستوفر و همکاران،۲۰۱۵).

[1] Industrial Control Systems (ICS)
[2] Supervisory Control and Data Acquisition (SCADA)
[3] Distributed Control System (DCS)
[4] Programmable Logic Controller (PLC)
[5] Remote Terminal Unit (RTU)

ب) سامانه‌های کنترل توزیع‌شده

سیستم‌های کنترل توزیع‌شده زیرمجموعه‌ای از سامانه‌های کنترل صنعتی است. این سامانه‌ها در مقایسه با اسکادا، فرآیندهای تصمیم‌گیری مستقل را پشتیبانی می‌کنند (لسزکزینا و همکاران، ۲۰۱۱). سیستم‌های کنترل توزیع‌شده برای کنترل فرآیندهای صنعتی از قبیل ایستگاه تولید برق، پالایشگاه‌های نفت، تأسیسات آب و فاضلاب و همچنین در کارخانه‌های شیمیایی، مواد غذایی و صنایع خودروسازی کاربرد دارند. بنابراین، معمولاً با کنترل یک فرآیند در یک منطقه محدود (مثلاً یک کارخانه) مرتبط هستند. طبق تعریف ISA، "نوعی از سامانه‌های کنترل هستند که در آن‌ها عناصر توزیع‌شده‌اند ولی باهم همبستگی دارد".

ج) کنترل‌کننده‌های منطقی برنامه‌پذیر

عملکرد PLC عبارت است از اینکه پردازنده، ورودی را از حافظه دریافت کرده، آن را از طریق اجرای یک برنامه کنترلی، اصلاح و نهایتاً نتیجه را در حافظه خروجی ذخیره می‌کند (دوممرمته و ارنست، ۱۹۷٤). درنتیجه، PLC داده‌های دریافت شده از حسگرها و عامل‌ها[1] را پردازش می‌کند. معمولاً PLC ها در سامانه‌های کنترل صنعتی به‌منظور تضمین عملکرد مداوم مطابق با توالی کنترل از پیش تعریف‌شده، به‌کار گرفته می‌شوند. بنابراین، PLC را می‌توان به‌عنوان کامپیوترهای بهینه‌سازی شده برای کاربردهای صنعتی در نظر گرفت.

د) واحد پایانه راه دور

PLC و RTU هر دو به یک منظور طراحی و در ICS بکار گرفته می‌شوند؛ هر دو وظیفه کنترل و جمع‌آوری داده‌های سایت را انجام می‌دهند. بر اساس تعریف، موتورولاها، RTU قدرت پردازش، قابلیت‌های ارتباطی و انعطاف‌پذیری بیشتری نسبت به PLC ها دارند. با این حال، RTU و PLC ویژگی‌های مشابه داشته و در کاربرد نوعی هم‌پوشانی دارند (SCADA Systems: A Comparision of RTUs and PLCs, 2007).

اگرچه سامانه‌های کنترل صنعتی از نظر مفاهیم مبتنی‌بر اصول و مبانی فناوری اطلاعات هستند، اما به لحاظ فنی، اجرایی و عملکرد پیچیده و منحصربه‌فرد می‌باشند (بلوگنا و همکاران،۲۰۱۵). تفاوت عمده بین امنیت سامانه‌های IT و خودکارسازی صنعتی نوع نگاه آن‌ها به سه مؤلفه محرمانگی، یکپارچگی و در دسترس بودن است. در مورد سامانه‌های خودکارسازی صنعتی ترتیب

[1] Sensors and Actuators

اهمیت به فرم AIC است. در ابتدا، سامانه‌های کنترل صنعتی شباهت ناچیزی به سامانه‌های فناوری اطلاعات داشتند، بدین‌معنی که سامانه‌هایی مجزا بودند که با استفاده از سخت‌افزار، نرم‌افزار و پروتکل‌های ارتباطی اختصاصی کار می‌کردند (هادزیوسمانوویک و همکاران،۲۰۱۲). ازآنجایی‌که سامانه‌های کنترل صنعتی به‌منظور ارتقاء اتصالات گروهی و بهبود قابلیت‌های دسترسی از راه دور از راه‌حل‌های فناوری اطلاعات استفاده کرده و با استفاده از کامپیوترهای استاندارد صنعتی، سامانه‌های عامل و پروتکل‌های شبکه‌ای طراحی و اجرا شده‌اند، به‌تدریج به سامانه‌های فناوری اطلاعات شباهت بیشتری پیدا کردند. این مسئله از قابلیت‌های جدید فناوری اطلاعات پشتیبانی می‌کند اما از طرف دیگر باعث می‌شود که این سامانه‌ها نسبت به سامانه‌های پیشین، به دنیای خارج بیشتر نزدیک شوند و درنتیجه نیاز بیشتری برای ایمن‌سازی این سامانه‌ها به وجود آید (رالستون و همکاران،۲۰۰۷). باوجوداینکه راه‌حل‌های امنیتی به‌منظور مقابله با این موضوعات در سامانه‌های فناوری اطلاعات طراحی شده‌اند، در زمان استفاده از همان راه‌حل‌ها در محیط‌های صنعتی بایستی بسیار احتیاط به‌عمل آورد. در بسیاری موارد به راه‌حل‌های امنیتی جدیدی که برای محیط صنعتی کاملاً بهینه‌شده باشند، نیاز خواهد بود.

سامانه‌های کنترل صنعتی تفاوت زیادی با سامانه‌های فناوری اطلاعات دارند. این تفاوت‌ها نه‌تنها به خصوصیات فنی محدود نمی‌شود، بلکه مواردی از قبیل تجربه، آموزش و حتی روش آگاهی‌رسانی را نیز شامل می‌شود. تفاوت‌های سامانه‌های فناوری اطلاعات و سامانه‌های **کنترل صنعتی** در جدول شماره ۲ ارائه شده است:

جدول ۲. تفاوت سامانه‌های فناوری اطلاعات و کنترل صنعتی

سامانه‌های فناوری اطلاعات	سیستم‌های اسکادا
در صورت از دست دادن داده و یا بروز وقفه‌های ناخواسته، می‌توان سیستم را با راه‌اندازی مجدد و یا برگرداندن فایل‌های پشتیبان به حالت اولیه برگرداند.	از دست دادن داده و یا بروز وقفه قابل تحمل نیست و ممکن است نتایج مهلکی را به دنبال داشته باشد.
با تأخیر ناخواسته می‌توان کنار آمد.	تأخیر زیاد قابل تحمل نیست.
در صورت بروز مشکلات حاد برای سیستم با راه‌اندازی مجدد آن می‌توان مشکل ناخواسته را به‌نوعی حل کرد!	کارکرد سیستم می‌بایست همواره عاری از خطا باشد. از UPS پشتیبان استفاده گردد. ازکارافتادن سیستم حتی برای لحظاتی اندک می‌تواند فاجعه‌آمیز باشد.

سامانه‌های فناوری اطلاعات	سیستم‌های اسکادا
از نرم‌افزارهای آنتی‌ویروس استفاده زیاد می‌شود.	به‌کارگیری نرم‌افزارهای آنتی‌ویروس در اکثر موارد مشکل است، چراکه تأخیر قابل تحمل نیست.
ارائه دوره‌های آموزشی به‌منظور افزایش سطح آگاهی کاربران در خصوص مسائل امنیتی بسیار متداول است.	ارائه دوره‌های آموزشی به‌منظور افزایش سطح آگاهی کاربران در خصوص مسائل امنیتی کم است.
از رمزنگاری استفاده می‌شود.	تعداد بسیار زیادی از سیستم‌های اسکادا داده و پیام‌های کنترلی را به‌صورت غیر رمز شده ارسال می‌نمایند.
آزمون نفوذ به‌صورت ادواری انجام می‌شود.	آزمون نفوذ به‌صورت ادواری در شبکه کنترلی انجام نمی‌شود و زمانی هم که این کار انجام می‌شود می‌بایست این کار با دقت صورت پذیرد تا باعث بروز اختلال نگردد.
پیاده‌سازی وصله‌های نرم‌افزارها به‌صورت ادواری انجام می‌شود.	پیاده‌سازی وصله‌های نرم‌افزاری می‌بایست با دقت صورت پذیرد و معمولاً" مستلزم هماهنگی با شرکت فروشنده تجهیزات اسکادا است.
ممیزی امنیت اطلاعات لازم است و معمولاً" به‌صورت ادواری انجام می‌شود.	ممیزی امنیت اطلاعات به‌طور ادواری انجام نمی‌شود.
تجهیزات معمولاً" هر سه تا پنج سال جایگزین و یا ارتقاء می‌یابند.	تجهیزات استفاده‌شده برای مدتی طولانی و بدون جایگزینی استفاده می‌گردند.

آسیب‌پذیری سامانه‌های کنترل صنعتی

آسیب‌پذیری‌های موجود در بخش‌های مختلف سامانه‌های صنعتی این امکان را برای مهاجمین سایبری فراهم ساخته تا به فکر حمله به زیرساخت‌های حیاتی کشور، آسیب رساندن و یا ایجاد اختلال در فرآیند کاری آن‌ها برآیند. ازآنجاکه بروز هرگونه نارسایی در بخش‌های مذکور ممکن است اثرات مخرب و جبران‌ناپذیری بر امنیت اقتصادی و توانمندی‌های دفاعی کشور برجای گذارد، ازاین‌رو اهمیت شناخت آسیب‌پذیری‌ها و یافتن راهکارهای تدافعی و بهبود امنیت این سامانه‌ها بیش‌ازپیش احساس می‌شود. به‌طورکلی آسیب‌پذیری‌های موجود در سامانه‌های کنترل

صنعتی را می‌توان به دودستهٔ عمده تقسیم‌بندی نمود:

۱- آسیب‌پذیری‌های فیزیکی

۲- آسیب‌پذیری‌های سایبری (عبد التاجدینی، ۱۳۹۲).

در هر دودسته برخی عوامل زیر منجر به آسیب‌پذیر شدن هرچه بیشتر این سیستم‌ها در مقابل طیف وسیعی از حملات سایبری گردیده است

- ضعف و آسیب‌پذیری ذاتی فناوری‌های بکار گرفته‌شده از قبیل پروتکل‌ها، سیستم‌های عامل، تجهیزات و غیره.
- ضعف تنظیمات مانند رها کردن تنظیمات پیش‌فرض، استفاده از گذرواژه‌های[1] نامناسب، عدم‌استفاده از رمزنگاری، راه‌اندازی سرویس‌های مختلف بدون اعمال تنظیمات لازم و غیره.
- ضعف در سیاست‌گذاری مانند عدم‌وجود سیاست امنیتی، عدم‌وجود طرح‌های مقابله با مخاطرات[2] و بازیابی[3]، نداشتن نظارت امنیتی مناسب (مدیریتی و فنی) و غیره (ستوفر و همکاران، ۲۰۱۵).

به‌طورکلی برخی از این آسیب‌پذیری‌ها در حال حاضر وجود دارند و برخی دیگر آسیب‌پذیری‌های بالقوه هستند. جدول شماره ۳ این آسیب‌پذیری‌ها را در دو رده نشان می‌دهد:

[1] Password
[2] Risk
[3] Recovery

جدول ۳. دسته‌بندی انواع آسیب‌پذیری‌ها

آسیب‌پذیری‌های بالقوه			آسیب‌پذیری‌های بالفعل
آسیب‌پذیری‌های خط‌مشی و روش‌های اجرایی	آسیب‌پذیری‌های سکو	آسیب‌پذیری‌های شبکه	در دسترس بودن اطلاعات عمومی
خط‌مشی دستورالعمل‌های پیاده‌سازی	پیکربندی سکو سخت‌افزار سکو نرم‌افزار سکو ضد بدافزار سکو	پیکربندی شبکه سخت‌افزار شبکه نرم‌افزار شبکه مرزهای شبکه پایش و ثبت رخدادهای شبکه ارتباطات اتصالات بی‌سیم	وب‌سایت‌ها اسناد طراحی راهنمای تعمیر و نگهداشت استانداردهای فنی

منبع: (ستوفر و همکاران، ۲۰۱۵).

تهدیدات سایبری در زیرساخت‌های حیاتی

گسترش کاربرد فرآورده‌های فن‌آوری اطلاعات، پذیرش فن‌آوری‌های استانداردشده و اتصال روزافزون سامانه‌های کنترل صنعتی به سایر شبکه‌ها در کنار منافعی که با خود به همراه داشته، باعث افزایش قابل‌توجه سطح تهدیدات سایبری شده است (ستوفر و همکاران، ۲۰۱۵). تهدیدات سایبری با بهره‌برداری از آسیب‌پذیری‌های متنوع در بخش‌های مختلف سامانه‌های کنترل صنعتی موجب آسیب رساندن و یا ایجاد اختلال در فرآیند کاری زیرساخت‌های حیاتی کشور می‌شوند. این تهدیدات شامل دامنه وسیعی از حملات جهت‌دار، نفوذهای مخرب، هجوم انواع ویروس‌ها، کرم‌ها و سایر بدافزارها و حتی نقض ناخواسته اصول امنیتی درنتیجه اشتباهات انسانی است. تا پیش از سال ۲۰۱۲، تنها دو نمونه از سلاح‌های سایبری مورداستفاده قرارگرفته بودند: استاکس‌نت و Duqu. بااین‌حال، تجزیه‌وتحلیل این بدافزارها، جامعه سایبری را مجبور کرد که به‌طور چشم‌گیری اهداف جنگ سایبری را مورد بازبینی قرار دهد. سال ۲۰۱۲ از سلاح‌های سایبری در سطح وسیع‌تری استفاده شده است. تا قبل از ۲۰۱۲ تنها ایران هدف این نوع سلاح‌ها بود، اما در طول سال ۲۰۱۲ این حملات در منطقه‌ای گسترده‌تر، از غرب آسیا تا ایران گسترش‌یافته است (گوستو۲۰۱۲). آمارها نیز نشان می‌دهد که طی سال‌های اخیر دولت‌ها در تجهیز خود به سلاح‌های سایبری درگیر رقابت تنگاتنگی شده‌اند. بررسی‌ها به‌وضوح نشان

می‌دهد تنها در فاصله بین سال‌های ۲۰۰۷ تا ۲۰۰۸ تعداد کشورهای متقاضی این‌گونه سلاح‌ها تقریباً ۲۰ درصد رشد داشته است. سیر تکاملی این تسلیحات سایبری نیز اخیراً رشد قابل‌توجهی داشته است و به مرحله‌ای از بلوغ خود رسیده‌اند که باید تهدیدات آن‌ها را بسیار جدی قلمداد نمود.

اسناد راهبردی دفاع سایبری، امنیت سایبری و مقابله با جرائم سازمان‌یافته سایبری کشورها، همچنین مراجعی از قبیل مراجع ملی مقابله با حوادث سایبری، دسته‌بندی‌های متعددی را برای منشأ تهدیدات سایبری[1] ارائه داده‌اند. برخی از عوامل کاملاً خارجی و بدون عمد قبلی هستند؛ در این دسته می‌توان مواردی نظیر خرابی سامانه‌ها در اثر حوادث محیطی، ضعف و آسیب‌پذیری ذاتی سامانه‌ها، اشتباهات اپراتوری در زمان بهره‌برداری از سامانه‌ها، اشتباهات متخصصان تعمیر و نگهداری را نام برد. اما برخی از این عوامل کاملاً براساس برنامه‌ریزی و به‌صورت منسجم عمل می‌کنند. مهم‌ترین منشأ تهدیدات سایبری در این دسته به ترتیب اهمیت، عبارت‌اند از: دولت‌های متخاصم[2]، مزدوران سایبری[3] یا گروه‌های تحت حمایت پنهان دولت‌های متخاصم[4]، جاسوسان سایبری[5]، تروریست‌های سایبری[6]، مجرمان سازمان‌یافته سایبری[7]، هکرهای دارای انگیزه سیاسی و بدافزارها و ویروس‌ها.

چالش‌های امنیت سامانه‌های کنترل صنعتی

مرور تهدیدات گسترده و متنوع امروزی، مؤید این امر است که امنیت سایبری صرفاً به فناوری و تجهیزات امنیتی مانند دیواره آتش[8]، ضد بدافزار و غیره محدود نمی‌شود. تمرکز مطلق بر جنبه فناوری نهایتاً منجر به ایجاد سامانه حفاظتی خواهد شد که در آن مشخص نیست هر کس چه وظایفی دارد و چگونه باید به رفع مشکلات بپردازد. مؤلفه‌های بنیادین سامانه‌های کنترل صنعتی عبارت‌اند از انسان، فرآیند و فناوری[9] که باید به‌طور کامل موردتوجه قرار گیرند (روس، ۲۰۱۱). در ادامه چالش‌های مرتبط با هر یک از این مؤلفه‌ها مرور می‌شود.

---

[1] Threat source
[2] Hostile states
[3] Cyber mercenaries
[4] State sponsored groups / proxies
[5] Cyber espionages
[6] Cyber terrorists
[7] Organized cyber criminals
[8] Firewall
[9] People, Process and Technology (PPT)

الف) چالش‌های فناوری

شناسایی آسیب‌پذیری‌های مرتبط با فناوری، یکی از چالش‌های مهم محیط‌هایی است که از سامانه‌های کنترل صنعتی برای راهبری فرآیندهای صنعتی استفاده می‌کنند (یگره و همکاران، ۲۰۰۶). شناسایی این آسیب‌پذیری‌ها نیز با توجه به پیچیدگی‌های ICS باید با مشارکت واحد امنیت فناوری اطلاعات و واحد کنترل صنعتی صورت پذیرد (ستوفر و همکاران، ۲۰۱۵). نمونه‌های زیادی از آسیب‌پذیری‌ها مانند انواع کدهای مخرب (ازجمله ویروس‌ها، کرم‌ها و غیره)، افزایش دسترسی از طریق کد نویسی، تجزیه‌وتحلیل ترافیک شبکه، نفوذ غیرمجاز به شبکه و غیره وجود دارد که در یک معماری باز قادر هستند از محیط شبکه به درون سامانه‌های کنترل صنعتی منتقل شوند (هملند سکوریتی، ۲۰۰۹). از سوی دیگر علی‌رغم اینکه ICSها از فناوری‌های معمول IT استفاده می‌کنند، نمی‌توان به‌سادگی از راهکارهای امنیت IT در محیط ICS استفاده کرد. در این رابطه تفاوت‌های زیادی میان محیط IT و ICS وجود دارد که مطابق جدول شماره دو باید این تفاوت‌ها درزمینهٔ امنیتی نیز موردتوجه قرار گیرند. در جدول شماره ٤ این موارد به‌صورت مقایسه‌ای ارائه شده است.

جدول ٤. تمرکز امنیت در IT و ICS

سرفصل‌های امنیت	فناوری اطلاعات	سامانه‌های کنترل صنعتی
آنتی‌ویروس و کدهای سیار	بسیار رایج؛ پیاده‌سازی و روزآمدسازی آسان	به دلیل تأثیرگذاری بر این نوع سامانه‌ها می‌تواند بسیار مشکل باشد؛ سامانه‌های قدیمی ممکن است غیرقابل تعمیر باشند
مدیریت وصله	آسان تعریف، اقدامات راه دور وسیع و خودکار	بسیار زمان‌بر و تأثیرگذار بر عملکرد
طول عمر پشتیبانی فناوری (برون‌سپاری)	۲ تا ۳ سال؛ فروشندگان متنوع، ارتقا فراگیر	۱۰ تا ۲۰ سال؛ همان فروشنده
آزمون و ممیزی امنیت سایبر (روش‌ها)	استفاده از روش‌های نوین	انجام آزمون باید متناسب با سامانه تنظیم شود؛ روش‌های نوین مناسب این سامانه‌های نیستند
مدیریت تغییرات	به‌طور منظم و برنامه‌ریزی شده؛ در زمان کم باری سامانه	برنامه‌ریزی بلندمدت
طبقه‌بندی دارائی‌ها	روش معمول سالیانه؛ به‌منظور برآورد هزینه تأمین امنیت سایبر	اجرا فقط در مواقع لازم؛ حفاظت از دارائی‌های حیاتی با هزینه‌های

سرفصل‌های امنیت	فناوری اطلاعات	سامانه‌های کنترل صنعتی
		بودجه مرتبط است.
پاسخگویی به حوادث و شواهد قانونی	توسعه و پیاده‌سازی آسان؛ جاسازی برخی الزامات قانونی در فناوری	غیرمعمول و پنهان در پس فعالیت سامانه، بازیابی مشکل ادله
امنیت فیزیکی و محیطی	از ضعیف تا عالی؛ سامانه‌های اداری، سامانه‌های عملیاتی حیاتی	عالی (مراکز عملیات، نگهبانان، دروازه‌ها و تفنگ‌ها)
توسعه سامانه‌های امنیتی	بخش جدائی‌ناپذیر فرایند توسعه	معمولاً بخش جدائی‌ناپذیر فرایند توسعه نیست.
انطباق امنیتی	نظارت قانونی محدود	راهنمای مقررات خاص (در برخی بخش‌ها)

ب) چالش‌های فرایندی

حرکت در مسیر امن سازی ICS ها و آمادگی در برابر تهدیدات سایبری مستلزم برداشتن گام‌های بلندی است که باید با سرعت هرچه بیشتر برداشته شود. متأسفانه علی‌رغم تأکید ماده ۱۹۸ فصل هفتم برنامه پنجم توسعه، حداکثر فعالیت سازمان‌ها محدود به نگارش و یا کپی‌برداری از تعدادی دستورالعمل مشابه است. در خوش‌بینانه‌ترین حالت نیز اجرای سامانه مدیریت امنیت اطلاعات[1] در در سامانه صنعتی بخش دولتی منجر به تولید چندین جلد سند الزامات و دستورالعمل با هزینه‌های چند ده‌میلیونی است که بایستی با توجه به نیاز سازمان طراحی و تدوین گردد، اما بیشتر شامل متن‌هایی است که به‌صورت عمومی و کلی می‌باشند. در این رابطه لازم است سیاست‌گذاری، استانداردسازی، طراحی برنامه راهبردی، پیاده‌سازی، کنترل و نظارت با توجه به نیاز هر سازمان و محدوده عملکردی آن موردتوجه قرار گیرد (یگره و همکاران،۲۰۰۶).

ج) چالش‌های نیروی انسانی

مشکلات نیروی انسانی نیز بخش مهمی از چالش‌های پیش روست. کمبود نیروی انسانی متخصص در ساختارهای بخش دولتی موضوع قابل‌توجهی است. مانع عمده، عدم‌تعهد و همراهی مدیریت ارشد سازمان‌های دولتی با برنامه‌های امنیت است که عمدتاً ناشی از عدم‌آگاهی و درک اهمیت موضوع است. مقاومت کارکنان در مقابل هرگونه تغییر در فرآیندها نیز مانع مهم دیگری است که در این رابطه وجود دارد (یگره و همکاران، ۲۰۰۶).

[1] Information Security Management System (ISMS)

روش‌شناسی تحقیق

نوع تحقیق حاضر براساس ماهیت توصیفی و از نظر هدف کاربردی است. گردآوری داده‌های اولیه از طریق روش کتابخانه‌ای و مرور و مطالعه پژوهش‌ها و تحقیقات قبلی، کتب و مقالات معتبر علمی و پژوهشی و اسناد رسمی منتشر شده در پایگاه‌های اطلاعات علمی معتبر صورت‌گرفته است. با استفاده از اطلاعات به‌دست‌آمده در مطالعات فوق و از طریق پنل خبرگان به بحث و تبادل‌نظر و احصاء گزینه‌های راهبردی به‌منظور دستیابی به امنیت سایبری سامانه‌های کنترل صنعتی زیرساخت‌های حیاتی با توجه به شرایط کشور اقدام گردید. پس از احصاء گزینه‌های راهبردی مدنظر در موضوع تحقیق به اولویت‌بندی راهبردهای استخراج‌شده با استفاده از آزمون آماری فریدمن[1] در نرم‌افزار SPSS پرداخته شده است. گردآوری داده‌ها با روش پیمایشی و با استفاده از پرسشنامه از بین جامعهٔ آماری خبرگان و کارشناسان حوزهِ سامانه‌های کنترل صنعتی انجام شده است. لذا از این منظر، تحقیق از نوع کمی است. انتخاب نمونه آماری نیز از روش نمونه در دسترس آغاز و سپس به شیوه گلوله برفی و معرفی سایر افراد از سوی نمونه در دسترس صورت گرفته است و شامل افرادی بوده است که دانش‌آموخته یا دانشجوی دکتری تخصصی در رشته‌های مرتبط با فضای سایبر و امنیت سایبری و یا حداقل دارای مدرک کارشناسی‌ارشد مرتبط و تجربه پنج سال فعالیت حرفه‌ای در حوزه امنیت فناوری یا سامانه‌های کنترل صنعتی بوده‌اند که در نهایت تعداد ۳۲ فقره پرسشنامه تکمیل و در آزمون آماری مورد بهره‌برداری قرار گرفته است. لازم به ذکر است که تعداد اندکی از خبرگان نیز به دلیل تجربه عملی طولانی‌مدت تخصصی در این حوزه و با معرفی و تأکید سایر خبرگان باوجود داشتن مدرک کارشناسی در تکمیل پرسشنامه مشارکت داشته‌اند.

با توجه به ماهیت آزمون آماری مورداستفاده فرضیه‌های تحقیق نیز به شرح زیر می‌باشد:

H0: میانگین رتبه گزینه‌های راهبردی احصاء شده دارای تفاوت معنی‌دار نیست.

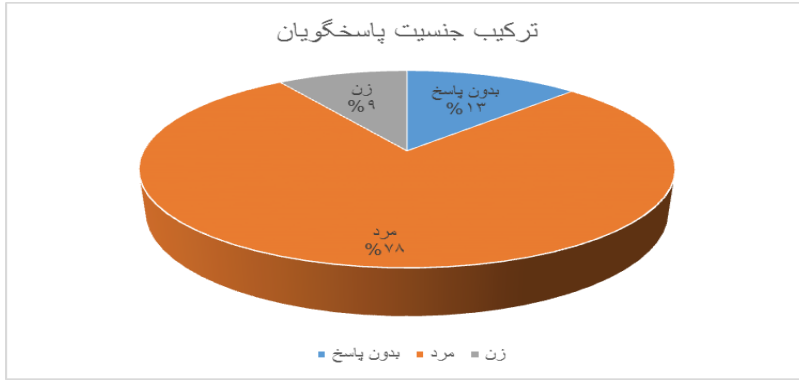
H1: میانگین رتبه گزینه‌های راهبردی احصاء شده با یکدیگر تفاوت معنی‌دار دارد.

[1] AHP(Analytical Hierarchy Process)

تجزیه‌وتحلیل داده‌ها و یافته‌های تحقیق

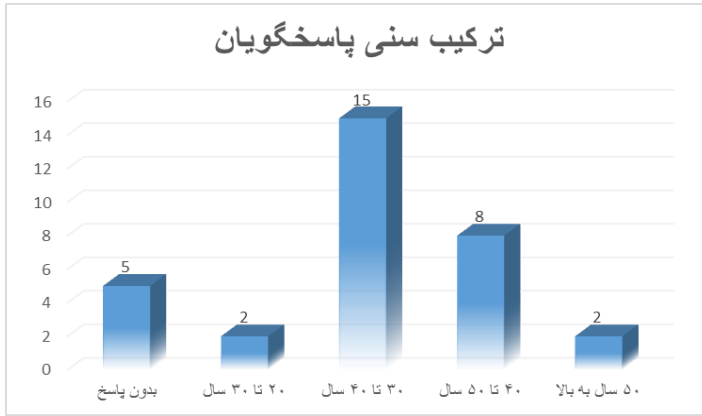
الف) تجزیه‌وتحلیل داده‌ها

همان‌طور که بیان گردید در پژوهش حاضر از پرسشنامه بهره گرفته شد و بر اساس تعداد ۳۲ پرسشنامه تکمیل‌شده توسط خبرگان سایبری و کارشناسان حوزه سامانه‌های کنترل صنعتی، تحلیل آماری نتایج صورت گرفت. در نتیجه آمار جمعیت‌شناختی نمونه آماری و پاسخ‌گویان به تحقیق به‌صورت زیر بوده است.



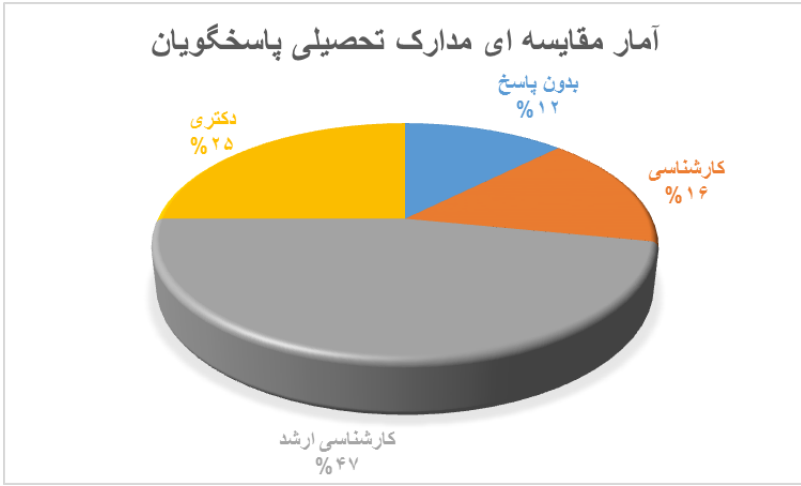
شکل ۲. نمودار ترکیب جنسیت پاسخگویان

مطابق شکل (۲) از بین پاسخگویان به پرسشنامه تعداد ۲۵ نفر مرد، ۳ نفر زن و ٤ مورد نیز بی‌پاسخ بوده است.



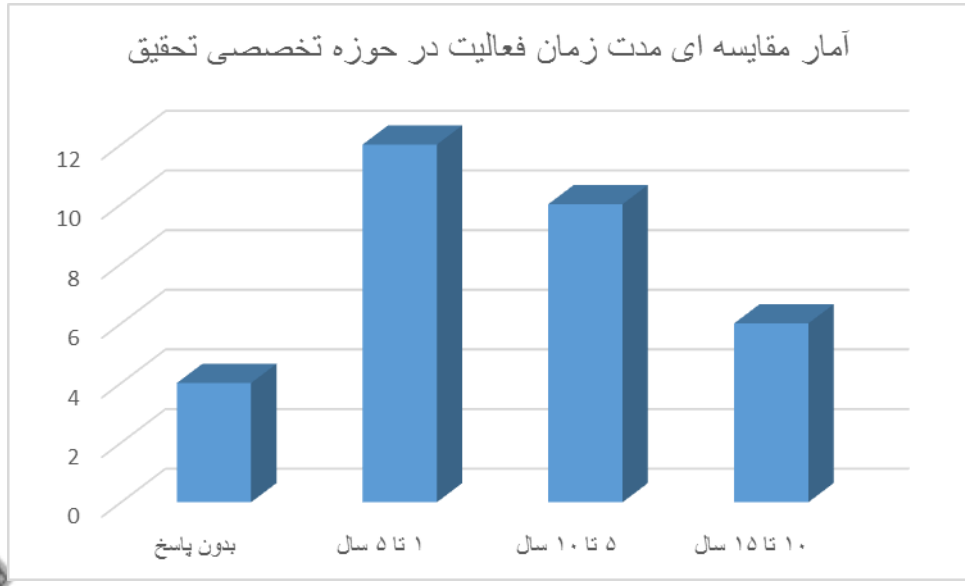
شکل ۳. نمودار ترکیب سنی پاسخگویان

از نظر سنی نیز تعداد ۵ مورد بدون پاسخ، ۲ مورد ۲۰ تا ۳۰ سال، ۱۵ مورد ۳۰ تا ٤٠ سال، ۸ مورد ٤٠ تا ۵۰ سال و دو مورد ۵۰ سال به بالا بوده‌اند که در شکل شماره ۳ مشخص گردیده بود.



شکل ٤. آمار مقایسه مدارک تحصیلی پاسخ‌گویان

ترکیب مدارک تحصیلی پاسخ‌گویان نیز به شرح شکل (٤) و به تعداد ۵ مورد کارشناسی، پانزده مورد کارشناسی ارشد، ۸ مورد دکتری و ٤ مورد بدون پاسخ بوده است.



شکل ۵. نمودار آمار مقایسه مدت‌زمان فعالیت در حوزه تحقیق

مطابق شکل (۵) از نظر مدت‌زمان فعالیت در حوزه تخصصی سامانه‌های مدیریت صنعتی و مدیریت فضای سایبر نیز ۱۲ نفر از پاسخگویان بین ۱ تا ۵ سال، ده نفر ۵ تا ۱۰ سال، ٦ نفر ۱۰ تا ۱۵ سال و ٤ مورد نیز بدون پاسخ بوده است.

با استفاده از آزمون فریدمن به رتبه‌بندی گزینه‌های راهبردی احصا شده پرداختیم که نتایج آمار توصیفی مربوط به راهبردهای مزبور به شرح جدول (۵) بوده است. در این جدول آماره‌های مربوط به میانگین، انحراف معیار و حداقل و حداکثر امتیاز داده شده به گزینهٔ راهبردی مربوطه مشخص شده است.

جدول ۵. آزمون فریدمن برای رتبه‌بندی گزینه‌های راهبردی

عنوان راهبرد	میانگین	انحراف معیار	حداقل	حداکثر
حمایت از تولید محصولات ملی و بومی‌سازی تدریجی سیستم‌های کنترل صنعتی	٤.١٦	١.٢٩٨	٢	٦
طبقه‌بندی و حفاظت ویژه از اطلاعات فنی و جغرافیائی زیرساخت‌های حیاتی	٤.٣٤	١.٠٩٦	٢	٦
توجه به اصل تولید، توسعه و سفارشی‌سازی فرایندها، استانداردها و پروتکل‌ها امنیت سیستم‌های کنترل صنعتی	٤.٠٠	١.١٦٤	٢	٦
تلاش در جهت رفع یا کاهش آسیب‌پذیری‌ها، امن سازی، مستحکم سازی، و تقویت بازدارندگی	٣.٩٤	١.٣١٨	٢	٦
رصد فضای سایبر زیرساخت‌های حیاتی به‌منظور کشف و مواجهه فعال و پیش کنشگر با تهدیدات سایبری	٤.٦٩	١.٢٨١	٣	٧
کشف و تحلیل روندهای جهانی و شناسایی تهدیدهای سایبری زیرساخت‌های حیاتی	٣.٩١	١.٢٠١	٢	٦
ساماندهی و سازمان‌دهی نیروی انسانی متعهد و متخصص	٣.٩١	١.٤٠٠	٢	٦
سازمان‌دهی تیم‌های مدیریت کشف و پاسخگویی به حوادث سایبری و تعامل با سازمان‌های مشابه منطقه‌ای و بین‌المللی	٤.٨٤	١.٢٧٣	٣	٧
فرهنگ‌سازی و ارائه آموزش‌های عمومی و تخصصی به ذینفعان و بازیگران	٤.٠٣	١.٢٠٤	٢	٦
ایجاد مکانیسم‌های احراز صلاحیت پیمانکاران و مشاورین سایبری زیرساخت‌های حیاتی	٣.٩١	١.٣٠٤	٢	٦
توجه ویژه به نیازهای قانونی نیروی انسانی شاغل در	٣.٩١	١.١٤٦	٢	٦

عنوان راهبرد	میانگین	انحراف معیار	حداقل	حداکثر
زیرساخت‌های حیاتی				
مدیریت دانش حاصل از تجارب اجرای راهبردهای امنیت فضای سایبر زیرساخت‌های حیاتی	٤.١٩	١.١٧٦	٢	٦
ایجاد نظام جامع بومی امنیت سیستم‌های کنترل صنعتی	٤.١٣	١.٠٤٠	٢	٦
ایجاد فرایندهای ارتباطی و سازمان‌دهی و هماهنگی بین دستگاهی	٣.٩٤	١.٤٥٨	٢	٦
ایجاد مرکز ملی امنیت، حفاظت و نظارت بر زیرساخت‌های حیاتی کشور	٤.١٣	١.٤٣١	٢	٦
کشف وابستگی متقابل بین انواع زیرساخت‌های حیاتی و شدت و تأثیر آن	٣.٩١	١.٢٧٩	٢	٦
مدیریت مخاطرات فضای سایبر زیرساخت‌های حیاتی	٤.٠٩	١.٤٦٧	٢	٦
طبقه‌بندی زیرساخت‌های فیزیکی و اطلاعاتی حیاتی بر اساس سطح اهمیت و شدت تأثیر بر جنبه‌های مختلف حیات	٣.٨٤	١.٢٩٨	٢	٦
تدوین سیاست‌ها و اصول امنیت فضای سایبر زیرساخت‌های حیاتی	٤.١٣	١.١٨٥	٢	٦
وضع قوانین و مقررات مناسب کیفری متناسب با اهمیت و نقش زیرساخت‌های حیاتی	٣.٩٤	١.٠٧٦	٢	٦
ایجاد فرایندهای نظارت و ممیزی امنیت سایبری زیرساخت‌های حیاتی	٤.٤٤	١.١٠٥	٢	٦

ب) یافته‌های تحقیق

ازآنجاکه زیرساخت‌های حیاتی و تأمین امنیت آن‌ها نقش ویژه‌ای در توسعه و پیشرفت همه‌جانبه کشور بر عهده دارند، به‌منظور کاهش آسیب‌پذیری زیرساخت‌ها، ارتقا پایداری ملی، حفاظت از مردم و منابع ملی کشور و تضمین استمرار خدمات آن‌ها، با تدوین راهبردهای مناسب می‌توان جهت‌گیری‌های ملی و کلان را ترسیم و هدایت نمود. برای این منظور بر اساس چارچوب جامع تدوین راهبرد به‌عنوان چارچوب نظری اولیه، با تشکیل پنل خبرگان و بحث و تبادل‌نظر با دستمایه قرار دادن نتایج مطالعات نظری درنهایت مناسب‌ترین راهبردها احصا و با نظر خبرگان سایبری در چهار سطح فنی تخصصی، انسانی، مدیریتی ساختاری، قانونی نظارتی قضائی به‌قرار زیر فهرست شد:

۱) راهبردهای فنی و تخصصی

۱-۱) حمایت از تولید محصولات ملی و بومی‌سازی تدریجی سیستم‌های کنترل صنعتی

۱-۲) طبقه‌بندی و حفاظت ویژه از اطلاعات فنی و جغرافیائی زیرساخت‌های حیاتی؛

۱-۳) توجه به اصل تولید، توسعه و سفارشی‌سازی فرایندها، استانداردها و پروتکل‌های امنیت سیستم‌های کنترل صنعتی؛

۱-٤) تلاش در جهت رفع یا کاهش آسیب‌پذیری‌ها، امن‌سازی، مستحکم‌سازی و تقویت بازدارندگی؛

۱-۵) رصد فضای سایبر زیرساخت‌های حیاتی به‌منظور کشف و مواجهه فعال و پیش‌کنشگر با تهدیدات سایبری؛

۱-٦) کشف و تحلیل روندهای جهانی و شناسایی تهدیدهای سایبری زیرساخت‌های حیاتی.

۲) راهبردهای انسانی

۲-۱) ساماندهی و سازمان‌دهی نیروی انسانی متعهد و متخصص؛

۲-۲) سازمان‌دهی تیم‌های مدیریت کشف و پاسخ‌گویی به حوادث سایبری و تعامل با سازمان‌های مشابه منطقه‌ای و بین‌المللی؛

۲-۳) فرهنگ‌سازی و ارائه آموزش‌های عمومی و تخصصی به ذی‌نفعان و بازیگران؛

۲-٤) ایجاد مکانیسم‌های احراز صلاحیت پیمانکاران و مشاورین سایبری زیرساخت‌های حیاتی؛

۲-۵) توجه ویژه به نیازهای قانونی نیروی انسانی شاغل در زیرساخت‌های حیاتی؛

۲-٦) مدیریت دانش حاصل از تجارب اجرای راهبردهای امنیت فضای سایبر زیرساخت‌های حیاتی.

۳) راهبردهای مدیریتی و ساختاری

۳-۱) ایجاد نظام جامع بومی امنیت سیستم‌های کنترل صنعتی؛

۳-۲) ایجاد فرایندهای ارتباطی و سازمان‌دهی و هماهنگی بین دستگاهی؛

۳-۳) ایجاد مرکز ملی امنیت، حفاظت و نظارت بر زیرساخت‌های حیاتی کشور؛

۳-٤) کشف وابستگی متقابل بین انواع زیرساخت‌های حیاتی و شدت و تأثیر آن؛

۳-۵) مدیریت مخاطرات فضای سایبر زیرساخت‌های حیاتی؛

٦-٣) طبقه‌بندی زیرساخت‌های فیزیکی و اطلاعاتی حیاتی بر اساس سطح اهمیت و شدت تأثیر بر جنبه‌های مختلف حیات.

٤) راهبردهای قانونی، نظارتی و قضائی

٤-١) تدوین سیاست‌ها و اصول امنیت فضای سایبر زیرساخت‌های حیاتی؛

٤-٢) وضع قوانین و مقررات مناسب کیفری متناسب با اهمیت و نقش زیرساخت‌های حیاتی؛

٤-٣) ایجاد فرایندهای نظارت و ممیزی امنیت سایبری زیرساخت‌های حیاتی.

جدول ٦. اولویت‌بندی گزینه‌های راهبردی

ردیف	اولویت‌بندی	
	عنوان راهبرد	رتبه
١	سازماندهی تیم‌های مدیریت کشف و پاسخگویی به حوادث سایبری و تعامل با سازمان‌های مشابه منطقه‌ای و بین‌المللی	١٤.٣٣
٢	رصد فضای سایبر زیرساخت‌های حیاتی به‌منظور کشف و مواجهه فعال و پیش‌کنشگر با تهدیدات سایبری	١٤.٠٠
٣	ایجاد فرایندهای نظارت و ممیزی امنیت سایبری زیرساخت‌های حیاتی	١٢.٤٥
٤	طبقه‌بندی و حفاظت ویژه از اطلاعات فنی و جغرافیائی زیرساخت‌های حیاتی	١٢.١٣
٥	مدیریت دانش حاصل از تجارب اجرای راهبردهای امنیت فضای سایبر زیرساخت‌های حیاتی	١١.٥٨
٦	حمایت از تولید محصولات ملی و بومی‌سازی تدریجی سیستم‌های کنترل	١١.١٤
٧	ایجاد نظام جامع بومی امنیت سیستم‌های کنترل صنعتی	١١.٣٩
٨	ایجاد مرکز ملی امنیت، حفاظت و نظارت بر زیرساخت‌های حیاتی کشور	١١.٣١
٩	تدوین سیاست‌ها و اصول امنیت فضای سایبر زیرساخت‌های حیاتی	١١.١١
١٠	مدیریت مخاطرات فضای سایبر زیرساخت‌های حیاتی	١٠.٩١
١١	فرهنگ‌سازی و ارائه آموزش‌های عمومی و تخصصی به ذینفعان و بازیگران	١٠.٥٥
١٢	تلاش در جهت رفع یا کاهش آسیب‌پذیری‌ها، امن سازی، مستحکم سازی، و تقویت بازدارندگی	١٠.٤١
١٣	ایجاد فرایندهای ارتباطی و سازماندهی و هماهنگی بین دستگاهی	١٠.٣٩
١٤	ساماندهی و سازماندهی نیروی انسانی متعهد و متخصص	١٠.٢٨
١٥	کشف و تحلیل روندهای جهانی و شناسایی تهدیدهای سایبری زیرساخت‌های حیاتی	١٠.٢٣
١٦	وضع قوانین و مقررات مناسب کیفری متناسب با اهمیت و نقش زیرساخت‌های حیاتی	١٠.٢٣
١٧	توجه به اصل تولید، توسعه و سفارشی‌سازی فرایندها، استانداردها و پروتکل‌ها امنیت سیستم‌های کنترل صنعتی	١٠.٢٠

ردیف	اولویت‌بندی	
	عنوان راهبرد	رتبه
۱۸	ایجاد مکانیسم‌های احراز صلاحیت پیمانکاران و مشاورین سایبری زیرساخت‌های حیاتی	۹.۸۹
۱۹	طبقه‌بندی زیرساخت‌های فیزیکی و اطلاعاتی حیاتی بر اساس سطح اهمیت و شدت تأثیر بر جنبه‌های مختلف حیات	۹.۸۶
۲۰	توجه ویژه به نیازهای قانونی نیروی انسانی شاغل در زیرساخت‌های حیاتی	۹.۳۱
۲۱	کشف وابستگی متقابل بین انواع زیرساخت‌های حیاتی و شدت و تأثیر آن	۹.۳۰

نتیجه‌گیری و پیشنهاد

زیرساخت‌های حیاتی و حساس نقش مهمی در پیشرفت و ثبات نظام‌های سیاسی، اقتصادی و اجتماعی کشورها دارند. پایداری و تداوم خدمات زیرساخت‌ها و صنایع حیاتی کشورها با توجه به اثرگذاری آن بر امنیت ملی مبین اهمیت آن، از جمله اولویت‌های دولت‌ها به شمار می‌رود. تنوع زیرساخت‌ها با توجه به شرایط اقتصادی، فناوری و ژئوپلیتیک ممکن است درکشورهای مختلف اندکی متفاوت باشد. اما وجه اشتراک همه آن‌ها این است که در صورت بروز هرگونه اختلال و یا تخریب آن‌ها اثرات مخرب بر امنیت، اقتصاد، سلامت و ایمنی عمومی جامعه یا ترکیبی از این موارد را در پی خواهد داشت. ازآنجاکه مرکز فرماندهی و کنترل این زیرساخت‌ها در فضای سایبر آن‌ها یعنی سامانه‌های کنترل صنعتی قرار دارد، امنیت سایبری این سیستم‌ها برای سازمان‌های متولی زیرساخت‌های حیاتی به یک چالش مهم تبدیل شده است. ازاین‌رو به‌منظور حفاظت از زیرساخت‌های حیاتی و تداوم فعالیت‌ها و ارائه خدمات توسط آن‌ها به‌عنوان یک ضرورت و اولویت کشور، راهبردهای مؤثر جهت تأمین امنیت سایبری آن‌ها با استناد به تجارب ملی تدوین و ارائه گردید. همچنین برای اتخاذ یک رویکرد کاربردی و اجرائی ازنظرت اثربخش خبرگان و متخصصان سایبری حوزه زیرساخت‌های حیاتی کشور برای تعیین گزینه‌های راهبردی و سپس اولویت‌بندی گزینه‌های راهبردی احصا شده با استفاده از پنل خبرگان و پیمایش و تحلیل آماری از طریق آزمون فریدمن استفاده شد. نتایج تحقیقات نشان داد که اولویت‌های بالاتر بین چهار طبقه مشخص شده توزیع‌شده‌اند و دسته راهبردهای فنی تخصصی و راهبردهای انسانی تعداد بیشتری از اولویت‌های برتر را به خود اختصاص داده‌اند. بر اساس این تحقیق، نتیجه جالب‌تری نیز نمایان گردید و آن اینکه، به ترتیب زوج اولویت‌های اول تا پنجم به‌مثابه یک پازل تجربه با تکمیل

یکدیگر، راهنمای ارزشمندی را پیش‌روی کارگزاران ذی‌ربط قرار می‌دهند.

راهبرد اول با عنوان سازمان‌دهی تیم‌های مدیریت کشف و پاسخگویی به حوادث سایبری و تعامل با سازمان‌های مشابه منطقه‌ای و بین‌المللی، مکمل دومین راهبرد با عنوان رصد فضای سایبر زیرساخت‌های حیاتی به‌منظور کشف و مواجهه فعال و پیش‌کنشگر با تهدیدات سایبری است. چراکه با توجه به گسترش دامنه تهدیدات سایبری در نقاط مختلف جهان و به‌ویژه زیرساخت‌های حیاتی کشور طی سال‌های اخیر و پیامدهای مخرب و فراگیر آن در جامعه اولین گام برای مقابله، پیشگیری است که با تشکیل تیم‌های ویژه و قرمز، امکان رصد و کشف تهدیدات و حملات در فضای سایبر زیرساخت‌های حیاتی پیش از وقوع میسر می‌شود، همان‌گونه که در (وزارت انرژی، ۲۰۰۲) و (افشار و همکاران،۱۳۹۳) بر آن تأکید شده است. راهبردهای سوم و چهارم نیز لازم و ملزوم یکدیگرند چرا که ایجاد فرایندهای نظارت و ممیزی امنیت سایبری زیرساخت‌های حیاتی مستلزم طبقه‌بندی و حفاظت ویژه از اطلاعات فنی و جغرافیائی زیرساخت‌های حیاتی است و برعکس. که در استاندارد (ایزو ۲۰۱۳) اکیداً توصیه شده است. مدیریت دانش حاصل از تجارب اجرای راهبردهای امنیت فضای سایبر زیرساخت‌های حیاتی به‌عنوان راهبرد پنجم می‌تواند اساس تولید محصولات داخلی و بومی‌سازی تدریجی سامانه‌های کنترل صنعتی در کشور (راهبرد ششم) باشد. که در این خصوص به آن پرداخته است (مددی و همکاران،۱۳۹۳). همان‌گونه که در (بوش، ۲۰۰۱) تأکید شده، برای تعیین ارکان حاکمیتی، ایجاد مرکز ملی امنیت، حفاظت و نظارت بر زیرساخت‌های حیاتی کشور (راهبرد هفتم) باید دستور کار سیاست‌های این حوزه باشد. همچنین ضرورت تعریف فرایندها و تبیین تعاملات بین ذی‌نفعان در قالب ایجاد نظام جامع بومی امنیت سیستم‌های کنترل صنعتی(راهبرد هشتم) باید مدنظر قرار گیرد. که این موضوع در (باما، ۲۰۱۳) تأکید شده است. مرکز ملی مذکور در واقع وظیفه راهبری، نظارت و هماهنگی بین سایر کارگزاران اجرائی در کشور را عهده‌دار خواهد بود. به‌منظور برقراری امنیت سایبری سامانه‌های کنترل صنعتی، ضرورت تدوین سیاست‌ها و اصول امنیت فضای سایبر زیرساخت‌های حیاتی (راهبرد نهم) و نهادینه نمودن آن‌ها در فرایندها و دارائی‌های سازمانی روشن است(ستوفر و همکاران،۲۰۱۱). همچنین برای اطمینان از رعایت این اصول لازم است از روش‌های استاندارد مدیریت مخاطرات فضای سایبر زیرساخت‌های حیاتی (راهبرد دهم) استفاده شود تا از پوشش امنیتی بر ریسک‌های احتمالی مترتب بر هر یک از دارائی‌ها مطمئن گردید، که به اهمیت و

روش‌های آن در منابع (دورمامی و همکاران،۲۰۱۰؛ سربه و همکاران،۲۰۱۳) اشاره شـده اسـت. سایر راهبردها اگرچه در اولویت‌های پایین‌تری نسبت به موارد مطرح شده قرار گرفته‌انـد لـیکن نقش آن‌ها در تکمیل بحث غیرقابل انکار است.

منابع و مآخذ

الف) منابع فارسی

- افشار، ا؛ ترمه‌چی، ع؛ گلشن، ع؛ آقائیان، آ؛ شهریاری، ح (۱۳۹۳). «مروری بر امنیت سایبری سیستم‌های کنترل صنعتی»، مجله کنترل، انجمن مهندسان کنترل و ابزار دقیق ایران، سال هشتم، شماره ۱، صص ٤٥-۳۱.
- جلالی، غ (۱۳۹۰). فضای سایبر، پنجمین عرصه جنگ است. قابل دسترسی در سایت: www.aftabir.com/news/view/2012/feb/18/c1_1329558363.php
- عبد التاجدینی، م (۱۳۹۲). «معرفی بخش‌های آسیب پذیر سامانه‌های کنترل صنعتی و اسکادا از دیدگاه سایبری و ارائه راهکارهائی جهت بهبود و ارتقای امنیت در آن‌ها»، ماهنامه صنعت هوشمند، سال چهارم، شماره سوم.
- مددی آتشگاه، ح؛ افشار نادری، م؛ و قزلجه، ع (۱۳۹۳). «دفاع سایبری دانش‌بنیان با رویکرد بومی‌سازی تکنولوژِی»، اولین کنفرانس ملی علوم مهندسی و ایده‌های نو، تهران: موسسه آموزش عالی آیندگان.

ب) منابع انگلیسی

- Angelini, M., Arcuri, M. C., Baldoni, R., Ciccotelli, C., Di Luna, G. A., Montanari, L., Verde, N. V. (2013). Italian Cyber Security Report Critical Infrastructure and Other Sensitive Sectors Readiness. ROME, Research Center of Cyber Intelligence and Information Security.
- Bush, G. W (2001). Executive Order 13231: Critical Infrastructure Protection in the Information Age, Pub. L. No. EO 13231; http://www.gpoaccess.gov/fr/
- Doremami, N., Afshar, A., و Mohammadi, A. D. (2010). Hierarchical Risk Assessment in Gas Pipelines Based on Fuzzy Aggregation end International Conference on Reliability, Safety and Hazard, IEEE.
- Dummermuth, Ernst. (1974). US Patent # 3,942,158. Programmable logic controller. Allen-Bradley Company. http://www.patents.com/us-3942158.html
- Good practice guide on non-nuclear critical energy infrastructure protection(NNCEIP). (2013). Organization for Security and Co-operation in Europe. www.osce.org

- Gostev, A. (2012). Kaspersky Security Bulletin 2012. Kaspersky. https://securelist.com/analysis/kaspersky-security-bulletin/36762/kaspersky-security-bulletin-2012-cyber-weapons/
- Hadziosmanovic, D., Bolzoni, D., Etalle, S., و Hartel, P. (2012). Challenges and opportunities in securing industrial control systems Proceedings of the IEEE Workshop on Complexity in Engineering, COMPENG 2012, Aachen, Germany: University of Twente and yEindhoven Technical University The Netherlands.
- HomeLand Security. (2009). Recommended Practice : Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies," 2009. HomeLand Security. https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf
- Igure, V. M., Laughter, S. A., و Williams, R. D. (2006). Security issues in SCADA networks. Computers & Security, 25(7), 498–506. http://doi.org/10.1016/j.cose.2006.03.001
- ISO27001. (2013). ISO/IEC 27001:2013 Information technology Security techniques -- Information security management systems Requirements. ISO. http://www.iso.org/iso/catalogue_detail?csnumber=54534
- Leszczyna, R., Egozcue, E., Tarrafeta, L., Villar, V. F., Estremera, R., و Alonso, J. (2011). Protecting Industrial Control Systems. Recommendations for Europe and Member States ENISA. European Network and Information Security Agency (ENISA): ENISA. بازیابی از https://www.enisa.europa.eu/publications/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states
- Miller, B., و Rowe, D. (2012). A survey SCADA of and critical infrastructure incidents st Annual conference on Research in information technology - RIIT, Calgary, Alberta, Canada: ACM Press. http://doi.org/10.1145/2380790.2380805
- Obama. Improving Critical Infrastructure Cybersecurity Executive Order 13636-Preliminary Cybersecurity Framework, Pub. L. No. 13636 (2013). http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf
- Office, و Office of Energy Assurance. (2002). 21 Steps to Improve Cyber Security of SCADA Network. U.S. Department of Energy.

http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps - SCADA.pdf

- Ralston, P. A. S., Graham, J. H., و Hieb, J. L. (2007). Cyber security risk assessment for SCADA and DCS networks. ISA Transactions, 46(4), 583–594. http://doi.org/10.1016/j.isatra.2007.04.003
- Rinaldi, S. M., Peerenboom, J. P., و Kelly, T. K. (2001). Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Magazine, 11–25.
- Robles, R. J., و Park, G.-C. (2011). Securing Communication between SCADA Master Station and Mobile Remote Components. Communications In Computer And Information Science, 200, 203–210.
- Ross, R. S. (2011). Managing Information Security Risk: Organization, Mission, and Information System View. NIST. http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf
- Saurabh, A., Schwartz, G. A., و Hussain, A. (2013). In Quest of Benchmarking Security Risks to Cyber-Physical Systems. IEEE Network, 27(1), 18–25.
- SCADA Systems: A Comparision of RTUs and PLCs. (2007). Motorola https://www.motorolasolutions.com/content/dam/msi/Products/scada-systems/SCADA_Sys_Wht_Ppr-2a_New.pdf
- Stouffer, K., Falco, J., و Scarfone, K. (2011). Guide to Industrial Control Systems (ICS) Security -Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-82.
- Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., و Hahn, A. (2015). Guide to Industrial Control Systems (ICS) Security Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology. بازیابی از http://dx.doi.org/10.6028/NIST.SP.800-82r2
- Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., و Hahn, A. (2015). Guide to Industrial Control Systems (ICS) Security Recommendations of the National Institute of Standards and Technology-Revision 2. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-82r2
- Tabansky, L. (2011). Critical Infrastructure Protection against Cyber Threats. Military And Strategic Affairs, 3(2).