تاریخ دریافت: ۱۳۹۹/۰۹/۲۱
تاریخ پذیرش: ۱۴۰۰/۰۲/۲۸

فصلنامه علوم و فنون نظامی
سال شانزدهم، شماره ۵۵، بهار ۱۴۰۰
صص ۵۰- ۲۷

# تبیین آسیب‌پذیری‌های فناورانه سامانه مکانیزه لجستیک نیروی هوایی ارتش جمهوری اسلامی ایران در برابر تهدیدات آینده و ارائه راهکارهای مناسب

رضا روشنی[۱]
حسین اکبری*[۲]
حمیدرضارضائی[۳]

**نوع مقاله: پژوهشی**

**چکیده**

سامانه مکانیزه لجستیک نهاجا یکی از سامانه‌های مهم و تأثیرگذار در پشتیبانی از پایگاه‌های هوایی و مراکز تعمیری نهاجا است که نقش بسزایی در عملیاتی نگه‌داشتن هواپیماها، وسایل زمینی و تجهیزات فرودگاهی در سطح نهاجا ایفا می‌کند؛ بنابراین هدف این پژوهش تبیین آسیب‌پذیری‌های فناورانه سامانه مکانیزه لجستیک نهاجا در برابر تهدیدات آینده و ارائه راهکارهای مناسب است. نوع پژوهش کاربردی، روش اجرای آن توصیفی و رویکرد آن آمیخته است. جامعه آماری در این تحقیق ۷۰ نفر به‌صورت تمام شمار شامل کارشناسان و مدیران آگاه به موضوع، طی سال‌های ۱۳۹۷-۱۳۹۶ در سطح ستاد نهاجا و شهر تهران است. ابزار گردآوری داده‌ها پرسشنامه محقق ساخته بود که روایی آن به رؤیت صاحب‌نظران، اساتید محترم راهنما و مشاور رسیده و پایایی آن با استفاده از ضریب آلفای کرونباخ ۰/۸۵۸ استخراج شد. با استفاده از آمار توصیفی و استنباطی داده‌های به‌دست‌آمده تجزیه‌وتحلیل شد و نتایج نشان داد که آسیب‌پذیری‌ها شامل؛ عدم پایداری شبکه ارتباطی با پایگاه‌های هوایی، عدم پیش‌بینی شبکه ارتباط رادیویی سیار، نداشتن سایت پشتیبان، آسیب‌پذیری در برابر بمب‌های الکترومغناطیسی و گرافیتی دشمن و ضعف تأسیساتی و امنیتی به دلیل عدم مقاوم‌سازی تأسیسات سرویس‌دهنده مرکزی هستند.

**واژه‌های کلیدی:**
***تهدیدات آینده، سامانه مکانیزه لجستیک، فناوری اطلاعات، نهاجا.***

---

۱- عضو هیئت‌علمی و استادیار دانشگاه فرماندهی و ستاد آجا، تهران، ایران.
۲- عضو هیئت‌علمی دانشگاه فرماندهی و ستاد آجا و دانشجوی دکترای تخصصی دانشگاه علامه طباطبائی، تهران، ایران.
۳- کارشناس ارشد مدیریت دفاعی، دانشگاه فرماندهی و ستاد آجا، تهران، ایران.
*نویسنده مسئول: akbari.ho@gmail.com

**مقدمه**

ارتش جمهوری اسلامی ایران در هر شرایطی برای انجام مأموریت‌های دفاعی و نظامی خود به سامانه آمادوپشتیبانی قوی، چابک و مداوم نیاز دارد. درگذر تاریخ جنگ‌ها، پشتیبانی آمادی از عملیات نظامی به‌وضوح ارزش خود را نمایان ساخته و نقش مهم و سازنده‌ای را در کسب پیروزی به همراه داشته است، به‌گونه‌ای که آماد رسانی و جنگ رابطه تنگاتنگ و انفصال ناپذیر دارند و اصولاً جنگ‌ها بدون آماد رسانی مناسب به پیروزی دست پیدا نمی‌کنند (زینلی، ۱۳۹۴:۱۰۰). برآورد، تأمین و توزیع اقلام و تجهیزات از مهم‌ترین فعالیت‌های سامانه آمادوپشتیبانی است که می‌بایستی نسبت به تأمین ملزومات نیروهای نظامی تحت پشتیبانی در زمان مناسب، مکان مناسب، باکیفیت مناسب و به مقدار کافی اقدام نماید. با توجه به اینکه مأموریت‌های نیروی هوایی ارتش جمهوری اسلامی ایران با خصوصیات واکنش سریع، تحرک و برد زیاد، پشتیبانی از نیروهای سطحی و تداوم عملیات با استفاده از انواع هواپیماها و سامانه‌های ارتباطی انجام می پذیرد، نیازمند سامانه آمادوپشتیبانی منعطف و پاسخگو بوده و یکی از سامانه‌های مهم و تأثیرگذار که نقش بی‌بدیل در پشتیبانی از هواپیماها را بر عهده دارد، سامانه مکانیزه لجستیک (ALS) نهاجا در مرکز کنترل ماتریل فرماندهی آمادوپشتیبانی هوایی نهاجا است. این سامانه، برای متمرکز کردن مدیریت و کنترل بر کلیه اقلام پشتیبانی تجهیزات عمده نهاجا و وسایل پشتیبانی آن‌ها سازمان‌دهی شده و در این تحقیق جهت جلوگیری از ایجاد وقفه و اخلال در عملکرد صحیح این سامانه و حفظ توان پشتیبانی خدمات رزمی با این سؤال که آسیب‌پذیری‌های فناورانه سامانه مکانیزه لجستیک نهاجا کدام‌اند و راهکارهای مقابله با آن‌ها چیست؟ به تبیین آسیب‌پذیری‌های فناورانه سامانه در برابر تهدیدات آینده پرداخته تا از زمین‌گیر شدن هواپیماها، کاهش قدرت هوایی و تشدید ناامنی در مرزهای هوایی جلوگیری به عمل آید.

مسئله اصلی این پژوهش این است که در صورت بروز هرگونه تهدیدات آینده و وارد آمدن آسیب به شبکه اطلاعاتی و ارتباطی آن، موجب ایجاد وقفه و اخلال در عملکرد صحیح و ایجاد ناامنی سامانه شده که نشان از ضعف در فناوری اطلاعات و ارتباطات (شبکه ارتباطی، ایستگاه‌های کاری و سرویس‌دهنده مرکزی) بوده و باعث کاهش توان پشتیبانی خدمات رزمی، زمین‌گیر شدن هواپیماها، کاهش توان عملیاتی پایگاه‌های هوایی و درنهایت کاهش قدرت هوایی و تشدید ناامنی در مرزهای هوایی می‌گردد. به همین منظور هدف اصلی از انجام این تحقیق، تبیین آسیب‌پذیری های فناورانه سامانه مکانیزه لجستیک نهاجا در برابر تهدیدات آینده و ارائه راهکارهای مناسب و اهداف فرعی عبارت‌اند از تبیین آسیب‌پذیری‌های ایستگاه‌های کاری، تبیین آسیب‌پذیری‌های شبکه ارتباطی و تبیین آسیب‌پذیری‌های سرور مرکزی سامانه مکانیزه لجستیک نهاجا در برابر

تهدیدهای آینده و ارائه راهکارهای مناسب است. محقق به دنبال آن است با تبیین آسیب‌پذیری های فناورانه در حوزه فناوری اطلاعات و ارتباطات راه‌کارهای مناسبی را قبل از وقوع هرگونه تهدید و همچنین کاهش آسیب‌پذیری‌ها به‌منظور مداومت آماد رسانی در شرایط بحران اقدام نماید. با در نظر گرفتن تهدیدهایی که در آینده ممکن است پیش روی این سامانه باشد، به دلایل؛ نیاز به پیش‌بینی واقعی و برآورد معقول، تأمین سریع و هدایت قطعات به گردان‌های آماد و نگهداری پایگاه‌ها و آماد رسانی به‌موقع و کافی در زمان تهدیدات، لزوم در اختیار داشتن مجموعه‌ای از آمادوپشتیبانی مؤثر، منعطف و چابک و لزوم تحقق طرح‌ها و برنامه‌های آمادوپشتیبانی به‌ویژه در هنگام تهدیدات؛ تبیین آسیب‌پذیری‌های فناوری اطلاعات و ارتباطات سامانه مکانیزه لجستیک نهاجا از اهمیت بالایی برخوردار است و اتخاذ تدابیر در راستای آماد رسانی مداوم و به‌موقع برای پایگاه‌های هوایی، بااهمیت به نظرمی رسد. همچنین با توجه به حیاتی بودن برقراری شبکه ارتباطی این سامانه با گردان‌های آماد متمرکز پایگاه‌های هوایی، مراکز تعمیراتی و همچنین آمادگاه اصلی فرماندهی آمادوپشتیبانی هوایی، تبیین آسیب‌پذیری در حوزه‌های فناوری اطلاعات و ارتباطات، سامانه آماد فنی نهاجا ضروری است؛ در غیر این صورت تأثیر منفی چشمگیری بر عملیاتی نگه‌داشتن انواع هواپیماها، بالگردها و سامانه‌های ارتباطی و تجهیزات فرودگاهی داشته و موجبات کاهش قدرت هوایی و توان بازدارندگی نیروی هوایی در برابر دشمنان متخاصم خواهد داشت.

## مبانی نظری پژوهش

### آماد فنی

تدارکات و آماد در لغت به معنی تهیه کردن، آماده ساختن و عوض چیزی را فراهم کردن آمده است. آماد به‌عنوان یکی از عوامل آمادوپشتیبانی از عناصر مهم و مؤثر تشکیل‌دهنده قدرت نظامی به‌حساب می‌آید. (زینلی، ۲۰:۱۳۹۴) آماد در نهاجا یکی از سامانه‌های بزرگ است که با در برگرفتن صدها هزار قلم جنس مصرفی و ابواب‌جمعی تعمیری و داغی دار نقش بسیار مهمی در عملیاتی نگه‌داشتن دستگاه‌ها ایفا می‌نماید. بخش آمادفنی شامل مجموعه فرآیندها و فعالیت‌های تخصصی آمادی ازجمله اقلام فنی، قطعات یدکی و تجهیزات (دستگاه‌ها، تسترها و خودروها) موردنیاز انواع سامانه‌های عمده پروازی و تخصصی نهاجا است که بر مبنای به‌کارگیری سیستم‌های مدیریت اطلاعات بر روی بستر بزرگ‌رایانه[۱] و تحت عنوان سیستم مکانیزه آمادفنی طراحی گردیده است. مرکز کنترل ماتریل ضمن مسئولیت مدیریت موجودی و پیش‌بینی

[۱]- MAINFRAME

نیازمندی‌های اقلام و قطعات فنی و پالایش درخواست‌های انجام‌شده توسط یگان‌های نهاجا و پیش‌بینی جهت چگونگی تأمین آن‌ها از منابع تأمین نیروی هوایی (داخلی و خرید خارج) را بر عهده دارد و مهم‌ترین وظایف این مرکز شامل کنترل موجودی، محاسبه تعداد اقلام موردنیاز، ایجاد ارتباط بین مراکز تهیه و تولید، نگهداری و تعمیر، درخواست از منابع داخل و خارج و همچنین پیش‌بینی و درخواست کلیه نیازمندی‌های سوخت و مواد نفتی موردنیاز یگان‌های نهاجا است. (دستورالعمل ۱-۳۶ ف آمادوپشتیبانی هوایی،۱۳۸۱: ۲) با نگرش به این موضوع که پشتیبانی خدمات رزمی در هر عملیات بدون تردید در ردیف حساس‌ترین مأموریت‌ها قرار دارد و در میدان نبرد، یکی از موارد تعیین کنند و سرنوشت‌ساز است، بدیهی است انجام دقیق این مأموریت نیاز به مدیریتی قوی و برنامه‌ای جامع دارد. سامانه آمادوپش با مدنظر قرار دادن میزان ضربه‌پذیری طرح‌های عملیاتی و حوزه‌های دفاعی تحت پوشش خود، امکانات آمادوپش اعم از تجهیزات و کارکنان را باید به‌گونه‌ای توزیع نماید که تمامی نیازمندی‌های نیروهای رزمی را پوشش دهد؛ بنابراین آمادوپشتیبانی درعین‌حال که از انعطاف‌پذیری و چابکی ویژه‌ای نیز برخوردار است باید به‌سرعت بتواند مأموریت‌های مختلف را پشتیبانی نماید. گستردگی شبکه در سطح کشور از ویژگی‌های بارز آمادوپشتیبانی پیشرفته است که همه واحدها و افراد، تحت شبکه هم‌زمان و هم‌فکر و هم‌جهت و هم حرکت می‌گردند. دیگر درخواستی مفقود نمی‌گردد، حتی اگر پاسخ منفی باشد بدون جواب باقی نخواهد ماند و زمان عملیات در این سامانه روی هر درخواست ثبت سابقه و گردش هر اعلام نیاز آمادوپشتیبانی حفظ می‌گردد. (آقا محمدی،۱۳۹۲: ۱۹۱-۲۰۴)

**سامانه مکانیزه لجستیک نهاجا**

سامانه مکانیزه لجستیک نهاجا مجموعه سیستم‌های به هم پیوسته‌ای است که به‌منظور مکانیزه نمودن ابعاد مختلف آمادوپشتیبانی در نهاجا طراحی و اجرا گردیده و مطالعه اولیه آن از سال‌های ۱۳۴۷ تا ۱۳۴۹ شروع و با استفاده از تجهیزات رایج رایانه‌ای تحت عنوان پی کم[۱] آغاز به کار نموده، در سال ۱۳۵۳ سخت‌افزار هانیول[۲] ۶۰۶۰ نیز خریداری و جهت پیاده‌سازی مورد بهره‌برداری قرار گرفت.(لطیفی،۱۳۸۸:۴۳) با توجه به اینکه نیروی هوایی، نیرویی تجهیزات محور است ازاین‌رو قطعه رسانی به‌موقع و سریع جهت عملیاتی نگه‌داشتن هواپیماها، وسایل زمینی، تجهیزات ارتباطی و فرودگاهی مستلزم ارتباط مداوم شبکه‌ای گردان‌های آماد پایگاه‌های هوایی

---

۱- PCAM

۲- HONIWELL

با فرماندهی آمادوپشتیبانی هوایی نهاجا از طریق این سامانه است. زبان سیستم‌عامل مورداستفاده، جیکاس[۱] و سیستم‌های فرعی از دو بعد اطلاعات و مدیریت کلی بر مأموریت‌های آمادوپشتیبانی کاملاً وابسته به یکدیگر بوده و توسط کاربران در سراسر نهاجا کاربری می‌شوند. محیط کاربردی و بسته نرم‌افزاری کاربردی موجود در نهاجا که کلیه برنامه‌های اجرایی فعلی با آن تهیه‌شده کوبول ۲۲۰۰۰ بوده و بانک اطلاعاتی به حالت فایلی۳ (دیتابیس ۲) است که بازنویسی شده است. به‌منظور اعطای قدرت و ابزار مدیریت و کنترل بر آمادهای یگان‌ها، از میان برداشتن کلیه معایب فوق، شیوه موجود حذف و با به‌کارگیری اطلاعات متعدد مدیریتی یک سیستم جدید جهت تحقق خواسته‌های موردنظر با ویژگی‌های زیر طراحی گردید:

- ایجاد بانک‌های اطلاعاتی مدیریتی متعدد جهت ذخیره‌سازی اطلاعات دستگاه‌های موجود در هر شعبه
- امکان ارائه اطلاعات به شعبه کنترل کیفیت در ماتریل کنترل گردان‌های نگهداری جهت تجزیه‌وتحلیل عیوب
- توان بازیابی اطلاعات، استقلال اطلاعات و فراهم نمودن گزارش‌های مدیریتی در زمان کوتاه
- فراهم آمدن امنیت لازم بدین ترتیب که دسترسی هر کاربر فقط به‌اندازه معیارهای تعیین‌شده برای خود باشد
- امکان قابلیت توسعه و تطبیق برنامه‌های کاربردی با نیازمندی‌های جدید نهاجا

بنابراین برنامه‌هایی که برای سامانه جدید آمادفنی نهاجا در نظر گرفته شد می‌بایست کلیه نواقص و اشکالات سامانه قدیم را پوشش داده به‌گونه‌ای که بتواند رضایتمندی همه‌جانبه کاربران و مدیران سامانه را فراهم آورده و توان انتقال اطلاعات و دریافت شفاف نیازمندی‌ها و همچنین تهیه گزارش‌های مدیریتی را در کمترین زمان برای سلسله‌مراتب داشته باشد لذا سامانه جدید آمادفنی مزیت‌های زیر را در بردارد:

- افزایش چشم‌گیر حیطه سرویس‌دهی کامپیوتر در هریک از یگان‌ها و امکان افزایش کاربران در داخل هر یگان
- صرفه‌جویی در هزینه‌های مخابراتی در اثر کاهش ارتباط مستمر یگان‌ها با مرکز
- افزایش قابل‌توجه سرعت در پاسخ‌گویی سیستم به نیازهای کاربران و افزایش امنیت اطلاعات ذخیره‌شده

---

۱- GCOS
۲- COBOL 2000
۳- DB2

- دسترسی سریع کاربران به اطلاعات اختصاصی خود از طریق شبکه‌های محلی
- تداوم حیات سیستم در هریک از یگان‌ها در اثر قطعی ارتباط (کارساز، مصاحبه شخصی،۱۳۹۶)

**تهدیدات آینده**

همان‌گونه که می‌دانیم طرح‌ریزی عملیاتی دشمن بر مبنای حمله به آسیب‌پذیری‌های ما در مراکز ثقل و مهم ما استوار است که امروز اهداف نظامی یکی از آن‌هاست. استیل (۱۹۹۸) هرم آسیب‌پذیری برای کشورهای توسعه‌یافته را با نگاه اطلاعات محوری ترسیم کرده که از پایین به بالا شامل زیرساخت‌های فیزیکی، نقاط ضعف نظامی، زیرساخت‌های غیرنظامی، داده‌های آمادوپشتیبانی، داده‌های مالی و جامعه اطلاعاتی است.(حبیبی، ۱۳۹۲: ۲۱۹) به دلیل اینکه در بحران‌ها، درک و شناخت دو مفهوم آسیب‌پذیری و تهدید بسیار مهم است؛ بنابراین شناخت تهدیدات زمانی میسر است که طراحان و فرماندهان نظامی، به درک معقولی از ماهیت تهدیدها و آسیب‌پذیری‌های مرتبط با آن دست یابند. (حبیبی، ۱۳۹۲: ۳۷۳) در تعریف آمده است که تهدید به معنی تمایل و قصد آسیب رساندن، نابود یا تنبیه کردن دیگران باانگیزه انتقام یا ارعاب است. با نگرش به این‌که رشد شتابان تحولات محیط امنیتی، فناوری و سامانه‌های دفاعی، آینده را از گذشته بسیار متفاوت نموده است و این رشد و وابستگی بسیار حساس به محیط خود، باعث شده که نظام‌ها تدابیری بیندیشند تا همواره نسبت به تغییرات محیط فعالیت خود و تأثیرات نهایی و آشکار این تغییرات بر نظام موردنظرشان تا حد امکان آگاه باشند؛ بنابراین یکی از وظایف اساسی کشور، توجه به آینده و کسب آمادگی‌های لازم برای مقابله با چالش‌های در پیش رو است. به این معنا که همواره بامطالعه مؤلفه‌های مؤثر بر آینده، احتمال‌های موجود را بررسی کرده و آمادگی لازم را کسب و شرایط مواجه با آن را فراهم آورند. شناخت صحیح ویژگی‌های تهدیدات آینده ما را قادر خواهد ساخت تا روش‌های برون‌رفت از معضلات ناشی از این تهدیدات را درک کنیم. این روش‌های برون‌رفت شامل روش‌های پیشگیری و بازدارندگی، پیش‌دستی، تهاجم، مقابله و دفاع در برابر تهدیدات آینده خواهد بود (حسن بیگی،۱۳۹۴:۴۱).

همان‌گونه که می‌دانیم در آینده ماهیت اصلی تهدید دشمن، نظامی است؛ یعنی اقدامات آن در بستر اقدامات نظامی شکل می‌گیرد. ولی مسئله فناوری و میزان مدرن بودن سامانه‌های عملیاتی، تهاجمی، اطلاعاتی، شناسایی، کنترل و فرماندهی به‌شدت بر توان نظامی مؤثر بوده و ماهیت حرکت نظامی را در درون خود، از انسان‌محور به فناوری محور تبدیل می‌کنند. این یعنی ترجیح فناوری بر انسان، لذا توان نظامی دشمن با محوریت فناوری و مدیریت است. لذا می‌توان ماهیت این تهدید را فناورانه بیان کرد. در تهدیدات فناورانه اولویت‌های تهاجم، حمله به مراکز صداوسیما

و ارتباطات و مخابرات، حمله به سیستم دفاع هوایی (سامانه‌های هشداردهنده، رادار، سایت‌ها) و سامانه‌های فرماندهی و کنترل، زیرساخت‌های صنعتی، اقتصادی، دفاعی و نظامی و مراکز تحقیق و توسعه هسته‌ای، مراکز تولید موشک، سلاح راهبردی و صنعت دفاعی است.(مرادیان، ۱۳۹۱: ۳۷۳) در جنگ‌های آینده نباید منتظر باشیم که دشمن حتماً حمله را از مناطق مقدم نبرد آغاز کند. بلکه شاید ابتدا دشمن به سراغ اهدافی در عمق کشور رفته و جنگ را از عمق شروع کرده سپس جنگ را به سطوح عملیاتی و تاکتیکی تسری دهد (حیدری،۱۷۲:۱۳۹۰). در جنگ‌های آینده دشمن از هدف‌های عمیق و راهبردی، عملیات را آغاز می‌کند و مراکز ثقل را مورد هدف قرار می‌دهد. جنگ‌های آینده قبل از اینکه مخلوطی از درگیری با سلاح‌های معمولی و یا جنبشی باشد شامل انواع سلاح‌های سایبری به‌عنوان یک قطع کننده ارتباطی بین نیروها است و کسب برتری سریع در حوزه‌ی فناوری اطلاعات یکی از عوامل کلیدی موفقیت خواهد بود. همه‌ی انسان‌ها، سازمان‌ها و ارگان‌ها ناگزیرند این واقعیت را بپذیرند که دیگر فضای مجازی (فناوری در جنگ‌های آینده) از فضای واقعی جدا نیست یا در برابر آن نیست، بلکه آمیخته با آن و نیز مکمل فضای واقعی است و می‌تواند سبک زندگی را برای انسان‌ها تولید کند. (حافظ نیا، ۱۳۹۰: ۳) خطر هنگامی روی می‌دهد که تهدیدات خارجی بر عوامل داخلی آسیب‌پذیر، تأثیرات تخریبی بگذارد؛ بنابراین اگر تهدیدات بر آسیب‌پذیری‌ها منطبق نگردد، خطر به وجود نمی‌آید. آنچه در کاهش آسیب‌پذیری مدنظر است عبارت‌اند از: کم شدن درجه ریسک و خطر، کاهش تهدید و حمله، کاهش خسارات بر تأسیسات، کاهش تلفات نیروی انسانی و خسارت وارده بر تجهیزات (امینی ورکی و همکاران، ۱۳۹۵: ۱۱۲) برای شناسایی نقاط بحرانی و آسیب‌پذیر در زیرساخت‌ها، نباید منتظر وقوع شکست یا خرابی ماند، بلکه باید برای پیش‌بینی مشکلات تهدیدات در حال شکل‌گیری تلاش کرده و پیش از آنکه اختلال‌های بزرگ روی دهد، استراتژی‌های اثربخش کاهش آسیب‌پذیری را شناسایی کرد. این مسئله به‌ویژه در شرایط تهدیدات انسان‌ساخت، بحران‌های طبیعی و حوادث غیرمترقبه به‌خوبی خود را نشان می‌دهد. (امینی ورکی و همکاران، ۱۳۹۵: ۶۱) تهدیدهای ساختمان‌ها به دودسته بلایای طبیعی و انسان‌ساخت تقسیم می‌شوند. تهدیدهای ناشی بلایای طبیعی (آتش‌سوزی، زلزله و...)، تهدیدهای انسان‌ساخت شامل تهدیدهای نظامی (تهاجم هوایی، زمینی و دریایی)، تهدیدهای امنیتی (عملیات خرابکارانه، بمب‌گذاری) و تهدیدهای اتفاقی (آتش‌سوزی، انفجار مخازن سوخت) تقسیم می‌شوند. (نیری، ۱۳۹۲: ۱۲) ساختمان‌های اداری قدیمی، فاقد مقاومت لازم در برابر وقوع یک زمین‌لرزه شدید یا تهدیدات سخت (حملات هوایی، زمینی، دریایی و فضایی) و نیمه سخت هستند (بمب‌های گرافیتی[۱] و

[۱]- Graphite unit bomb

الکترومغناطیسی) هستند.(جلالی فراهانی،۱۳۹۱:۱۵۰) بانک‌های اطلاعاتی، تأسیسات ارتباطی پایگاه‌های نظامی، سایت‌های راداری و موشکی از اهداف اصلی بمب‌های گرافیتی و الکترومغناطیسی بوده و در صورت ضعیف بودن ساختار زیر بنایی می‌بایست از راهکار قفس فارادی و هدف کاذب استفاده کرد. قفس فارادی از ورود میدان الکترومغناطیسی به داخل تجهیزات جلوگیری می‌نماید.(گلنتاج،۱۳۹۵:۶۳) جهت تقلیل آسیب‌پذیری تأسیسات در برابر حملات هوایی، زمینی، دریایی و فضایی. تمرکززدایی، تفرقه و پراکندگی کارکنان تجهیزات از محل استقرار اصلی به محل دیگر بسیار ضروری خواهد بود.(حبیبی، ۱۳۹۲: ۳۴۵) همچنین در خصوص مقاوم‌سازی ساختمان‌ها باید متخصصین و مسئولین اقدامات لازم را در این خصوص به عمل‌آورند؛ بایگانی پرونده‌ها و انبار از اماکنی هستند که به علت وجود وسایل قابل اشتعال، پس از وقوع یک زلزله شدید و یا آتش‌سوزی، در معرض خطر قرارگرفته و باید به سیستم اعلام و اطفا حریق خودکار و هوشمند مجهز شوند (میر سمیعی و چشمه نور، ۱۳۹۵: ۱۰۸).

**فناوری اطلاعات و ارتباطات[1]**

به مجموعه‌ای از دانش، روش‌ها و ابزارها، سخت‌افزار و نرم‌افزار که به‌منظور تسهیل و انجام فرآیند تولید، گردآوری، سازمان‌دهی، ذخیره، بازیابی و نشر اطلاعات با استفاده از رایانه به‌عنوان ابزار پردازش و شبکه به‌عنوان شاهراه ارتباطی به کار گرفته می‌شوند، فناوری اطلاعات و ارتباطات گفته می‌شود (آذر و مسلمی، ۱۳۹۳: ۱۶). از دلایل آسیب‌پذیری سیستم‌های اطلاعاتی و ارتباطی می‌توان پیشرفت در ارتباطات و نرم‌افزارهای رایانه‌ای، دسترسی‌های غیرمجاز، سوءاستفاده و یا تقلب در داده‌ها، نفوذ گران هکرها، ویروس‌های رایانه‌ای نام برد. (حسن‌زاده اسدی و همکاران، ۱۳۹۰:۳۰) با رشد و توسعه فزاینده فناوری اطلاعات و گسترش شبکه‌های ارتباطی، آسیب‌پذیری فضای تبادل اطلاعات افزایش‌یافته است و روش‌های اعمال تهدیدهای یادشده پیچیده‌تر می‌شود. ازاین‌رو حفظ ایمنی فضای تبادل اطلاعات ازجمله مهم‌ترین اهداف توسعه فناوری اطلاعاتی و ارتباطی محسوب می‌شود. (مدیری و شاه ولایتی،۱۳۹۰: ۲۹) ضعف امنیتی موجود در داخل یک سرمایه، رویه‌های امنیتی یا کنترل‌های داخلی، یا پیاده‌سازی آن سرمایه ملی سایبری که قابلیت بهره‌برداری یا فعال شدن توسط تهدیدات داخلی و خارجی به‌منظور جنگ سایبری را داشته باشد، آسیب‌پذیری سایبری اطلاق می‌گردد.(جلالی فراهانی و همکاران،۱۳۹۵: ۵۰) و روش‌های حمله در عملیات حمله رایانه‌ای عبارت‌اند از:

- نفوذ گر (هکر) کسی است که با دانش خود می‌تواند وارد سایت‌ها و سیستم‌ها شده و اقدام به یکسری کارها و عملیات نماید و انواع آن شامل نفوذ گران کلاه‌سفید، کلاه‌سیاه، کلاه

[1]- IT =Information communication Technology

خاکستری کلاه صورتی و نفوذ گران جوان است. نفوذ گران معمولاً سامانه‌هایی را شکار می‌کنند که اقدامات احتیاطی پایه را (مثل محصولاتی که نام کاربری و گذرواژه در آن‌ها به‌طور پیش‌فرض است و اغلب کاربران فراموش می‌کنند، آن را تغییر دهند) نادیده گرفته‌اند.(جعفری لاری،۱۳۹۴:۳۳)

- هکرهای مهاجم طراحانی هستند که روش‌های نفوذ را ابداع و به کار می‌گیرند تا بتوانند در سیستم‌ها، سرورها و سایت‌ها نفوذ کرده و عملیات خود را به اجرا گذارند. (شهلایی،۱۳۹۳: ۶۸-۶۶)
- مهاجمان هدف‌دار مهاجمان خبره‌ای‌اند که هدفشان سرقت اطلاعات، تخریب و از بین بردن داده‌ها، از کار انداختن سرویس‌ها و سامانه‌ها در خلال یک بازه زمانی است.
- اشتباه کارمندان و مشاوران و بی‌توجهی عمدی آن‌ها (مخاطرات ناشی از سهل‌انگاری نیروی انسانی) می‌تواند تهدیدی جدی برای سامانه‌ها ایجاد کند.
- اسب تروآ (تروجان‌ها) برنامه‌هایی که به نظر مفید و کاربردی هستند؛ اما در عمل کدهایی هستند که باعث ایجاد باز شدن درگاه‌های نرم‌افزاری شده و نفوذ گر از همان درگاه‌ها استفاده نموده و وارد سیستم می‌گردد.
- درهای پشتی: در پشتی، برنامه‌ای است که امکان دستیابی به یک سیستم را بدون بررسی و کنترل امنیتی، فراهم می‌کند. (ابولحسینی، ۱۳۹۲: ۳۷ و ۱۱۲)

**جدول (۱) آسیب‌پذیری‌های رایانه‌ای (شهلایی،۱۳۹۳:۵۲)**

| آسیب‌پذیری | توضیحات |
|---|---|
| نرم‌افزار | برنامه‌های کاربردی و یا نرم‌افزارهای سیستمی و سیستم‌عامل ممکن است به علت نقص در طراحی دارای نقاط ضعفی باشد که به‌صورت تصادفی و یا عمدی ایجادشده است. |
| سخت‌افزار | آسیب‌پذیری می‌تواند در سخت‌افزار یافت شود، ازجمله ریزپردازنده، میکرو کنترل‌ها، پانل‌های مدار، منابع تغذیه، لوازم جانبی مانند چاپگر، دستگاه‌های ذخیره‌سازی، تجهیزات و ارتباطات (کارت‌های شبکه) باشد. |
| نقاط ضعف رایانه‌ای | یک مثال از چنین حفره‌ای ممکن است برنامه‌ریزی حافظه فقط خواندنی از یک کامپیوتر (سیستم‌عامل) که می‌تواند به‌طور نادرست و مخفیانه انجام شود. |
| کانال‌های ارتباطات | کانال‌های ارتباطات بین یک سیستم یا شبکه و خارج از شبکه می‌تواند توسط دشمن به‌عنوان یک کاربر مجاز در شبکه معرفی نموده و ضمن انکار دسترسی خودی به شبکه اقدام به اقدامات خرابکارانه بپردازد. |

| | |
|---|---|
| پیکربندی | همه سامانه‌ها که بر اساس کاربردی بودن آن‌ها پیکربندی می‌شوند. این پیکربندی بر اساس امنیت و یا دسترسی آسان به سایر منابع تنظیم‌شده و ازآنجاکه اکثر کاربران راحتی کار را بر امنیت مقدم می‌سازند می‌تواند به‌عنوان یک پیکربندی غلط باعث ایجاد ناامنی‌های خطرناکی گردد. |
| کاربران و اپراتورها | کاربران را می‌توان از راه‌هایی تهدید، رشوه و یا فریب و انجام خریدهایی در فضای مجازی از کار اصلی خود جدا کرده و از همین راه نفوذ را انجام داد. |
| ارائه‌دهندگان خدمات | بسیاری از تأسیسات کامپیوتر به طرف‌های خارجی جهت ارائه خدمات تعمیر و نگهداری و اینترنتی تکیه می‌کنند و دشمن ممکن است قادر به متقاعد کردن ارائه‌دهندگان خدمات به اقدامات ویژه‌ای از طرف آن‌ها شود. |

**تهدیدات تروریسم سایبر**

تروریسم سایبری عبارت است از حمله‌ای باانگیزه سیاسی و از پیش برنامه‌ریزی‌شده در برابر اطلاعات، سیستم‌های کامپیوتری، برنامه‌های کامپیوتری و داده‌هایی که منجر به خشونت علیه اهداف توسط زیرگروه‌های ملی یا مأموران مخفی و یا گروه‌های تروریستی است (جعفری لاری،۱۳۹۴: ۷۲) فعالیت‌های نظامی سایبری نیز شامل عملیات متمرکز بر شبکه، حملات شبکه رایانه‌ای و بهره‌برداری از آن، عملیات نفوذ ژئوپلیتیکی و امنیتی خواهد بود. با توجه به اینکه تهدید پایه در جمهوری اسلامی ایران، کشور آمریکا است و از طرفی به دلیل توانمندی آمریکا در دانش و فناوری اطلاعات و ارتباطات و صاحب فنّاوری بودن آن‌ها در این موضوع و استفاده از نرم‌افزارها و تجهیزات شبکه آمریکایی مانند سوییچ‌های سیسکو و به‌تبع آن‌ها آسیب‌پذیری شبکه‌های ارتباطی و رایانه‌ای کشور و همچنین سرمایه‌گذاری آمریکا بر روی جنگ سایبری بنابراین تهدید اصلی و پایه سایبری در شبکه ارتباطات زیرساختی ایران، کشور آمریکا است لذا؛ در فضای سایبر همه‌چیز ناامن است و امنیت نسبی را با تمهیدات و ملاحظات امنیتی و پدافندی باید ایجاد و به‌صورت دائم آن‌ها به‌روز نمود و با جدیت باید مراقب این تغییر حالت بود تا فرصت‌ها به تهدید نگردد و با شناخت تهدیدات سایبری مربوطه و تعیین آسیب‌پذیری‌های خود، می‌بایست راه‌کارهای پدافندی را برای حفاظت از آن‌ها بکار بست. (خواجوی و جلالی فراهانی، ۱۳۹۰: ۱۱۷)

**جدول (۲) منابع تهدید و روش‌های حملات سایبری و جدول آسیب‌پذیری‌های کامپیوتری (جلالی فراهانی و همکاران،۵۸:۱۳۹۵)**

| منبع تهدید | توصیف تهدید |
|---|---|
| هکرها | هکرها گاهی اوقات برای اظهار وجود خود وارد شبکه می‌شوند. در شرایط فعلی نفوذ به شبکه‌ها با حداقل دانش و مهارت امکان‌پذیر است به این طریق که آن‌ها برنامه‌های لازم را از اینترنت دریافت نموده و همان‌ها را علیه سایت‌های دیگر به کار می‌برند. |
| عوامل ناراضی داخلی | عوامل ناراضی داخلی که در درون سازمان فعالیت می‌کنند منبع اصلی جرائم رایانه‌ای هستند و این دسته از عوامل لازم نیست دانش قابل‌توجهی در خصوص تهاجم رایانه‌ای داشته باشند زیرا اطلاع آن‌ها از سیستم مورد هدف غالباً امکان دسترسی نامحدود برای واردکردن ضربه به سامانه‌ها و یا سرقت اطلاعات سازمان را فراهم می‌سازد. تهدید عوامل داخلی شامل کارکنان پیمانکاران نیز می‌شود. |
| تروریست‌ها | تروریست‌ها به دنبال تخریب، ناتوان‌سازی و یا بهره‌برداری بدخواهانه از زیرساخت‌های حیاتی به‌منظور تهدید کردن امنیت ملی، وارد آوردن خسارات سنگین، تضعیف اقتصاد کشور و تخریب روحیه و اعتماد عمومی می‌باشند. |

**امنیت شبکه**

شبکه‌های ارتباطی زیرساخت لازم برای عرضه اطلاعات در یک سازمان را فراهم می‌نمایند. جایگاه امنیت در شبکه کامپیوتری و ارتباطی یکی از مسائل مهم در دنیای امروز است. مدت‌ها است که استفاده گسترده از کامپیوتر در ارتش و تأسیسات دفاعی، به‌کارگیری قوانین و آیین‌نامه‌های ویژه‌ای را برای حفظ امنیت در سیستم‌های فضای سایبر ضروری ساخته است. یک اصل اساسی در زمینه امنیت دستگاه‌های کامپیوتری، قرار دادن کل سیستم در محیطی است که نفوذپذیری در آن تا حد قابل قبولی کاهش‌یافته باشد.(دهستانی،۱۳۹۱: ۱۲۰) اگر ما بهترین سیستم سخت‌افزاری و یا سیستم‌عامل را به خدمت بگیریم ولی کاربران و یا عوامل انسانی درگیر در یک سیستم کامپیوتری، پارامترهای امنیتی را رعایت ننمایند، کاری را از پیش نخواهیم برد. مدیران سازمان و کاربران معمولی جملگی عوامل انسانی در یک سازمان می‌باشند که حرکت و یا حرکات اشتباه هر یک می‌تواند پیامدهای منفی در ارتباط با امنیت اطلاعات را به دنبال داشته باشد. (ابولحسینی،۱۳۹۲: ۴۶)

**امنیت فیزیکی و ساختمانی شبکه**

در ابتدا ساختمان سایت‌های سخت‌افزاری و نرم‌افزاری، مراکز داده و مراکز کنترل شبکه‌ها، باید در مقابل حوادث طبیعی، جرائم، نزدیکی به پروژه‌های ساختمانی ایمن گردند. به همین خاطر در طراحی و ساخت مکان و مشخصات ساختمانی محیط‌های رایانه‌ای باید موارد زیر مدنظر قرار گیرد.

۱. محیط سایت‌های کامپیوتری باید در مکانی باشد که ریسک ناشی از بلایای طبیعی (حریق، رعدوبرق، طوفان، زمین‌لرزه و سیل) به میزان قابل قبولی باشد و در برابر این بلایا و حملات نظامی، الکترومغناطیسی و ... مقاوم باشند.

۲. بهتر است سایت پشتیبان در مرکز شهر نباشد و دور از حوادث انسان‌ساخت مانند انفجار و آتش‌سوزی باشد.

۳. مراکز داده و کنترل شبکه‌ها نباید با تابلو مشخص شود به‌گونه‌ای که هر رهگذری به‌سادگی از محل آن مطلع شود.

۴. محل مراکز داده از مرکز فرماندهی حدوداً بیست مایل و محل آن از جاده اصلی حدود صد فوت فاصله داشته باشد.

۵. هرچه نقاط ورودی ساختمان کمتر باشد کنترل دسترسی بهتر امکان‌پذیر است.

۶. نزدیک‌ترین فاصله به مراکز مخابراتی و امکان برخورداری از اتصال به دو شبکه برق مستقل و متفاوت، ارتباطات حداقل دو منطقه مخابراتی مستقل و متفاوت.(مدیری و شاه ولایتی،۱۳۹۰: ۱۳۷)

- دفاع از شبکه‌های کامپیوتری: دفاع از شبکه‌های کامپیوتری که شامل تمام اقدامات لازم برای محافظت از سیستم‌های خود و زیرساخت در برابر حملات مخفیانه و یا آشکار دشمن به کامپیوتر و شبکه خودی است.(شهلایی،۱۳۹۳: ۴۶) مهم‌ترین روش‌های دفاع از شبکه‌های کامپیوتری عبارت‌اند از: ضد بدافزار، دیواره آتش، ضد تروجان، تشخیص تهاجم، مانع از هجوم، رمز کننده، شبکه مجازی خصوصی، منحرف‌کننده مهاجم، تشخیص هویت، حفاظت فیزیکی (ابولحسینی، ۱۳۹۲: ۴۶)
- پدافند غیرعامل در شبکه‌های کامپیوتری: منظور از پدافند غیرعامل در محیط‌های فناوری اطلاعات، مجموعه تمهیدات، اقدامات و طرح‌هایی است که با استفاده از ابزار، شرایط و حتی‌المقدور بدون نیاز به نیروی انسانی به‌صورت خوداتکا، موجب کاهش آسیب‌پذیری در برابر حملات و اعمال برنامه‌ریزی‌شده و هدفمند علیه رایانه‌ها، برنامه‌ها و اطلاعات ذخیره‌شده در درون آن‌ها می‌گردد. (مدیری و شاه ولایتی، ۱۳۹۰: ۲۵۰)

- دفاع سایبر: دفاع سایبری به فعالیت‌هایی اشاره دارد که از سوی یک‌طرف برای محافظت از منافع خود در برابر یک حمله، صورت می‌گیرد و به همین علت وجود نسخه پشتیبان داده‌ها در زمان بازیابی فایل‌هایی که خراب‌شده‌اند بسیار ضروری است. (کرامر و همکاران، ۱۳۹۴: ۳۸)

## پیشینه‌های پژوهش

**جدول (۳) پایان‌نامه‌های مرتبط با موضوع تحقیق**

| موضوع تحقیق | **ارتقا کارایی سامانه آماد مکانیزه برای پاسخگویی به عملیات آمادی آینده نهاجا.** |
|---|---|
| محقق | علی صفر رضوی زاده |
| آدرس | پایان‌نامه دافوس، دوره ۲۱ |
| نتایج تحقیق | امروزه داشتن سیستم اطلاعاتی برای هر سازمان بسیار ضروری است و با توجه به تنوع زیاد اقلام در نهاجا طراحی سیستم‌های اطلاعاتی از اهمیت بسیار بالایی برخوردار است. از طرفی در عملیات جنگی، این سامانه آمادوپشتیبانی است که باعث تداوم مأموریت و توازن رزمی یگان می‌شود و باگذشت سنوات طولانی و پیچیدگی فن‌آوری جدید و تفاوت جنگ‌های آینده نیاز به ارتقاء این سامانه کاملاً محسوس است. در حال حاضر این سامانه به دلیل هزینه‌های بالا مطابق فناوری روز نیست و کارها با کندی انجام می‌گیرد. |
| موضوع تحقیق | فنون پدافند غیرعامل آجا در دفاع سایبری در برابر تهدیدات فرا منطقه‌ای |
| محقق | داود آذر |
| آدرس | پایان‌نامه دافوس، دوره ۷ |
| نتایج تحقیق | عضویت غیرارادی سرورها و رایانه‌های کشور در گروه‌های هکری و سربازگیری الکترونیکی موسوم به بات نت یکی از آسیب‌های ناخواسته مراکز رایانه‌ای آجا است و یکی از روش‌های اولیه حملات سایبری نفوذ ویروس‌ها و هکرها بوده و این مراکز امروز نمی‌توانند با همان فنون و تجهیزات غیربومی قدیمی با این حملات مبارزه کنند. لذا به افراد کارآزموده و صلاحیت‌دار نیاز بوده و تمام تعاملات کاربران را می‌توان با مکانیسمی مانند کنترل دسترسی تحت کنترل و نظارت قرار داد. |
| موضوع تحقیق | چالش‌های امنیتی شبکه‌های رایانه‌ای به‌منظور مقابله با آسیب‌پذیری‌های مربوطه |

| | |
|---|---|
| محقق | منوچهر اسکندری |
| آدرس | پایان‌نامه دافوس، دوره ۴ |
| نتایج تحقیق | تعدادی از روش‌های نفوذ و اختلال در سرویس‌دهی تجهیزات فیزیکی ارتباطی شبکه ساحفاجا که به آن‌ها پرداخته‌شده است عبارت‌اند از: استراق سمع از هاب و سوییچ، از کار انداختن سویچ و گمراه کردن تجهیزات و همچنین دسترسی فیزیکی به تجهیزات و تغییر پیکربندی آن‌ها. لذا باید با به‌کارگیری تجهیزات امنیتی مناسب در شبکه مانند مانیتورینگ و دیوار آتش بومی و تائید شده و نصب و راه‌اندازی نرم‌افزار تشخیص نفوذ، تهیه پشتیبان دوره‌ای و منظم از اطلاعات و نگهداری آن‌ها دور از محل سرویس‌دهنده‌ها، مراتب تأمین فیزیکی و تجهیزات ارتباطی و جلوگیری از اختلال در سرویس‌دهی آن‌ها فراهم آید. |

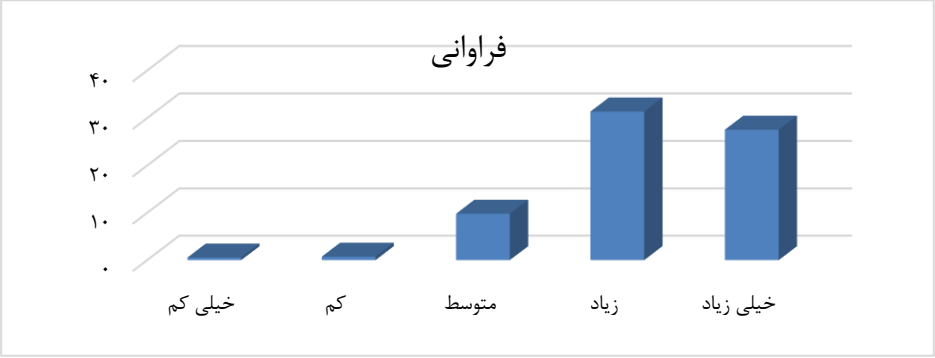
## روش‌شناسی پژوهش

ازآنجاکه هدف این تحقیق تبیین آسیب‌پذیری سامانه مکانیزه لجستیک نهاجا در برابر تهدیدهای آینده و ارائه راهکارهای مناسب و یافتن پاسخی برای سؤالات مطرح‌شده است، انتظار می‌رود تا نتایج آن برای ارائه راه‌کارهای مناسب به کار گرفته‌شده و باعث کاهش آسیب‌پذیری‌های سامانه شود، لذا دارای سودمندی عملی بوده و تحقیقی کاربردی است و محقق با استفاده از مطالعه اسناد، مدارک، کتب و مقاله‌های علمی و پژوهشی و سؤال‌های مصاحبه اطلاعات کیفی را جمع-آوری نموده و به‌صورت کیفی تحلیل (تحلیل محتوا) نموده و با جمع‌آوری اطلاعات کمی، این اطلاعات را به‌صورت کمی تحلیل و در پایان به‌صورت آمیخته مورد تحلیل قرار داده است، به همین خاطر رویکرد این تحقیق آمیخته (کمی و کیفی) است. جامعه آماری به‌صورت تمام شمار بوده، جامعه نمونه بر جامعه آماری منطبق است و شامل ۷۰ نفر از کارشناسان و مدیران معاونت-های عملیات، آمادوپشتیبانی، فاوا نهاجا، فرماندهی آمادوپشتیبانی هوایی، دانشگاه هوایی و فرماندهی مرکز آموزش‌های هوایی شهید خضرایی که حداقل دارای ۱۵ سال سابقه خدمت، مدرک کارشناسی و بالاتر و آگاه به موضوع طی سال‌های ۱۳۹۷-۱۳۹۶ در سطح ستاد نهاجا و شهر تهران است. محقق ابتدا به مطالعه اسناد و مدارک موجود پرداخته که به‌منظور تکمیل اطلاعات کتابخانه‌ای با انجام مصاحبه با صاحب‌نظران حوزه‌های آمادوپشتیبانی، فناوری اطلاعات و ارتباطات و پدافند غیرعامل، نسبت به استخراج شاخص‌های متغیرهای موضوع تحقیق و تنظیم پرسش‌نامه اقدام نموده، با تقسیم آن در جامعه نمونه، نتایج را جمع‌آوری و با استفاده از آمار توصیفی و استنباطی داده‌های به‌دست‌آمده را تجزیه‌وتحلیل و در آخر، آسیب‌پذیری‌های فناورانه سامانه مکانیزه لجستیک را احصا و راه‌کارهای مناسب برای کاهش هرکدام از آسیب‌پذیری‌ها را ارائه کرده است.

### روایی و پایایی ابزار گردآوری اطلاعات

پایایی پرسشنامه‌ها از طریق اجرای آزمون اعتبار سنجی توسط نرم‌افزار spss و سنجش ضریب آلفای کرونباخ ارزیابی گردید. ضریب پایایی شاخص‌های پرسشنامه ۰/۸۵۸(برای متغیر اول ۸۵۹/. متغیر دوم ۸۵۸/؛ و متغیر سوم ۸۵۷/.) که نشان از دقت بالای ابزار اندازه‌گیری مورداستفاده در این تحقیق دارد. در تهیه پرسشنامه از شاخص‌های حملات سایبری، عدم پیش‌بینی شبکه ارتباطی رادیوئی تاکتیکی، عدم نصب تجهیزات امنیتی در برابر حملات سایبری (دیواره آتش)، اتصال به ایستگاه‌های کاری غیرمجاز (تلفن همراه، تبلت و لپ‌تاپ)، عدم رعایت دستورالعمل‌های امنیتی کار با رایانه و داشتن دسترسی غیرمجاز کارکنان، عدم برگزاری همایش‌ها و جلسات آگاه‌سازی امنیت اطلاعات برای کاربران، (عدم تحرک، پراکندگی و توزیع مناسب)، نفوذ گران، حمله هکرها و برنامه‌های مخرب، عدم رعایت مسائل ایمنی (امنیت فیزیکی) در تجهیزات سرور مرکزی، نداشتن سایت پشتیبان (نرم‌افزاری، سخت‌افزاری و اطلاعاتی) استفاده‌شده و مورد تائید کارشناسان و صاحب‌نظران استفاده گردید تا روایی پرسشنامه تأمین گردد. پرسشنامه تهیه‌شده ابتدا به صاحب‌نظران، اساتید محترم راهنما و مشاور ارائه و تصحیح لازم در آن انجام گردید تا روایی آن مورد تائید قرار گیرد.

### تجزیه‌وتحلیل داده‌ها




**نمودار (۱) توزیع فراوانی**

با توجه به نمودار بالا، در رابطه با آسیب‌پذیری‌های فناورانه سامانه مکانیزه لجستیک نهاجا، نتایج حاصله مبین این مطلب است که از تعداد ۷۰ نفر پاسخ‌دهندگان (حجم نمونه) تعداد ۲۸ نفر (۳۹٪) گزینه خیلی زیاد، تعداد ۳۱ نفر (۴۴٪) گزینه زیاد، تعداد ۱۰ نفر (۱۴٪) گزینه متوسط، تعداد ۱ نفر (۱٪) گزینه کم و تعداد ۱ نفر (کمتر از ۱٪) گزینه خیلی کم را انتخاب نموده‌اند.

**جدول (۴) نظرات جامعه آماری در خصوص آسیب‌پذیری‌های فناورانه سامانه مکانیزه لجستیک نهاجا**

| ابعاد | مؤلفه‌ها | خیلی کم | کم | متوسط | زیاد | خیلی زیاد |
|---|---|---|---|---|---|---|
| شبکه ارتباطی | ۱. استفاده از شبکه‌های زیرساخت مخابرات و امکان ایجاد اخلال و نفوذ خرابکاران | ۰ | ۲ | ۱۰ | ۲۶ | ۳۲ |
| | ۲. نداشتن شبکه ارتباطی موازی، امن و پایدار | ۱ | ۰ | ۳ | ۳۰ | ۳۶ |
| | ۳. عدم پیش‌بینی شبکه ارتباطی رادیوئی تاکتیکی (سیار) | ۰ | ۰ | ۵ | ۴۱ | ۲۴ |
| | ۴. عدم نصب تجهیزات امنیتی در برابر حملات سایبری | ۲ | ۱ | ۱۰ | ۳۰ | ۲۷ |
| ایستگاه کاری (NODE) | ۵. اتصال به ایستگاه‌های کاری غیرمجاز | ۱ | ۱ | ۱۰ | ۲۴ | ۳۴ |
| | ۶. عدم رعایت دستورالعمل‌های امنیتی کار با رایانه و داشتن دسترسی غیرمجاز کارکنان | ۰ | ۰ | ۹ | ۳۴ | ۲۷ |
| | ۷. عدم برگزاری جلسات آگاه‌سازی امنیت اطلاعات برای کاربران | ۰ | ۱ | ۱۷ | ۳۶ | ۱۶ |
| سرویس‌دهنده مرکزی (SERVER) | ۸. تمرکزی بودن سرویس‌دهنده مرکزی (عدم تحرک و پراکندگی) | ۰ | ۱ | ۱۷ | ۳۰ | ۲۲ |
| | ۹. نفوذ گران، حمله هکرها و برنامه‌های مخرب | ۲ | ۲ | ۱۲ | ۳۵ | ۱۹ |
| | ۱۰. عدم رعایت مسائل امنیت فیزیکی در تجهیزات سرور مرکزی | ۰ | ۰ | ۱۱ | ۳۲ | ۲۷ |
| | ۱۱. نداشتن سایت پشتیبان | ۰ | ۰ | ۴ | ۲۷ | ۳۹ |
| | ۱۲. عدم تجهیز ساختمان به سپر الکترومغناطیسی | ۰ | ۰ | ۱۱ | ۲۲ | ۳۷ |
| | ۱۳. تمرکز کارکنان متخصص سامانه در یک ساختمان | ۰ | ۱ | ۸ | ۳۶ | ۲۵ |
| | ۱۴. عدم مقاوم‌سازی اماکن و تأسیسات سامانه | ۰ | ۰ | ۴ | ۳۳ | ۳۳ |
| | ۱۵. عدم پراکندگی (توزیع) مناسب تأسیسات سامانه | ۰ | ۰ | ۱۲ | ۴۲ | ۱۶ |
| | میانگین | .۵۵ | .۷۳ | ۸۲.۹ | ۳۶.۳۱ | ۵۵.۲۷ |

## تجزیه‌وتحلیل یافته‌های پژوهش

**جدول (۵) آسیب‌پذیری‌های فناورانه سامانه مکانیزه لجستیک نهاجا ازنظر خبرگان پژوهش**

| | |
|---|---|
| عدم پایداری شبکه ارتباطی سامانه و قطع شدن مکرر شبکه ارتباطی گردان‌های آماد و فاوا در پایگاه‌های هوایی (به دلیل تکمیل نبودن فیبر نوری) و دوگانه یا چندگانه نبودن مسیر زیرساخت شبکه | مصاحبه‌شونده چهارم |
| ضعف در ایستگاه‌های کاری و سرویس‌دهنده مرکزی رایانه مرکزی، ایستگاه‌های کاری و شبکه ارتباطی، سیستم‌عامل، بانک اطلاعاتی، محیط برنامه‌نویسی | مصاحبه‌شونده دوم |
| نداشتن سامانه‌های پشتیبان از بعد سخت‌افزاری و نرم‌افزاری (بانک اطلاعاتی و محیط اجرایی نرم‌افزار) | مصاحبه‌شونده ششم |
| دست‌کاری و اختلال در برنامه‌های نرم‌افزاری توسط افراد نفوذی | مصاحبه‌شونده اول |
| عدم تجهیز سامانه در برابر تهدیدات سایبری، بمب‌های الکترومغناطیسی و بمب‌های گرافیتی | مصاحبه‌شونده چهارم |
| نفوذ ویروس‌ها از طریق نرم‌افزار و بدافزارهای موجود و همچنین تجهیزات همراه و ایستگاه‌های کاری | مصاحبه‌شونده پنجم |
| عدم برگزاری جلسات آگاه‌سازی امنیت اطلاعات برای کارکنان و عدم رعایت دستورالعمل‌های امنیتی کار با رایانه | مصاحبه‌شونده چهارم |
| خرابکاری در برنامه‌ها و وارد نمودن داده‌های اشتباه در سامانه | مصاحبه‌شونده سوم |
| عدم اتصال انبارها به شبکه و سامانه آمادفنی و دستی بودن روش‌های آمادی، حسابداری انبار و عدم استفاده از فنّاوری جدید بارکد خوان در انبارگردانی و دریافت و واگذاری اقلام و تجهیزات | مصاحبه‌شونده چهارم |

با کمک اطلاعات جمع‌آوری‌شده از مصاحبه با صاحب‌نظران، مطالعه اسناد و مدارک و پرسش‌نامه، اهم نظرات مصاحبه‌شوندگان در خصوص آسیب‌پذیری‌های فناورانه سامانه آمادفنی نهاجا در برابر تهدیدهای آینده عبار تند از عدم پایداری شبکه ارتباطی و ضعف در ایستگاه‌های کاری و سرویس-دهنده مرکزی؛ آسیب‌پذیری نرم‌افزاری و سخت‌افزاری و کاربری و امکان نفوذ در اطلاعات موجودی کلی قطعات و ایجاد اخلال در تأمین اقلام و اخلال در شبکه‌های ارتباطی، قطع مکرر شبکه ارتباطی با پایگاه‌ها، انجام امور آمادی (حسابداری و انبارداری) به روش دستی، فریب و جعل و اختلال زا طریق آسیب‌پذیری‌های سایبری و وارد آمدن خسارت به دلیل تسلیحات الکترومغناطیسی و بمب‌های گرافیتی (پودری و رشته‌ای) دشمن و نداشتن سامانه پشتیبان. بر اساس مطالعه اسناد و مدارک، هر فن‌آوری رایانه‌ای ذاتاً آسیب‌پذیری‌هایی دارد که می‌تواند مورد بهره‌برداری مخالفان قرار گیرد. به همین دلیل تمام فعالیت‌های آگاه امنیتی از یکسری اقدامات

متقابل استفاده می‌کنند تا این آسیب‌ها را به حداقل برسانند. برخی علل آسیب‌پذیری شبکه عبارت‌اند از ضعف دانش کاربران، ضعف فناوری و وابستگی فناوری به شرکت‌های خارجی، ضعف در فناوری امنیت شبکه، دفاع از شبکه و ردیابی نفوذ گران و ضعف مدیریت.

انواع حملات و تهدیدات در حوزه فن‌آوری اطلاعات شامل حملات تخریب سرویس و حمله از طریق برنامه مخرب (تهدیدات نرم) است. تهدیدات نرم را می‌توان با دو معیار اساسی از تهدیدات سخت بازشناخت. اولین معیار غیر خشونت‌آمیز بودن روش تهدید و معیار دوم، نرم‌افزاری بودن پیامد تهدید است. با توجه به معیارهای دوگانه تهدیدات نرم، این نوع تهدیدات را می‌توان به چند دسته اصلی تقسیم کرد: دسته اول تهدیدات نرم دارای روش خشونت‌آمیز، اما با پیامدهای نرم‌افزاری یا غیر خشونت‌آمیز و دسته دوم تهدیداتی که روش آن غیر خشونت‌آمیز، اما پیامدهایش خشونت‌آمیز است؛ مانند استفاده از کرم‌ها و بمب‌های منطقی که سیستم کنترل و فرمان یا ناوبری هواپیماها را از کار می‌اندازد. دسته سوم تهدیداتی است که روش و پیامدهای آن غیر خشونت‌آمیز است؛ مانند استفاده از انواع سلاح‌های سایبری به‌عنوان یک قطع کننده ارتباطی بین نیروها. مهم‌ترین روش‌ها برای دفاع از تهدیدات سایبری شامل استفاده از ضد بدافزار، دیواره آتش، ضد تروجان، تشخیص تهاجم، مانع از هجوم، رمز کننده، شبکه مجازی خصوصی، منحرف‌کننده مهاجم، تشخیص هویت، حفاظت فیزیکی است. دسته چهارم تهدیدات عمدی هستند که از خرابی خودسر یا دست‌کاری تعمدی نرم‌افزار یا سخت‌افزار، ناشی می‌شوند و منابع پتانسیل این تهدیدات، شامل کارکنان ناراضی، پیمان‌کاران، مشاوران، نفوذ گران، مشتریان، کارپردازان، کلاه‌برداران و مجرمان می‌شود. روش‌های حمله که در تهدیدات شبکه‌ای کاربرد دارد نیز عبارت‌اند از: ویروس، کرم، جاسوس‌افزار، اسب تروآ، بمب‌ها، در پشتی و نامه‌های الکترونیکی ناخواسته.

با توجه به اینکه امروزه امنیت اطلاعات به‌عنوان یکی از مسائل مهم مطرح است. دفاع از شبکه‌های کامپیوتری نیز شامل اقدامات لازم برای محافظت از سیستم‌های خود و زیرساخت در برابر حملات مخفیانه و یا آشکار دشمن به شبکه کامپیوتری خودی است. پدافند شبکه رایانه‌ای عبارت است از اقدام‌های پدافندی به‌منظور حفاظت و دفاع از اطلاعات، رایانه‌ها و شبکه‌ها در برابر اختلال، عدم دسترسی، افت کیفیت یا تخریب که شامل مجموعه تمهیدات و طرح‌هایی است که با استفاده از ابزار، شرایط و حتی‌المقدور بدون نیاز به نیروی انسانی به‌صورت خوداتکا، موجب کاهش آسیب‌پذیری در برابر حملات و اعمال برنامه‌ریزی‌شده و هدفمند علیه رایانه‌ها، برنامه‌ها و اطلاعات ذخیره‌شده در درون آن‌ها می‌گردد مانند دیوارهای آتش، سیستم‌های تشخیص مزاحمت و نرم‌افزار ضدویروس. در پدافند شبکه‌ی رایانه‌ای با استفاده از اقدامات امنیتی در شبکه‌های رایانه‌ای

اجازه داده نمی‌شود که دشمن درباره توانمندی‌ها و مقاصد نظامی نیروهای خودی به اطلاعات ارزشمند دست یابد.

**جدول (۶) آسیب‌پذیری‌های سامانه مکانیزه لجستیک نهاجا با توجه به اسناد و مدارک**

| | |
|---|---|
| خطاهای انسانی | شامل ضعف مدیریت، دانش کاربران سامانه و نادیده گرفتن اقدامات احتیاطی پایه (جعفری لاری،۱۳۹۴:۳۳) |
| نرم‌افزار | برنامه‌های کاربردی و یا نرم‌افزارهای سیستمی و سیستم‌عامل که به‌صورت تصادفی و یا عمدی ضعیف ایجاد شده لذا می‌تواند یک حفره امنیتی برای نفوذ و خرابکاری باشد. (شهلایی،۱۳۹۳:۵۲) |
| سخت‌افزار | ازجمله ریزپردازنده، میکرو کنترل‌ها، پانل‌های مدار، منابع تغذیه، لوازم جانبی مانند چاپگر یا اسکنر، دستگاه‌های ذخیره‌سازی که با دست‌کاری آن‌ها ممکن است قابلیت‌های در نظر گرفته‌شده از اجزا تغییر و یا فراهم نمودن فرصت برای انتقال نرم‌افزارهای مخرب به سیستم باشد. (شهلایی،۱۳۹۳:۵۲) |
| ارائه‌دهندگان خدمات | بسیاری از تأسیسات کامپیوتر به طرف‌های خارجی جهت ارائه خدمات تکیه می‌کنند و غافل از اقدامات ویژه دشمن در نفوذ به ارائه‌دهندگان خدمات هستند. (شهلایی،۱۳۹۳:۵۲) |
| فعالیت‌های نفوذ سایبری | مانند اینترنت، رادیو، تلویزیون، وسایل ارتباطی همچون تلفن‌های همراه (خواجوی،۱۳۹۰:۱۱۷) |

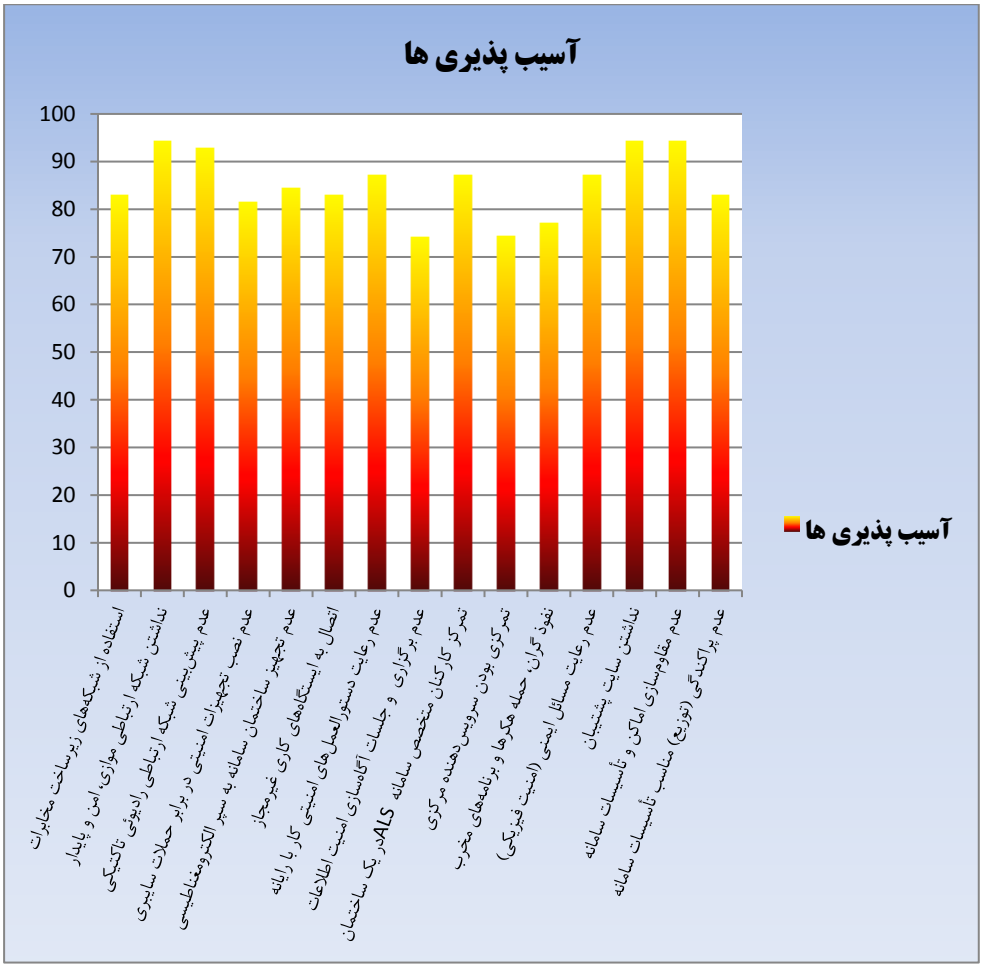
## نتیجه‌گیری

علی صفر رضوی زاده به این نتیجه می‌رسد امروزه داشتن سیستم اطلاعاتی برای هر سازمان بسیار ضروری است و با توجه به تنوع زیاد اقلام در نهاجا طراحی سیستم‌های اطلاعاتی از اهمیت بسیار بالایی برخوردار است و باگذشت سنوات طولانی و پیچیدگی فن‌آوری جدید و تفاوت جنگ‌های آینده نیاز به ارتقاء این سامانه کاملاً محسوس است.

منوچهر اسکندری در پایان‌نامه خود به این نتیجه می‌رسد که تعدادی از روش‌های نفوذ و اختلال در سرویس‌دهی تجهیزات فیزیکی ارتباطی شبکه‌های ارتباطی عبارت‌اند از استراق سمع از هاب و سوییچ، از کار انداختن سوییچ و گمراه کردن تجهیزات و همچنین دسترسی فیزیکی به تجهیزات و تغییر پیکربندی آن‌ها و با به‌کارگیری تجهیزات امنیتی مناسب در شبکه مانند مانیتورینگ و دیوار آتش بومی و تائید شده و نصب و راه‌اندازی نرم‌افزار تشخیص نفوذ، تهیه پشتیبان دوره‌ای و منظم از اطلاعات و نگهداری آن‌ها دور از محل سرویس‌دهنده‌ها فراهم می‌آید.

سامانه‌های رایانه‌ای ذاتاً آسیب‌پذیری‌هایی دارد که می‌تواند مورد بهره‌برداری مخالفان قرار گیرد. عمده آسیب‌پذیری‌های فناوری اطلاعات در برابر تهدیدات نرم است. روش‌های حمله در تهدیدات شبکه‌ای عبارت‌اند از: ویروس، کرم، جاسوس‌افزار، اسب تروآ، بمب‌ها، در پشتی، نامه‌های الکترونیکی ناخواسته و کدهای مخرب. با توجه به امکان نفوذ در اطلاعات موجودی کلی قطعات

و ایجاد اخلال در تأمین اقلام و اخلال در شبکه‌های ارتباطی، قطع مکرر شبکه ارتباطی با پایگاه‌ها (به دلیل تکمیل نبودن فیبر نوری)، در صورت بروز تهدیدات در آینده، رایانه مرکزی، ایستگاه‌های کاری و شبکه ارتباطی، سیستم‌عامل، بانک اطلاعاتی، محیط برنامه‌نویسی و محیط اجرایی برنامه‌ها و نیز ساختار ارتباطی سامانه مکانیزه لجستیک نهاجا همگی با مشکل مواجه شده و باید سامانه پشتیبان هر یک وجود داشته باشد. لذا ازجمله آسیب‌پذیری‌های فناورانه سامانه مکانیزه لجستیک نهاجا که از پرسشنامه استخراج گردیده عبارت‌اند از: استفاده از شبکه‌های زیرساخت مخابرات و امکان ایجاد اخلال و نفوذ خرابکاران به سامانه، نداشتن شبکه ارتباطی موازی، امن و پایدار در برابر حملات سایبری، عدم پیش‌بینی شبکه ارتباطی رادیوئی تاکتیکی (سیار) در سامانه، عدم نصب تجهیزات امنیتی در برابر حملات سایبری (دیواره آتش) در سامانه، عدم رعایت مسائل ایمنی (امنیت فیزیکی) در سرور مرکزی سامانه، نداشتن سایت پشتیبان (نرم‌افزاری، سخت‌افزاری و اطلاعاتی) برای سامانه، عدم تجهیز ساختمان به سپر الکترومغناطیسی در برابر بمب‌های الکترومغناطیسی و گرافیتی، تمرکزی بودن سرویس‌دهنده مرکزی (عدم تحرک و توزیع مناسب) سامانه، نفوذ گران، حمله هکرها و برنامه‌های مخرب، به سرویس‌دهنده مرکزی سامانه، عدم رعایت دستورالعمل‌های امنیتی کار با رایانه و داشتن دسترسی غیرمجاز کارکنان به سامانه، اتصال سامانه به ایستگاه‌های کاری غیرمجاز (گوشی تلفن همراه، تب لت و لپ تاب)، تمرکز کارکنان متخصص سامانه در یک ساختمان در زمان تهدیدهای موشکی، عدم برگزاری همایش‌ها و جلسات آگاه‌سازی امنیت اطلاعات برای کاربران، نداشتن سایت پشتیبان، عدم مقاوم‌سازی ساختمان و اماکن تأسیسات سامانه در برابر بلایای طبیعی و انسان‌ساخت. دفاع از شبکه‌های کامپیوتری که شامل تمام اقدامات لازم برای محافظت از سیستم‌ها و زیرساخت در برابر حملات مخفیانه و یا آشکار دشمن به کامپیوتر و شبکه و بهره‌برداری از شبکه‌های کامپیوتری خودی است. نتایج پژوهش به شرح نمودار (۲) جمع‌بندی می‌شود.




**نمودار (۲) آسیب‌پذیری‌های سامانه مکانیزه لجستیک نهاجا در برابر تهدیدات آینده**

**پیشنهادها**

۱. استفاده از شبکه امن، چندلایه و استفاده از زیرساخت دوگانه (فیبر نوری ویژه نیروهای مسلح به‌صورت کامل و سیستم رادیویی تاکتیکی بومی) و عدم وابستگی زیرساخت‌های ارتباطی نهاجا به زیرساخت ارتباطی کشور و راه‌کارهای امنیت سایبر توسط معاونت فاوا و آمادوپشتیبانی نهاجا به‌صورت متمرکز و سرا سری برای کلیه یگان‌های نهاجا.

۲. الزام اجرای دوره‌های آموزشی دستورالعمل امنیتی کار با رایانه، تعریف و تعویض دوره‌ای کلمه عبور برای هریک از کارکنان مرتبط با سامانه مکانیزه لجستیک نهاجا توسط معاونت فاوا و معاونت تربیت و آموزش نهاجا.

۳. به‌کارگیری نرم‌افزارهای ضدویروس و ضد بدافزار، تدوین استراتژی امنیتی برای حفظ امنیت در زیرساخت‌های فناوری اطلاعات و ارتباطات و آموزش یگان‌های اجرایی برای کشف جرائم اطلاعاتی و تروریستی در محیط‌های فناوری اطلاعات توسط م فاوا و م تربیت و آموزش نهاجا.
۴. برنامه‌ریزی لازم در خصوص فراهم‌سازی ابزار نظارت ستادی برای انجام فعالیت‌های امنیتی و همچنین پیش‌بینی استفاده از بزرگ‌رایانه‌های موجود در سازمان‌های نظامی و یا دولتی در سطح شهر تهران به‌عنوان سایت پشتیبان موازی و جایگزین (بر خط) با رعایت فاصله از سایت اصلی و مرکز فرماندهی (پست فرماندهی) م فاوای نهاجا.
۵. در اختیار داشتن کارکنان متخصص در حوزهٔ امنیت فاوا با کمک معاونت فاوا و معاونت آموزش نهاجا و سرمایه‌گذاری مناسب و تخصیص منابع مالی در جهت ارتقاء امنیت فاوا از طرف م طرح و برنامه‌وبودجه و م آمادوپشتیبانی نهاجا.
۶. پیش‌بینی، طراحی و ساخت سامانه آمادفنی و سرور مرکزی سیار و چابک و قابل‌گسترش به اماکن جغرافیایی امن در زمان‌های تهدید و بحران توسط م فاوا، م آمادوپشتیبانی و ف آمادوپشتیبانی هوایی نهاجا.
۷. طراحی و ساخت سپر الکترومغناطیسی و یا قفس فارادی و همچنین انجام مهندسی مجدد اماکن سامانه و سرور مرکزی برای مقاوم‌سازی تأسیسات سامانه با همکاری معاونت مهندسی و پدافند غیرعامل نهاجا و فرماندهی آمادوپشتیبانی هوایی و با نظارت معاونت عملیات نهاجا.

## قدردانی

از خبرگان توانمندی که در طول پژوهش، دانش خویش را سخاوتمندانه در اختیار محققان این پژوهش قرار دادند و استواری پژوهش حاضر بر مشارکت و دانش این بزرگواران قرارگرفته است بسیار سپاسگزاریم.

## منابع


- آذر، داوود، مسلمی، حسین، (۱۳۹۳) *شناخت تهدیدات فضای سایبری و پدافند آن*، تهران: انتشارات دافوس.
- آقا محمدی، داوود، (۱۳۹۲) *سامانه‌های رزم زمینی چابک*، تهران: انتشارات دافوس.

- *آمادفنی*، آیین‌نامه ۶-۳۳ ه، (۱۳۷۸) تهران: انتشارات مرکز تحقیقات فرماندهی آمادوپش هوایی نهاجا.
- ابولحسینی، علیرضا، (۱۳۹۲)، *معرفی و برآورد تهدیدات سایبری*، تهران: انتشارات دیده‌بان.
- امینی ورکی، سعید، مشهدی، حسن، مبانی نظری (۱۳۹۵) *مدیریت آسیب‌پذیری زیرساخت‌ها*، تهران: چاپ بوستان حمید.
- جعفری لاری، علی‌اصغر، (۱۳۹۴) *امنیت سایبری و جنگ سایبری*، تهران: انتشارات پندار پارس.
- جلالی فراهانی، غلامرضا، (۱۳۹۱) *مقدمه‌ای بر روش و مدل برآورد تهدیدات در پدافند غیرعامل*، تهران: موسسه چاپ و انتشارات دانشگاه امام حسین.
- جلالی فراهانی، غلامرضا، رسولی آهاری، سید داوود، اسکندری، حمید، (۱۳۹۵) *گذری بر قوانین و مقررات پدافند غیرعامل*، تهران: انتشارات دانشگاه امام حسین.
- حافظ نیا، محمدرضا، (۱۳۹۰) *جغرافیای سیاسی فضای مجازی*، تهران: انتشارات سمت.
- حبیبی، نیک بخش، (۱۳۹۲) *ماهیت شناسی جنگ در فضای نامتقارن*، تهران: مرکز انتشارات راهبردی نیروی هوایی.
- حبیبی، نیک بخش، (۱۳۹۲) *ماهیت قدرت هوایی*، تهران: مرکز انتشارات راهبردی نیروی هوایی.
- حسن بیگی، ابراهیم، (۱۳۹۴) *ارائه الگوی راهبردی دفاع دانش‌بنیان در مقابل تهدیدات آینده*، پایان‌نامه مطالعات گروهی دانشگاه و پژوهشگاه راهبردی عالی دفاع ملی.
- حسن‌زاده اسدی، جعفر و انتظار شبستری، رضا و هایی، حمیده، (۱۳۹۰) *دفاع سایبری*، تهران: انستیتو ایزایران.
- حیدری، کیومرث، (۱۳۹۰) جنگ‌های آینده، تهران: نشر آجا.
- خواجوی، محسن، جلالی فراهانی، غلامرضا، (۹۰ ۱۳) *بررسی تهدیدات و آسیب‌پذیری‌های سایبری در حوزه ارتباطات زیرساختی کشور*، مجموعه مقالات نخستین همایش ملی دفاع سایبری.
- *دستورالعمل اجرایی شماره ۱-۳۶* ف آمادوپش هوایی، (۱۳۸۱) تهران: انتشارات معاونت طرح و خط و مشی ف آمادوپشتیبانی هوایی نهاجا.
- دهستانی، علیرضا، (۱۳۹۱) *کامل‌ترین مرجع کاربردی شبکه‌های کامپیوتری و ارتباطی*، تهران: ناشر نیاز دانش.
- رستمی، محمود، (۱۳۷۸). *فرهنگ واژه‌های نظامی*، تهران: ستاد مشترک ارتش جمهوری اسلامی ایران، چاپ اول.

- زینلی، نصرالله، (۱۳۹۴) *آمادوپش (لجستیک) هوایی در دفاع مقدس*، تهران: مرکز انتشارات راهبردی نهاجا.
- شهلایی، محمدابراهیم، شهلایی، هما، (۱۳۹۳) *مبانی سایبرنتیک و تهدیدات در حوزه سایبر*، تهران: انتشارات مرکز آموزشی و پژوهشی شهید سپهبد صیاد شیرازی.
- کرامر، فرانکلین، استلر، استوارت، ونیز، لری؛ (۱۳۹۴) *قدرت سایبری و امنیت ملی*، مترجم معاونت پژوهش و تولید علم، ناشر، تهران: موسسه چاپ و انتشار دانشکده اطلاعات.
- گلنتاج، عیسی، (۱۳۹۵)، پدافند غیرعامل تجهیزات الکترونیکی در مقابل بمب‌های الکترومغناطیسی، *دوفصلنامه علمی تخصصی پدافند غیرعامل*،تهران: انتشارات قرارگاه پدافند هوایی خاتم‌الانبیا (ص) آجا.
- لطیفی، اکبر، (۱۳۸۸) *آمادوپشتیبانی در نهاجا*، تهران: چاپخانه دانشگاه هوایی شهید ستاری.
- مدیری، ناصر، شاه ولایتی، منیر سادات، (۱۳۹۰) *مهندسی پدافند غیرعامل شبکه‌های کامپیوتری*، چاپ اول، تهران: انتشارات مهرگان قلم.
- مرادیان، محسن، (۱۳۹۱) *مبانی نظری امنیت*، تهران: چاپخانه پشتیبانی سازمان حفاظت اطلاعات ارتش ج ا ا.
- میر سمیعی، سید محمد، چشمه نور، مرتضی، (۱۳۹۵)، *مدیریت بحران و مقابله با بلیات*، انتشارات پشتیبان، چاپ اول.
- نیری، آرش، (۱۳۹۲) *تحلیل و طراحی ساختمان‌ها در برابر اثرات انفجار*، تهران: دانشگاه صنعتی مالک اشتر.