دریافت مقاله: ۱۳۹۹/۰۷/۲۵ فصلنامهٔ مدیریت نظامی
پذیرش مقاله: ۱۳۹۹/۱۲/۲۶ سال بیستم، شمارهٔ ۳، پائیز ۱۳۹۹
**مقاله پژوهشی** ص‌ص ۱۶۷- ۱۹۴

# ارائه الگوی ارزیابی آسیب‌پذیری سایبری سازمان‌های نظامی در حوزه نرم‌افزار

مهدی بصیری[۱*]، امید اردلان[۲]، مهدی صمیمی[۳]

**چکیده**

آسیب‌پذیری نرم‌افزاری همواره به‌عنوان یک مسئله مهم در حوزه امنیت سایبری سازمان‌های نظامی مطرح بوده است. برخورداری از نرم‌افزار فاقد آسیب‌پذیری در عمل امکان‌پذیر نبوده و به همین دلیل برای بالا بردن سطح امنیت نیاز به مدیریت آسیب‌پذیری‌ها است. هدف مقاله پیش‌رو بررسی و شناخت آسیب‌پذیری‌های سایبری سازمان‌های نظامی در حوزه نرم‌افزار و ارائه الگویی برای ارزیابی این آسیب‌ها می‌باشد. نوع تحقیق کاربردی و روش تحقیق بکار رفته آمیخته از نوع توصیفی(موردی- زمینه‌ای) بوده و از روش‌های کمی و هم کیفی در تحلیل داده‌های جمع‌آوری‌شده استفاده شده است. جامعه آماری تحقیق شامل کارشناسان و خبرگان حوزه سایبری ستاد نهاجا بوده است. محقق با بهره‌گیری از منابع کتابخانه‌ای و بررسی اسناد و مدارک به شناسایی انواع آسیب‌پذیری‌های سایبری نرم‌افزارها پرداخته و سپس با انجام مصاحبه با خبرگان به شناسایی ابعاد و مؤلفه‌های الگوی ارزیابی آسیب‌پذیری اقدام نموده است. یافته‌های تحقیق بیانگر آن است که الگوی ارزیابی آسیب‌پذیری سایبری سازمان‌های نظامی در حوزه نرم‌افزاری دارای چهار بعد (فرآیند تولید نرم‌افزار، روش‌ها، ساختار سازمانی و آموزش) و سیزده مؤلفه می‌باشد؛ که از میان این چهار بعد، فرآیند تولید نرم‌افزار بیش‌ترین اهمیت و فرآیند آموزش کمترین اهمیت را در پوشش آسیب‌پذیری دارد. تقویت ساختارهای سایبری، ارتقای سطح آموزش‌های مدیران و کارکنان، پشتیبانی، نگهداری و ارتقاء فنی نرم‌افزارهای کاربردی ازجمله راه‌کارهای پیشنهادی به منظور کاهش آسیب‌پذیری‌های سایبری در سازمان‌های نظامی می‌باشد.

**واژهای کلیدی:** الگو، آسیب‌پذیری سایبری، نرم‌افزار، سازمان‌های نظامی.

---

۱. دکتری مدیریت تکنولوژی اطلاعات، تهران، ایران، (* نویسنده مسئول)؛ basiri٦٠@gmail.com
۲. استادیار دانشگاه فرماندهی و ستاد آجا، تهران، ایران
۳. استادیار دانشگاه افسری امام علی(ع)، تهران، ایران

**مقدمه**

ارزیابی تهدیدات و آسیب‌پذیری‌ها، یکی از دغدغه‌های اصلی و همیشگی مسئولان حوزه امنیت در یک کشور است. این موضوع چنان مهم است که در بسیاری از مـــوارد می‌تواند باعث کاهش چشمگیر آسیب‌پذیری‌ها شود یا پیامدهای یک تهدید را به حداقل ممکن کاهش دهد. بر این اساس، هدف اصلی این مقاله پاسخ دادن به بررسی و شناخت آسیب‌پذیری‌های سایبری سازمان‌های نظامی در حوزه نرم‌افزار و ارائه الگویی برای ارزیابی این آسیب‌ها می‌باشد. رسیدن به این مهم، نیازمند به‌کارگیری روش‌هایی است که بتواند ارزیابی و برآورد صحیحی از وضعیت آسیب‌ها در یک مجموعه ارائه دهد. در این زمینه اقداماتی صورت پذیرفته است، اما آنچه در بررسی‌های اولیه مشخص شد، حکایت از آن دارد که یک الگو یا چارچوب مدون و بومی‌شده‌ای که بتواند فهرستی از آسیب‌ها سایبری را پوشش دهد، وجود ندارد و آنچه اکنون ملاحظه می‌شود، غالباً ترجمه روش‌ها یا الگوهایی است که در خارج از کشور تدوین شده‌اند (مشهدی، ۱۳۹۴: ۳).

نامتعارف‌بودن ساختارهای سایبری، رشد سریع و نامتوازن زیرساخت‌های سایبری، گمنامی، افزایش چشم‌گیر وابستگی حاکمیت ملی و سازمانی بر فعالیت‌های سایبری علی‌رغم تبعات مثبت، موجب افزایش آسیب‌پذیری و تهدیدات متنوع و حوادث خطرناک در این زمینه گردیده است (قوچانی خراسانی و حسین پور، ۱۳۹۶: ۵۱)

حوزه کارکردی تهدیدات سایبری بسیار وسیع و حیاتی بوده و به دلیل تغییرات دائمی در شکل و ماهیت این تهدیدات و به عبارتی پویا بودن آن‌ها، هر روزه تهدیدات جدیدتری ایجاد و مطرح می‌گردد (خواجوی و جلالی، ۱۱۹:۱۳۹۰).

آسیب‌پذیری نرم‌افزاری همواره به‌عنوان یک مسئله مهم در حوزه امنیت رایانه مطرح بوده است. برخورداری از نرم‌افزار فاقد آسیب‌پذیری، یک دستاورد ایده‌ال بوده که با این حال در عمل دست‌نیافتنی است. به همین دلیل برای بالا بردن سطح امنیت نیاز به مدیریت و کنترل آسیب مطرح است (فریدون زاده،۲۰۳:۱۳۹۰).

ساماندهی و بهره‌برداری امن و پایدار از فناوری اطلاعات و ارتباطات در نهاجا و توجه به تهدیدات و آسیب‌های متصور در این حوزه جهت دستیابی به امنیت مطلوب، متناسب با پیشرفت فناوری اطلاعات امری اجتناب‌ناپذیر می‌نماید چراکه بررسی‌ها نشان از بروز جنگ

سایبری بین ایران و سرویس‌های جاسوسی غربی دارد که از آن جمله می‌توان به مواردی چون طراحی تجهیزات سخت‌افزاری و نرم‌افزاری جهت ارتباطات امن با جاسوس‌های خود در ایران (اینترنت چمدانی، vpnها و فیلترشکن‌ها) و همچنین طراحی بدافزارهای رایانه‌ای جهت ضربه زدن به امنیت جمهوری اسلامی و به‌ویژه مراکز امنیتی و نظامی از طریق ویروس‌هایی همچون stuxnet, wiper flame و..... نام برد. بنابراین با توجه به نقش حیاتی که نرم‌افزار در مدیریت و ذخیره‌سازی اطلاعات و تأمین ارتباطات شبکه‌ای دارد، مطالعه‌ی تهدیدات و بررسی ابعاد مختلف آن و شناسایی آسیب‌پذیری‌های در این حوزه به‌منظور ارائه راه‌کارهای پدافندی ازجمله موضوعات بسیار مهمی است که پژوهش در این زمینه را ضروری می‌سازد.

در سازمان‌های نظامی با وجود استفاده روزافزون از رایانه به‌ویژه در بخش نرم‌افزار هنوز تحقیق علمی و منسجمی در این زمینه صورت نگرفته است. نظر به اهمیت، ابعاد و عمق تأثیرگذاری فضای سایبر، این پژوهش به دنبال پاسخ به پرسش‌های زیر است:

- ✓ آسیب‌پذیری‌های ایجادشده برای نهاجا در حوزه نرم‌افزاری در فضای سایبری کدام‌اند؟
- ✓ ابعاد و مؤلفه‌های الگوی ارزیابی آسیب‌پذیری نرم‌افزاری نهاجا کدام است؟

## مبانی نظری و پیشینه

### مفهوم فضای سایبر

فضای سایبر شبکه‌های وابسته به یکدیگر، از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه‌های رایانه‌ای، پردازنده‌های تعبیه‌شده، نرم‌افزارهای کاربردی و اثر متقابل بین این محیط و انسان به منظور تولید، پردازش، ذخیره‌سازی، مبادله، بازیابی و بهره‌برداری از اطلاعات را شامل می‌شود. این فضا ممکن است در ارتباط مستقیم و مداوم با سامانه‌های فناوری اطلاعات و شبکه‌های ارتباطی اعم از اینترنت و یا ... باشد یا تنها قابلیت اتصال به محیط پیرامونی در آن تعبیه‌شده باشد (محمودزاده و اسماعیلی، ۱۳۹۷).

فضای سایبری سازمان‌های نظامی شامل تمامی سامانه‌هایی است که با تجهیزات و سامانه‌های فاوا مرتبط بوده و از طریق آن اجرای مأموریت انجام می‌گردد. به‌عبارتی فضای سایبر سازمان‌های نظامی مشتمل بر تمامی شبکه‌های داده‌ای، نرم‌افزارهای عملیاتی، سخت‌افزارهای ارتباطی، تجهیزات و ادوات نظامی مجهز به سامانه‌های فاوا به‌صورت مستقل یا مرتبط، محدود یا گسترده که در آن تبادل اطلاعات در راستای اجرای مأموریت ایجاد و

درحال‌توسعه است، می‌باشد (طرح ارتقا امنیت و افزایش قدرت دفاع سایبری در ن. م، ۱۳۹۴، ۱۳).

## مفهوم و ماهیت آسیب‌پذیری

در ارتباط با تعریف، مفهوم و ماهیت آسیب‌پذیری تاکنون بحث‌های زیادی ارائه‌شده است. اکثر این تعاریف مرتبط و هم سو باهدف یا اهداف تحقیقاتی یا تجاری گروه کاری یا نویسنده مربوطه است.

با توجه به وجود تعاریف متعدد از آسیب‌پذیری، در این بخش تعدادی از آن‌ها را موردبحث قرار داده‌ایم و سعی شده است ابهامات، نقاط ضعف و قوت آن‌ها بیان شود. هم‌چنین در ادامه یک تعریف مناسب از آسیب‌پذیری که تا حد امکان جامع و کامل باشد ارائه‌شده است (موسسه توسعه و گسترش افتا، ۱۳۹۰).

تاکنون تعاریف بسیاری برای آسیب‌پذیری ارائه‌شده است. آسیب‌پذیری بستری بالقوه و مستعد برای وقوع حمله است که هر زمان اتفاق بیفتد، می‌تواند رفتاری نامطلوب و غیرصحیح به‌وجود آورد (هانسمن، ۲۰۰۵).

در تعریف دیگری بیشاپ آسیب‌پذیری را به معنای وجود ضعف امنیتی در سیستم تعریف نموده است که امکان سوءاستفاده از سیستم و تهدید صحت و جامعیت اطلاعات را از جانب مهاجمان فراهم می‌آورد (بیشاپ، ۲۰۰۳).

آمان[۱]، ویجسکرا[۲] و کائوشیک[۳] تعریف مناسب‌تری از آسیب‌پذیری آورده‌اند که: هر ویژگی از یک سیستم رایانه‌ای که امکان نقض خطی مشی‌های امنیتی آن سیستم را به فرد یا افرادی بدهد، آسیب‌پذیری نام دارد. این تعریف یک نقطه‌ضعف دارد و آن اینکه آسیب‌پذیری را به یک سیستم رایانه‌ای محدود کرده است، درحالی‌که آسیب‌پذیری می‌تواند مرتبط با یک نرم‌افزار، یک سیستم، یک شبکه و یا حتی رفتار کاربران آن باشد. البته این مورد در تعریف قابل‌تعمیم است. ممکن است سیستم کلمه‌ای جامع در نظر گرفته شود که شامل تمام این

---

۱. Amman
۲. Wijesekera
۳. Kaushik

موارد باشد (آمان و همکاران، ۲۰۰۲: ۳).

## عوامل ایجاد آسیب‌پذیری

نرم‌افزارهای رایانه‌ای نیز همانند بقیه سامانه‌های رایانه‌ای به‌طور کامل امن نبوده و دارای نقاط ضعف و آسیب‌پذیر بسیاری می‌باشند و امکان رخنه و نفوذ به درون آن‌ها و درنتیجه سرقت اطلاعات و یا فروپاشی آن‌ها وجود دارد. معمولاً آسیب‌پذیری‌های نرم‌افزارهای رایانه‌ای به یکی از چهار صورت زیر ایجاد می‌شوند: برخی از آسیب‌پذیری‌ها قبل از ایجاد سیستم و در مرحله تجزیه‌وتحلیل و بررسی نیازمندی‌های سیستم ایجاد می‌شوند. بدین‌صورت که کاربر (کارفرما یا مرجعی که سیستم را سفارش می‌دهد) در هنگام توصیف نیازمندی‌های خود دچار اشتباه شده و یا به دلیل سهل‌انگاری برخی از خطی مشی‌های امنیتی[۱] خود را بیان نکرده و یا ناقص بیان می‌کند.

به‌عنوان‌مثال ممکن است برای یکی از کارکنان بخش انبار که به‌هیچ‌وجه نباید بتواند حقوق سایر کارکنان را کم یا زیاد کند در مرحله توصیف نیازمندی‌ها سهل‌انگاری شده و این مورد فراموش شود. هنگامی‌که چنین سامانه‌ای به بهره‌برداری می‌رسد، این رخنه یا نقطه‌ضعف در آن وجود دارد و کارمند بخش انبار می‌تواند به‌صورت غیرمجاز حقوق خود و دیگران را تغییر دهد.

آسیب‌پذیری‌هایی که در مرحله طراحی سیستم ایجاد می‌شوند. در این موارد کاربر نیازهای خود را به‌طور واضح، صریح و دقیق بیان می‌کند، ولی مهندسان در هنگام طراحی سیستم مربوطه دچار اشتباهات طراحی‌شده که درنهایت منجر به ایجاد یک یا چند آسیب‌پذیری در سیستم می‌شود. به‌عنوان‌مثال در هنگام طراحی یک نگارش خاص برای اتصالات نیمه‌باز[۲] یک صف یا بافر(حافظه حائل داخلی) محدود در نظر گرفته‌شده است. TCPپروتکل تعداد زیادی SYNمهاجمان از این نقطه‌ضعف استفاده می‌کنند و با ارسال پیاپی بسته‌های اتصال نیمه‌باز با سرویس‌دهنده مربوطه برقرار می‌کنند. پس از مدتی بافر اختصاص داده‌شده به اتصالات نیمه‌باز

---

۱. Security Policy
۲. Half Open Connections

پرشده و سیستم از کار می‌افتد.[۱]

آسیب‌پذیری‌هایی که در مرحله کد نویسی یا برنامه‌نویسی به وجود می‌آیند. این دسته از آسیب‌پذیری‌ها که در بین برنامه‌های کاربردی تحت وب[۲] بسیار شایع است، در اثر سهل‌انگاری و بی‌دقتی کد نویسان و برنامه‌نویسان به وجود می‌آید. به‌عنوان‌مثال در هنگام نوشتن یک تابع به زبان C در یک برنامه کاربردی، ممکن است برنامه‌نویس طول آرگومان‌های رشته‌ای که به تابع ارسال می‌شوند را بررسی نکند. یک مهاجم باهوش می‌تواند با ارسال پارامترهای غیرمجاز با طول بیش‌ازحد مجاز یک حمله از نوع سرریزی پشته[۳] را ترتیب دهد و باعث فروپاشی سیستم شود. البته در مورد سامانه‌های سخت‌افزاری نیز این‌گونه آسیب‌پذیری‌ها وجود دارد (الخوالد و دیگران، ۲۰۱۹: ۵).

آسیب‌پذیری‌هایی که در هنگام نگهداری[۴] و یا پیکربندی[۵] سیستم ایجاد می‌شوند. برخی از این آسیب‌پذیری‌ها از اشتباهات، خطاها و سهل‌انگاری‌های تولیدکنندگان سامانه‌ها ناشی نمی‌شود، بلکه مستقیماً ناشی از اقدامات مدیر سیستم[۶] و یا افرادی است که سیستم را در حین استفاده نگهداری می‌کنند. به‌عنوان‌مثال یک مسئول شبکه ممکن است به‌اشتباه، یکی از پورت‌های بلااستفاده سیستم را باز بگذارد و یک راه بسیار خوب و مطمئن برای نفوذ به سیستم را در اختیار مهاجمان قرار دهد. این دسته از آسیب‌پذیری‌ها بسیار شایع است (الخوالد و دیگران، ۲۰۱۹: ۵).

علاوه بر موارد بالا، به علت پراکندگی، توزیع‌شدگی و تعداد زیاد عناصر موجود در یک شبکه، امکان وجود نقاطی که از آن‌ها بتوان به سیستم نفوذ کرد بیشتر از سایر سامانه‌های رایانه‌ای است. با بزرگ‌تر شدن یک شبکه و افزایش سرویس‌های ارائه‌شده توسط آن، ضرورت حفظ امنیت شبکه و پیشگیری و مقابله با حملات احتمالی بیشتر می‌شود و نیاز به تدابیر

---

۱. این حمله یکی از حملات رایج و معروف باشد که یک نوع حمله منع سرویس یا (Dos) است.

۲. Web Applications
۳. Buffer Overflow
۴. Maintenance
۵. Configuration
۶. System Administrator

امنیتی قوی‌تر و مؤثرتری است (موسسه توسعه و گسترش افتا، ۱۳۹۰: ۴۵).

**جدول شمارهٔ ۱: آخرین آسیب‌پذیری‌های نرم‌افزارهای پرکاربرد کشور(مرکز ماهر،۱۳۹۹)**

| سرویس‌دهنده‌ها (وب، پست الکترونیک، پراکسی و غیره) | | | |
|---|---|---|---|
| دریافت آخرین نسخه‌ی پایدار | | | |
| موضوع | آخرین نسخه‌ی پایدار | تاریخ عرضه | لینک دریافت |
| Apache Web Server | 2.4.33 | 2018-03-17 | goo.gl/ySdR |
| Squid Proxy & Cache Server | 3.5.27 | 2017-08-19 | goo.gl/ZCyZ6f |

| آسیب‌پذیری‌ها | | | | | | | |
|---|---|---|---|---|---|---|---|
| موضوع | شناسه | منبع | تاریخ انتشار | سطح خطر | خلاصه‌ای از آسیب‌پذیری | نحوه رفع | اطلاعات بیشتر |
| Microsoft Project Server, Microsoft SharePoint | CVE-2018-8254<br>CVE-2018-8252 | goo.gl/j3jjPY<br>goo.gl/YysDAv | 2018-06-12 | متوسط | آسیب‌پذیری افزایش سطح دسترسی و XSS در Microsoft SharePoint به واسطه‌ی عدم پاک‌سازی مناسب درخواست‌های وب جعلی | برای Microsoft SharePoint Enterprise Server 2016: goo.gl/bg49ms<br>برای Microsoft Project Server 2010 SP2: goo.gl/zVhF4A | goo.gl/kvYuUk<br>goo.gl/LDBaLC |
| Windows DNS | CVE-2018-8225 | goo.gl/Mw9xZc | 2018-06-12 | زیاد | آسیب‌پذیری اجرای کد از راه دور در ویندوز به واسطه‌ی عملکرد نامناسب DNSAPI.dll و بروز خطا هنگام مدیریت پاسخ‌های DNS | برای ویندوز 10 1507 32, 64bit: goo.gl/SDirZr<br>برای ویندوزهای Server 2012 R2 و 8.1 32, 64bit: goo.gl/a2sdhv | goo.gl/WUWNqf |

## پیشینه تحقیق

الهمزمی و همکارانش (۲۰۰۷) یک مدل جهت استخراج شدت آسیب‌پذیری‌های نرم‌افزاری سیستم‌ها ارائه نموده، سپس این مدل را بر روی پنج سیستم‌عامل مختلف آزمایش و نتایج آن را مورد بررسی قرار داده‌اند. قسام کبار (۲۰۰۹) یک روش مدیریت ریسک جهت ارزیابی ریسک‌های امنیتی ارائه نموده است که این ریسک‌ها از طریق سه مؤلفه: آسیب‌پذیری‌ها، احتمال شکست و حملات احتمالی که منجر به تهدید می‌شوند محاسبه می‌گردد. گلان و همکارش(۲۰۱۱) به ارائه روشی پرداخته‌اند که از ترکیب گراف حملات با چارچوب سیستم عمومی ارزیابی آسیب‌پذیری(CVSS[۱]) برای شناسایی صدمات شبکه‌ها و میزبان‌ها استفاده می‌کند.

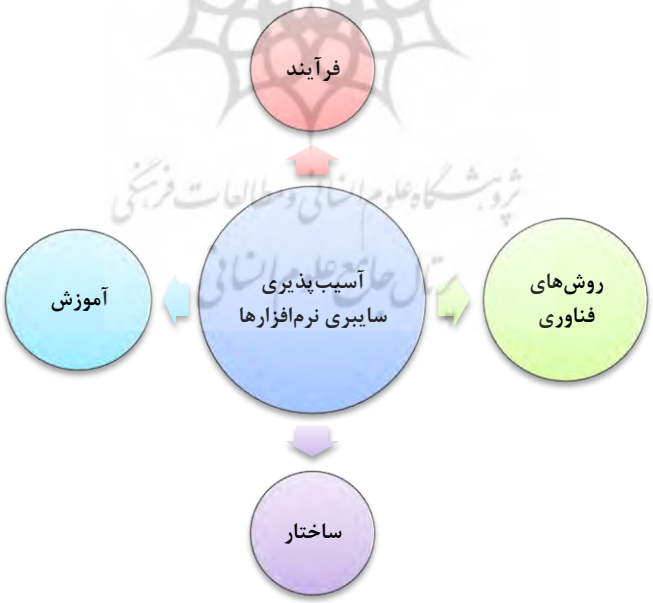
نتایج این روش شدت هر حمله را با استفاده از روش سیستم عمومی ارزیابی آسیب‌پذیری شناسایی و ارائه می‌کند. گری و همکارانش به ارائه یک رویکرد به نام MCDA پرداخته‌اند که

۱. Common Vulnerability Scoring System

ضمن شناسایی شدت کمی آسیب‌پذیری‌های نرم‌افزاری به استخراج هزینه‌های اقتصادی ناشی از سوءاستفاده از این آسیب‌پذیری‌ها می‌پردازد. سپس با ارائه یک آنالیز از نتایج در خصوص اولویت‌بندی و تصمیم‌گیری در خصوص آسیب‌پذیری‌ها اقدام می‌نماید. صالحی (۱۳۸۵) در تحقیقی با عنوان «بررسی امنیت شبکه‌های رایانه‌ای در محیط‌های نظامی و بررسی لزوم تولید یک پروتکل جدید برای امنیت شبکه» به دنبال پاسخ به این سؤال بوده‌اند که امنیت شبکه‌های رایانه‌ای محیط‌های نظامی در چه سطحی بوده و رابطه هر یک از عوامل انسانی، سخت‌افزار، نرم‌افزار، سیستم‌عامل و پروتکل‌ها با امنیت این شبکه‌ها به چه میزان است؟ نتایج این تحقیق نشان می‌دهد که ایجاد امنیت برای شبکه‌ها علاوه بر تولید پروتکل ارتباطی در شبکه‌های رایانه‌ای محیط‌های نظامی، امنیت فیزیکی شبکه‌های رایانه‌ای هم که ریشه در بحث عامل انسانی دارد از عواملی است که باید موردتوجه قرار گیرد.

## مدل مفهومی تحقیق

با در نظر داشتن ابعاد مشخص‌شده در حوزه نرم‌افزاری سازمان‌های نظامی، مدل مفهومی تحقیق را به‌صورت زیر می‌توان نمایش داد. فرآیند، روش‌ها، ساختار و آموزش ابعاد آسیب‌پذیری سایبری سازمان‌های نظامی در حوزه نرم‌افزاری بوده و ارتباط دوسویه باهم دارند.




**شکل شمارهٔ ۱: مدل مفهومی تحقیق**

**روش‌شناسی تحقیق:**

پژوهش حاضر از نظر نوع کاربردی و از نظر ماهیت و روش از نوع توصیفی (موردی – زمینه‌ای) بوده که بر روی موردی خاص و زمینه‌ی ویژه‌ای تمرکز داشته و تصویری جامع و گسترده از آن را برای آینده ارائه می‌نماید. شیوه انجام تحقیق بدین‌صورت است که در بخش اول محقق با بهره‌گیری از منابع کتابخانه‌ای به بررسی آسیب‌پذیری‌های حوزه نرم‌افزاری سازمان‌های نظامی پرداخته و سپس اقدام به تهیه سؤالات و انجام مصاحبه با صاحب‌نظران نموده است و با بهره‌گیری از این منابع اقدام به تهیه و توزیع پرسشنامه نموده است. در بخش دوم با تقسیم‌بندی منابع مورد مطالعه و اسناد و مدارک جمع‌آوری‌شده و تجزیه و تحلیل پاسخ‌های ارائه‌شده در پرسشنامه و با استفاده از تجزیه و تحلیل آماری جهت نیل به پاسخ سؤالات به ارائه راهکارها منطبق بر اهداف پرداخته‌شده است.

جامعه آماری تحقیق شامل کلیه صاحب‌نظران و کارشناسان حوزه فناوری اطلاعات و رایانه‌ای دارای مدرک کارشناسی ارشد و بالاتر و نیز برخوردار از تجربه کاری بالای ده سال در حوزه فاوا ستاد نهاجا به تعداد ۴۲ است. روش نمونه‌گیری مورداستفاده نیز با توجه به محدود بودن جامعه آماری روش تمام شماره بوده است. به منظور جمع‌آوری داده‌ها و اطلاعات ترکیبی از روش کتابخانه‌ای و میدانی(مصاحبه و پرسشنامه) استفاده شده است.

به منظور سنجش اعتبار ابزار پرسشنامه از روش اعتبار محتوا و سنجش پایایی از روش آلفای کرون باخ استفاده گردید. روایی محتوای پرسشنامه مزبور با نظرسنجی از خبرگانی که به‌طور همزمان دارای دانش و همچنین تجربه کاری در حوزه پژوهش هستند سنجیده شد. بدین ترتیب با ارائه آن خبرگان و دریافت نظرات اصلاحی آن‌ها، روایی محتوای پرسشنامه موردنظر تأیید قرار می‌گیرد. به منظور سنجش پایایی تحقیق، تعداد ۱۵ نفر از افراد برای هر گروه که تجانس و همگونی با جامعه آماری داشته‌اند انتخاب و پس از توجیه نمودن آنان با بهره‌گیری از روش پیش آزمون، سؤالات تنظیم‌شده در بین آنان توزیع گردیده است. بدین منظور یک نمونه اولیه شامل ۱۵ پرسشنامه پیش آزمون گردید و سپس با استفاده از داده‌های به‌دست‌آمده از این پرسشنامه‌ها و به کمک نرم‌افزار آماری spss میزان پایایی پرسشنامه مورد آزمون قرار گرفت که نتایج آن به شرح جدول ۲ است:

**جدول شمارهٔ ۲: پایایی مؤلفه‌های الگو مفهومی**

| مقیاس | ضریب آلفای کرونباخ |
|---|---|
| بعد آموزش | ۰/۸۶ |
| بعد فرهنگ‌سازمانی | ۰/۸۳ |
| بعد زیرساخت | ۰/۹۱ |
| بعد خط‌مشی فناوری اطلاعات | ۰/۹۳ |
| بعد ساختار سازمانی | ۰/۸۴ |
| بعد برنامه‌های نرم‌افزاری | ۰/۹۲ |
| کل پرسشنامه | ۰/۹۵ |

تحلیل مصاحبه برای استخراج مطالب و اطلاعات مورد نیاز حاصل از مصاحبه با صاحب‌نظران از جدول ۳ استفاده شد، به صورتی که با تفکیک بیاناتی که دارای مضامین موردنظر بودند، تحلیل محتوای کمّی این بخش از پژوهش انجام گردید. محقق نکات کلیدی مصاحبه‌شوندگان را انتخاب و با مشورت پنج تن از خبرگان حوزه سایبری و فاوا تمرکز جملات تعیین گردید. در مرحله بعد مفاهیمی که از تمرکز و متن جملات برداشت می‌شد استخراج گردید. سپس متغیرها یا مقولات حاصل از مفاهیم نام‌گذاری و در ستون چهارم درج شد.

**جدول شمارهٔ ۳: جدول مورد استفاده برای تحلیل محتوای مصاحبه**

| نکات کلیدی مصاحبه‌شوندگان | تمرکز جملات | مفاهیم | متغیرهای استخراج‌شده | کدگذاری |
|---|---|---|---|---|
| | | | | |

در مرحله پایانی به هر یک از متغیرها باهدف کمّی‌سازی تحلیل مصاحبه یک کد تخصیص داده شد که در طراحی مدل مفهومی تحقیق کمک نماید. متغیرهای با فراوانی بیشتر وارد تحقیق شد و متغیرهای با فراوانی کمتر از تحقیق خارج گردید.

**جدول شمارهٔ ۴: کدگذاری متغیرهای تحقیق**

| ردیف | متغیرهای استخراج‌شده | کد |
|---|---|---|
| | **فرآیندها** | ف |
| ۱ | فرآیندهای اصلی(برنامه‌های نرم‌افزاری) | ف/۱ |
| ۲ | فرآیندهای مدیریتی(فرهنگ‌سازمانی کاربران) | ف/۲ |

| | | |
|---|---|---|
| ۳ | فرآیندهای پشتیبانی | |
| | - شبکه | ف/۳۱ |
| | - سخت‌افزار | ف/۳۲ |
| | - ارتباط | ف/۳۳ |
| | **روش‌ها** | ر |
| ۱ | خط‌مشی‌های کلان | ر/۱ |
| ۲ | خط‌مشی‌های خرد(فنی) | ر/۲ |
| | **ساختار سازمانی** | س |
| ۱ | ساختار امنیت | س/۱ |
| ۲ | ساختار فناوری اطلاعات | س/۲ |
| ۳ | ساختار ارتباط | س/۳ |
| ۴ | میزان انعطاف‌پذیری ساختار سازمانی | س/۴ |
| | **آموزش** | آ |
| ۱ | آموزش عمومی فناوری اطلاعات | آ/۱ |
| ۲ | آموزش متخصصین فناوری اطلاعات | آ/۲ |
| ۳ | آموزش مدیران درزمینهٔ فناوری اطلاعات | آ/۳ |

به منظور تجزیه و تحلیل پرسشنامه تحقیق در گام اول با استفاده از نشست خبرگی اقدام به شناسایی آسیب‌پذیری‌های سایبری سازمان‌های نظامی در حوزه نرم‌افزاری شد. محقق با توزیع پرسشنامه بین کارشناسان فضای سایبر در حوزه نرم‌افزاری و جمع‌آوری پرسشنامه‌های تکمیل‌شده اقدام به تحلیل آن به کمک نرم‌افزار SPSS کرده است. در گام دوم محقق اقدام به ارزیابی این آسیب‌پذیری‌ها در دو بعد احتمال و تأثیر آن‌ها در جهت تخمین میزان آسیب‌پذیری کمّی و کیفی پرداخت و در مرحله‌ی پایانی با انجام تجزیه و تحلیل اطلاعات، پاسخ سؤالات تحقیق مشخص‌شده و بر اساس اهداف پژوهش، مورد تجزیه‌وتحلیل نهایی قرار گرفت.

## یافته‌های تحقیق

### الف) یافته‌های توصیفی

اطلاعات حاصل از جدول ۴ نشان می‌دهد که ۱۵ نفر پاسخ‌دهندگان دارای سابقه کار تخصصی در حوزه سایبر(فاوا) زیر ۱۵ سال، ۲۰ نفر ۱۵تا ۱۹ سال و ۷ نفر ۲۰ تا ۲۴ سال

بوده‌اند. همان‌طور که مشخص است افراد دارای سابقه کار تخصصی ۱۵تا ۱۹ سال بیش‌ترین و افراد دارای سابقه خدمت ۲۰ تا ۲۴ سال کمترین سهم را از نمونه آماری به خود اختصاص داده‌اند.

**جدول شمارهٔ ۵: توزیع فراوانی پاسخ‌دهندگان بر حسب سابقه کار تخصصی در حوزه سایبر(فاوا)**

| متغیر سنوات خدمت کلی | فراوانی | درصد فراوانی |
|---|---|---|
| زیر ۱۵ سال | ۱۵ | ۳۵,۷ |
| ۱۹-۱۵ سال | ۲۰ | ۴۷,۶ |
| ۲۴ – ۲۰ سال | ۷ | ۱۶,۷ |
| کل | ۴۲ | ۱۰۰ |

به‌منظور آگاهی از وضعیت سطح تحصیلات و سواد افراد جامعه، سطوح تحصیلی نمونه مورد ارزیابی، شامل چهار طیف"کاردانی"، "کارشناسی"،"کارشناسی ارشد"و"دکتری"در نظر گرفته‌شده است. بدین ترتیب اطلاعات حاصل از جدول ۵ نشان می‌دهد، از ۱۴۰ پاسخ‌دهنده، ۲ نفر معادل ۴/۸٪ دارای مدرک کاردانی، ۲۸ نفر معادل ۶۷ ٪ دارای مدرک کارشناسی و۱۱ نفر معادل ۲۶/۲ ٪ دارای مدرک کارشناسی ارشد و ۱ نفر دکترا معادل ۲ ٪ دارای مدرک دکتری بوده‌اند. جدول ۶ توزیع فراوانی پاسخ‌دهندگان بر حسب تحصیلات را نشان می‌دهد.

**جدول شمارهٔ ۶: توزیع فراوانی پاسخ‌دهندگان بر حسب تحصیلات**

| سطح تحصیلات شاخص | کارشناسی | کارشناسی ارشد | دکتری | جمع کل |
|---|---|---|---|---|
| فراوانی | ۳۰ | ۱۱ | ۱ | ۴۲ |
| درصد | ٪۷۱ | ۲۶,۲ | ٪ ۲ | ۱۰۰ |

## یافته‌های کیفی

با استفاده از روش تحلیل محتوا به بررسی ابعاد ارزیابی آسیب‌پذیری سایبری سازمان‌های نظامی در حوزه نرم‌افزاری و کدگذاری مفاهیم و معانی از مصاحبه‌های خبرگان این حوزه پرداخته شد. مجموع آنچه تحت عنوان مؤلفه‌ها و نقاط تمرکز ابعاد الگوی ارزیابی آسیب‌پذیری فضای سایبری در طی جداول تحلیل محتوا به‌دست‌آمده است.کدگذاری در تحلیل محتوا بر اساس مفاهیم و معانی موردنظر و عملیاتی نمودن متغیرها صورت می‌گیرد. بنابراین، محقق به پالایش مفاهیم می‌پردازد و ارتباط موجود میان مفاهیم را به دست می‌آورد و از طریق کدگذاری یا طبقه‌بندی مفاهیم موردنظر، به عملیاتی نمودن بررسی محتوا دست می‌یابد (

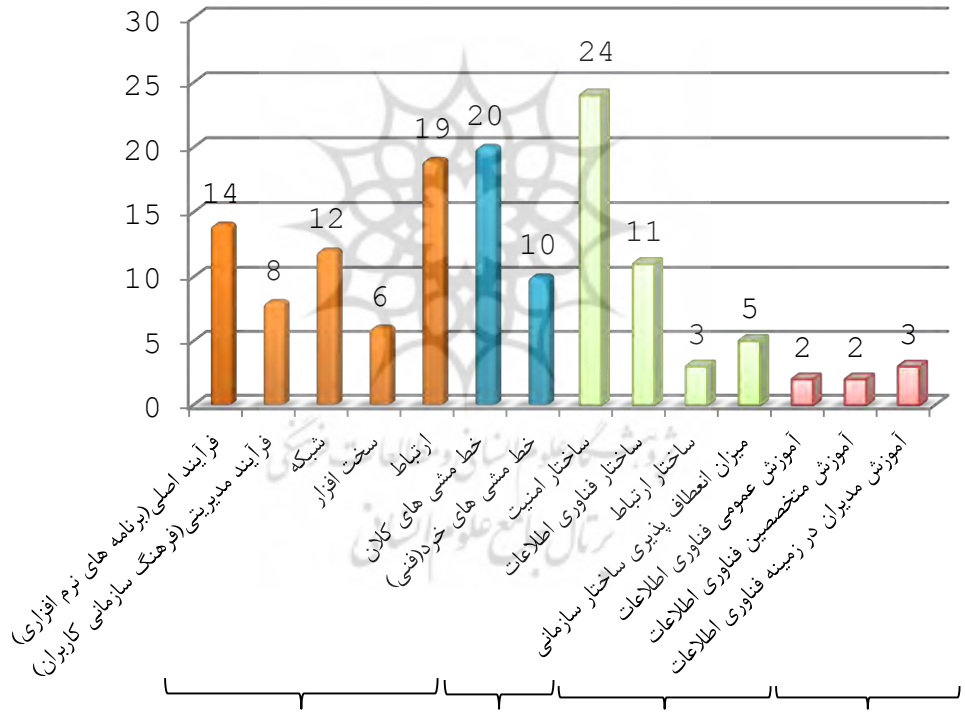
ارل بَبی، ۱۳۸۸). با استفاده از روش تحلیل محتوا به بررسی ابعاد آسیب‌پذیری سایبری سازمان‌های نظامی در حوزه نرم‌افزاری و کدگذاری مفاهیم و معانی از مصاحبه‌های خبرگان این حوزه می‌پردازیم. مجموع آنچه تحت عنوان مؤلفه‌ها و نقاط تمرکز ابعاد الگوی ارزیابی آسیب‌پذیری فضای سایبری در سازمان‌های نظامی در طی جداول تحلیل محتوا به‌دست‌آمده است را می‌توان به‌صورت جداول ذیل و مؤلفه‌های تأکید بر هر کدام از این ابعاد نشان داد:

**جدول شمارهٔ ۷: جدول استخراج و کدگذاری برخی از متغیرها از نکات کلیدی مصاحبه شوندگان**

| نکات کلیدی مصاحبه‌شوندگان | تمرکز متن | مفاهیم | متغیرهای استخراج‌شده | کدگذاری |
|---|---|---|---|---|
| تولید نرم‌افزارها در بخش‌های مختلف بدون هماهنگی با فاوا | ≠ تولید نرم‌افزارهای نامطمئن<br>≠ بخش‌های مختلف | ناهماهنگی در تولید نرم‌افزارها | ≠ امنیت<br>≠ ساختار<br>≠ نرم‌افزار<br>≠ روش‌ها<br>≠ فرهنگ‌سازمانی | ≠ س/۱<br>≠ س/۲<br>≠ ف/۱<br>≠ ر/۲<br>≠ ف/۲ |
| ایجاد شبکه‌های داخلی یگان‌ها بدون در نظر گرفتن مسائل امنیتی و حتی هماهنگی با مبادی ذی‌ربط | ≠ شبکه‌های داخلی نامطمئن<br>≠ عدم وجود امنیت لازم | شبکه‌های داخلی نامطمئن | ≠ شبکه<br>≠ امنیت<br>≠ ساختار<br>≠ فرهنگ‌سازمانی | ≠ ف/۳۱<br>≠ س/۱<br>≠ س/۲<br>≠ ف/۲ |
| استفاده از رایانه‌ها، سخت‌افزار و نرم افزارهای مختلف و بدون هماهنگی | ≠ نرم‌افزارهای نامطمئن | سخت‌افزار و نرم افزارهای نامطمئن | ≠ سخت‌افزار<br>≠ نرم‌افزار<br>≠ فرهنگ‌سازمانی<br>≠ امنیت | ≠ ف/۳۲<br>≠ ف/۱<br>≠ ف/۲<br>≠ س/۱ |
| اعتبارات پشتیبانی از شبکه رایانه‌ای سازمان‌های نظامی بحث مهمی است که عدم‌کفایت آن باعث آسیب‌پذیری در حوزه سایبری خواهد شد. | ≠ کفایت اعتبارات پشتیبانی از شبکه رایانه‌ای | پشتیبانی از شبکه رایانه‌ای | ≠ شبکه<br>≠ خط‌مشی کلان | ≠ ف/۳۱<br>≠ ر/۱ |
| در نظر است که یک مرکز پایش و مانیتورینگ جهت ارتقاء امنیت این فضا ایجاد شود که کل ترافیک شبکه‌ها موردبررسی قرار گیرد و سامانه نرم‌افزاری شبکه کنترل خواهد نمود | ≠ ایجاد مرکز پایش و مانیتورینگ | کنترل سامانه نرم‌افزاری شبکه | ≠ امنیت<br>≠ شبکه<br>≠ نرم‌افزار<br>≠ ساختار فناوری اطلاعات | ≠ س/۱<br>≠ ف/۳۱<br>≠ ف/۱<br>≠ س/۲ |

| نکات کلیدی مصاحبه‌شوندگان | تمرکز متن | مفاهیم | متغیرهای استخراج‌شده | کدگذاری |
|---|---|---|---|---|
| در آن زمان(قبل از پیروزی انقلاب) هدف از به‌کارگیری رایانه در سازمان‌های نظامی مشخص بود : آماد و پرسنلی | ≠ هدف‌گذاری | روش‌ها | ≠ خط‌مشی کلان<br>≠ شبکه<br>≠ ارتباط | ≠ ر/۱<br>≠ ف/۳۱<br>≠ ف/۳۳ |

با کدگذاری متغیرهای استخراج‌شده و دسته‌بندی و شمارش کدها متغیرهای مربوط به هر بعد از تحقیق به بیش‌ترین و کمترین تکرار و تأکید از نظر مصاحبه‌شوندگان پی برده شد. در جدول ۷ فراوانی ابعاد فضای سایبر سازمان‌های نظامی در حوزه نرم‌افزار حاصل از تحلیل محتوای مصاحبه آمده است.




**نمودار شمارهٔ ۱: فراوانی مطلق و نسبی ابعاد استخراج‌شده از مصاحبه با صاحب‌نظران**

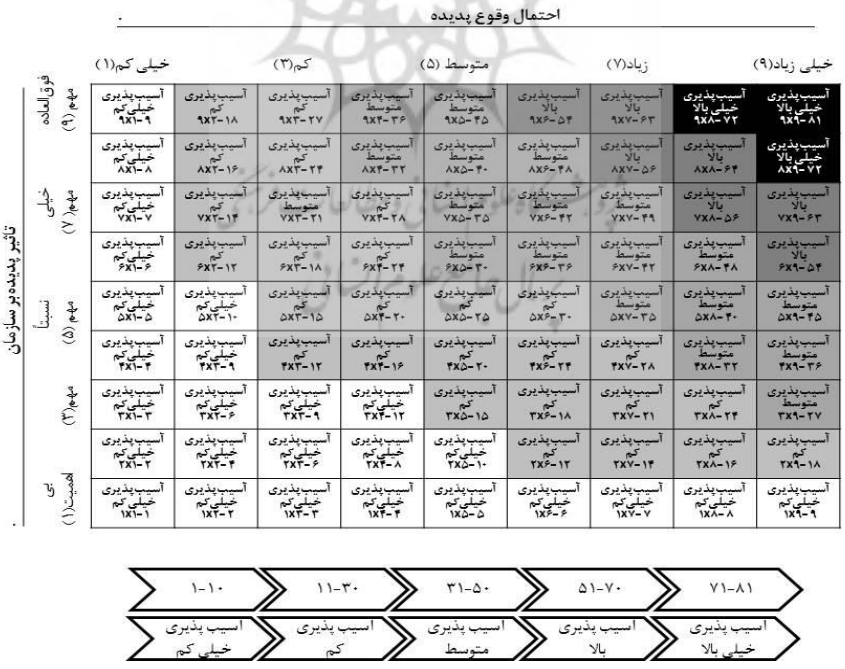
یافته‌های پژوهش حاصل از تحلیل محتوای مصاحبه نشان می‌دهد که بعد فرآیندها به تعداد ۵۹ تکرار دارای بیش‌ترین فراوانی است، ساختار سازمانی با تعداد ۴۳ و روش‌ها به تعداد ۳۰ تکرار در رتبه‌های بعدی قرار دارند. کمترین تعداد تکرار مربوط به بعد آموزش به تعداد

هفت بار است. به‌منظور پاسخگویی به سؤالات پژوهش هر کدام از ابعاد، مؤلفه‌ها و متغیرهای ارزیابی آسیب‌پذیری سایبری در حوزه نرم‌افزاری به‌صورت مجزا تحلیل‌شده و متناسب با نتایج حاصله، میزان آسیب موجود مشخص گردیده است. جهت تصمیم‌گیری درباره میزان تأثیرگذاری هر یک از مؤلفه‌ها بر آسیب‌پذیری سایبری سازمان‌های نظامی در حوزه نرم‌افزاری پژوهشگر بر آن شد تا بر اساس استاندارد محقق ساخته به قضاوت بپردازد. در جدول ۸ مشاهده می‌شود بر اساس استاندارد موردنظر، میانگین یک تا ۱۰ وجود آسیب خیلی بالا، میانگین ۱۱ تا ۳۰ آسیب بالا، میانگین ۳۱ تا ۵۰ آسیب متوسط، میانگین ۵۱ تا ۷۰ آسیب کم و میانگین ۷۱ تا ۷۸ وجود آسیب خیلی کم را نشان می‌دهد. باید به این نکته توجه داشت که در بررسی وضع موجود(میزان آسیب) بین میانگین به‌دست‌آمده و میزان آسیب رابطه معکوس وجود دارد یعنی هرچه میانگین کمتر باشد میزان آسیب در آن متغیر بیشتر است و برعکس.

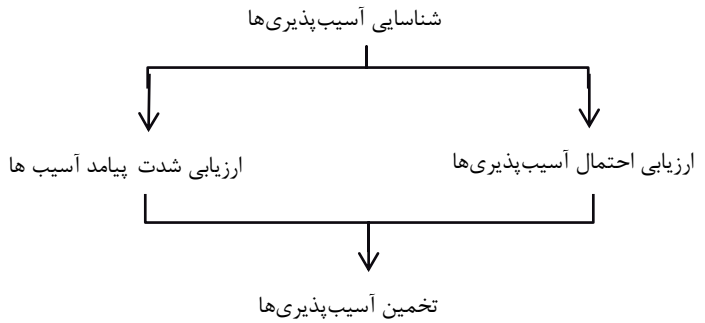
**جدول شمارهٔ ۸: شاخص ارزیابی میزان تأثیرگذاری هر یک از مؤلفه‌های موردبررسی بر آسیب‌پذیری سایبری در حوزه نرم‌افزاری در وضع موجود**

| نوع آسیب | آسیب خیلی بالا | آسیب بالا | آسیب متوسط | آسیب کم | آسیب خیلی‌کم |
|---|---|---|---|---|---|
| | ۱ تا ۱۰ | ۱۱ تا ۳۰ | ۳۱ تا ۵۰ | ۵۱ تا ۷۰ | ۷۱ تا ۸۱ |

**جدول شمارهٔ ۹: شاخص ارزیابی میزان تأثیرگذاری**



## فرایند تخمین آسیب‌پذیری




**شکل شمارهٔ ۲: فرایند تخمین آسیب‌پذیری**

فرمول تخمین آسیب‌پذیری عبارت است از:

تخمین آسیب‌پذیری= احتمال وقوع آسیب‌پذیری × تأثیر آسیب‌پذیری نرم‌افزار

## تحلیل ابعاد الگو

### الف) بعد فرآیند نرم‌افزار

فرآیند نرم‌افزار برای شناسایی کامل، به چهار متغیر مالکیت نرم‌افزارها، پشتیبانی، نگهداری و ارتقای فنی نرم‌افزارها، طراحی، معماری و کدنویسی، رویدادنگاری و ردگیری، تقسیم شد. در ادامه فراوانی و درصد میزان آسیب موجود و احتمال آسیب‌پذیری در آینده و میانگین بعد نرم‌افزار ارائه‌شده است.

**جدول شمارهٔ ۱۰: میانگین، فراوانی و درصد متغیرهای فرآیند نرم‌افزار برای بررسی میزان آسیب موجود**

| متغیر | آسیب خیلی بالا | | آسیب بالا | | آسیب متوسط | | آسیب کم | | آسیب خیلی کم | | میانگین | وضعیت |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | فراوانی | درصد | فراوانی | درصد | فراوانی | درصد | فراوانی | درصد | فراوانی | درصد | | |
| مالکیت نرم‌افزارها | ۸ | ۱۹ | ۲۰ | ۴۷,۶ | ۹ | ۲۱,۴ | ۴ | ۹,۵ | ۱ | ۲,۴ | ۲۶,۶۶ | آسیب بالا |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| پشتیبانی، نگهداری و ارتقا فنی نرم‌افزارها | ۶ | ۱۴,۳ | ۱۷ | ۴۰,۵ | ۱۰ | ۲۳,۸ | ۸ | ۱۹ | ۱ | ۲,۴ | ۳۲,۶۹ | **آسیب متوسط** |
| طراحی، معماری و کدنویسی | ۷ | ۱۶,۷ | ۱۲ | ۲۸,۶ | ۱۶ | ۳۸,۱ | ۵ | ۱۱,۹ | ۲ | ۲,۸ | ۳۲,۱۱ | **آسیب متوسط** |
| رویدادنگاری و ردگیری | ۹ | ۲۱,۴ | ۱۷ | ۴۰,۵ | ۱۳ | ۳۱ | ۳ | ۷,۱ | ۰ | ۰ | ۲۸,۱۱ | **آسیب بالا** |

**جدول شمارهٔ ۱۱: میانگین، فراوانی و درصد متغیرهای فرآیند نرم‌افزار برای بررسی میزان آسیب‌پذیری در آینده**

| متغیر | آسیب‌پذیری خیلی‌کم | | آسیب‌پذیری کم | | آسیب‌پذیری متوسط | | آسیب‌پذیری بالا | | آسیب‌پذیری خیلی بالا | | میانگین | وضعیت |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | فراوانی | درصد | فراوانی | درصد | فراوانی | درصد | فراوانی | درصد | فراوانی | درصد | | |
| مالکیت نرم‌افزارها | ۳ | ۷,۱ | ۲ | ۴,۸ | ۴ | ۳۳,۳ | ۱۱ | ۲۶,۲ | ۱۲ | ۲۸,۶ | ۵۴,۸۵ | آسیب‌پذیری بالا |
| پشتیبانی، نگهداری و ارتقا فنی نرم‌افزارها | ۱ | ۲,۴ | ۴ | ۹,۵ | ۲ | ۲۸,۶ | ۱۰ | ۲۳,۸ | ۱۲ | ۳۵,۷ | ۵۶,۳ | آسیب‌پذیری بالا |
| طراحی، معماری و کدنویسی | ۱ | ۲,۴ | ۳ | ۷,۱ | ۴ | ۳۳,۳ | ۱۲ | ۲۸,۶ | ۱۲ | ۲۸,۶ | ۵۶,۸۸ | آسیب‌پذیری بالا |
| رویدادنگاری و ردگیری | ۱ | ۲,۴ | ۸ | ۱۹ | ۹ | ۲۱,۴ | ۶ | ۱۴,۳ | ۱۸ | ۴۲,۹ | ۵۶,۵۴ | آسیب‌پذیری بالا |

### ب) بعد روش‌های فناوری

بعد روش‌ها دو مؤلفه خط‌مشی‌های کلان و خط‌مشی‌های خرد (فنی) را به خود اختصاص داده است. که هر کدام از مؤلفه‌ها دارای چهار متغیر می‌باشند. فراوانی و درصد میزان آسیب موجود میانگین متغیرها در جدول ۱۲ ارائه‌شده است.

**جدول شمارهٔ ۱۲: میانگین، فراوانی و درصد متغیرهای فرآیند نرم‌افزار برای بررسی میزان آسیب‌پذیری در آینده**

| مؤلفه | متغیر | آسیب خیلی بالا | | آسیب بالا | | آسیب متوسط | | آسیب کم | | آسیب خیلی کم | | میانگین | وضعیت |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | فراوانی | درصد | فراوانی | درصد | فراوانی | درصد | فراوانی | درصد | فراوانی | درصد | | |
| خط‌مشی‌های کلان | راهبردهای فضای سایبر | ۷ | ۱۶,۷ | ۱۵ | ۳۵,۷ | ۱۷ | ۴۰,۵ | ۳ | ۷,۱ | ۰ | ۰ | ۲۹,۵۹ | آسیب بالا |
| | دستورالعمل‌ها در فضای سایبر | ۱۱ | ۲۶,۲ | ۱۴ | ۳۳,۳ | ۱۳ | ۳۱ | ۳ | ۷,۱ | ۱ | ۲,۴ | ۲۷,۳ | آسیب بالا |
| | تدابیر فرماندهان فاوا در فضای سایبر | ۹ | ۲۱,۴ | ۲۰ | ۴۷,۶ | ۸ | ۱۹ | ۳ | ۷,۱ | ۲ | ۴,۸ | ۲۷,۶۱ | آسیب بالا |
| | خط‌مشی فرماندهان استفاده‌کننده از فاوا و یا تأثیرگذار بر فاوا در امر فاوا | ۹ | ۲۱,۴ | ۱۷ | ۴۰,۵ | ۱۲ | ۲۸,۶ | ۲ | ۴,۸ | ۲ | ۴,۸ | ۲۷,۷۱ | آسیب بالا |
| خط‌مشی‌های خرد(فنی) | مدیریت منابع(مانیتورینگ زیرساخت‌ها و تعیین خط و مشی فنی) | ۱۰ | ۲۳,۸ | ۱۵ | ۳۵,۷ | ۱۵ | ۳۵,۷ | ۲ | ۴,۸ | ۰ | ۰ | ۲۶,۵ | آسیب بالا |
| | ورود، تولید و یا گسترش یک سامانه در زیرساخت | ۷ | ۱۶,۷ | ۱۸ | ۴۲,۹ | ۱۵ | ۳۵,۷ | ۲ | ۴,۸ | ۰ | ۰ | ۲۶,۸ | آسیب بالا |
| | تعمیر و نگهداری سامانه | ۸ | ۱۹ | ۱۲ | ۲۸,۶ | ۱۸ | ۴۲,۹ | ۴ | ۹,۵ | ۰ | ۰ | ۲۹,۲۳ | آسیب بالا |
| | مستندسازی هنگام ورود و حین کار | ۱۵ | ۳۵,۷ | ۱۸ | ۴۲,۹ | ۷ | ۱۶,۷ | ۲ | ۴,۸ | ۰ | ۰ | ۲۱,۹ | آسیب بالا |

**جدول شمارهٔ ۱۳: میانگین، فراوانی و درصد متغیرهای روش‌های فناوری برای بررسی میزان آسیب‌پذیری در آینده**

| مؤلفه | متغیر | آسیب‌پذیری خیلی‌کم | | آسیب‌پذیری کم | | آسیب‌پذیری متوسط | | آسیب‌پذیری بالا | | آسیب‌پذیری خیلی بالا | | میانگین | وضعیت |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | فراوانی | درصد | فراوانی | درصد | فراوانی | درصد | فراوانی | درصد | فراوانی | درصد | | |
| خط‌مشی‌های کلان | راهبردهای فضای سایبر در نهاجا | ۱ | ۲,۴ | ۱۰ | ۲۳,۸ | ۱۱ | ۲۶,۲ | ۲۰ | ۴۷,۶ | ۰ | ۰ | ۶۴,۰۴ | آسیب‌پذیری بالا |
| | دستورالعمل‌ها در فضای سایبر | ۱ | ۲,۴ | ۵ | ۱۱,۹ | ۱۵ | ۳۵,۷ | ۱۰ | ۲۳,۸ | ۱۱ | ۲۶,۲ | ۵۳,۲۱ | آسیب‌پذیری بالا |
| | تدابیر فرماندهان فاوا در فضای سایبر | ۱ | ۲,۴ | ۳ | ۷,۱ | ۱۲ | ۲۸,۶ | ۱۰ | ۲۳,۸ | ۱۶ | ۳۸,۱ | ۵۹,۴۵ | آسیب‌پذیری بالا |
| | خط‌مشی فرماندهان استفاده‌کننده از فاوا و یا تأثیرگذار بر فاوا در امر فاوا | ۵ | ۱۱,۹ | ۶ | ۱۴,۳ | ۵ | ۱۱,۹ | ۱۱ | ۲۶,۲ | ۱۵ | ۳۵,۷ | ۵۳,۶۴ | آسیب‌پذیری بالا |
| خط‌مشی‌های خرد(فنی) | مدیریت منابع (مانیتورینگ زیرساخت‌ها و تعیین خط و مشی فنی) | ۱ | ۲,۴ | ۳ | ۷,۱ | ۱۲ | ۲۸,۶ | ۱۵ | ۳۵,۷ | ۱۱ | ۲۶,۲ | ۵۶,۷۸ | آسیب‌پذیری بالا |
| | ورود، تولید و یا گسترش یک سامانه در زیرساخت | ۱ | ۲,۴ | ۷ | ۱۶,۷ | ۱۷ | ۴۰,۵ | ۸ | ۱۹ | ۹ | ۲۱,۴ | ۴۹,۸۳ | آسیب‌پذیری متوسط |
| | تعمیر و نگهداری سامانه | ۱ | ۲,۴ | ۶ | ۱۴,۳ | ۱۴ | ۳۳,۳ | ۱۱ | ۲۶,۲ | ۱۰ | ۲۳,۸ | ۵۳,۱۶ | آسیب‌پذیری بالا |
| | مستندسازی هنگام ورود و حین کار | ۱ | ۲,۴ | ۱۰ | ۲۳,۸ | ۷ | ۱۶,۷ | ۱ | ۱۶,۷ | ۱۷ | ۴۰,۵ | ۵۴,۵۷ | آسیب‌پذیری بالا |

### ج) بعد ساختار سازمانی

بعد ساختار سازمانی چهار مؤلفه ساختار فضای سایبر، ساختار ارتباط، ساختار امنیت و میزان انعطاف‌پذیری ساختار سازمانی را به خود اختصاص داده است. فراوانی و درصد میزان آسیب موجود و میانگین متغیرها در جدول ۱۴ ارائه‌شده است.

**جدول شمارهٔ ۱۴: میانگین، فراوانی و درصد مؤلفه‌های ساختار سازمانی برای بررسی میزان آسیب موجود**

| مؤلفه | آسیب خیلی بالا | | آسیب بالا | | آسیب متوسط | | آسیب کم | | آسیب خیلی کم | | میانگین | وضعیت |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | فراوانی | درصد | فراوانی | درصد | فراوانی | درصد | فراوانی | درصد | فراوانی | درصد | | |
| ساختار امنیت | ۷ | ۱۶,۷ | ۱۳ | ۳۱ | ۱۹ | ۴۵,۲ | ۳ | ۷,۱ | ۰ | ۰ | ۲۹,۸۸ | آسیب بالا |
| ساختار فضای سایبر | ۶ | ۱۴,۳ | ۱۳ | ۳۱ | ۱۷ | ۴۰,۵ | ۵ | ۱۱,۹ | ۱ | ۲,۴ | ۳۱,۸۸ | آسیب متوسط |
| ساختار ارتباط | ۱۰ | ۲۳,۸ | ۱۶ | ۳۸,۱ | ۱۲ | ۲۸,۶ | ۳ | ۷,۱ | ۱ | ۲,۴ | ۲۷,۸۸ | آسیب بالا |
| میزان انعطاف‌پذیری ساختار سازمانی | ۱۷ | ۴۰,۵ | ۱۷ | ۴۰,۵ | ۷ | ۱۶,۷ | ۱ | ۲,۴ | ۰ | ۰ | ۱۹,۸۸ | آسیب بالا |

**جدول شمارهٔ ۱۵: میانگین، فراوانی و درصد مؤلفه‌های ساختار سازمانی برای بررسی میزان آسیب‌پذیری در آینده**

| مؤلفه | آسیب‌پذیری خیلی کم | | آسیب‌پذیری کم | | آسیب‌پذیری متوسط | | آسیب‌پذیری بالا | | آسیب‌پذیری خیلی بالا | | میانگین | وضعیت |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | فراوانی | درصد | فراوانی | درصد | فراوانی | درصد | فراوانی | درصد | فراوانی | درصد | | |
| ساختار امنیت | ۱ | ۲,۴ | ۳ | ۷,۱ | ۶ | ۱۴,۳ | ۱۲ | ۲۸,۶ | ۲۰ | ۴۷,۶ | ۶۳,۶۱ | آسیب‌پذیری بالا |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ساختار فضای سایبر | ۲ | ۴,۸ | ۴ | ۹,۵ | ۵ | ۱۱,۹ | ۱۳ | ۳۱ | ۱۸ | ۴۲,۹ | ۶۰,۳۵ | آسیب‌پذیری بالا |
| ساختار ارتباط | ۱ | ۲,۴ | ۰ | ۰ | ۴ | ۹,۵ | ۹ | ۲۱,۴ | ۲۸ | ۶۶,۷ | ۷۰,۰۲ | آسیب‌پذیری خیلی بالا |
| میزان انعطاف‌پذیری ساختار | ۱ | ۲,۴ | ۵ | ۱۱,۹ | ۹ | ۲۱,۴ | ۹ | ۲۱,۴ | ۱۸ | ۴۲,۹ | ۶۰,۱۱ | آسیب‌پذیری بالا |

## د) یافته‌های بعد آموزش

بعد آموزش سه مؤلفه آموزش عمومی، آموزش متخصصین و آموزش مدیران را به خود اختصاص داده است. دو مؤلفه اول این بعد هر کدام سه متغیر و مؤلفه سوم شامل دو متغیر است. در ادامه فراوانی و درصد میزان آسیب موجود و میانگین متغیرها ارائه‌شده است.

**جدول شمارهٔ ۱۶: میانگین، فراوانی و درصد متغیرهای آموزش برای بررسی میزان آسیب موجود**

| مؤلفه | متغیر | آسیب خیلی بالا | | آسیب بالا | | آسیب متوسط | | آسیب کم | | آسیب خیلی‌کم | | میانگین | وضعیت موجود |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | فراوانی | درصد | فراوانی | درصد | فراوانی | درصد | فراوانی | درصد | فراوانی | درصد | | |
| آموزش عمومی فضای سایبر | التزام به داشتن اطلاعات اولیه در بدو استخدام یا هنگام ارائه مدرک علمی بالاتر | ۲۵ | ۵۹,۵ | ۱۱ | ۲۶,۲ | ۶ | ۱۴,۳ | ۰ | ۰ | ۰ | ۰ | ۱۳,۹۵ | آسیب بالا |
| | آموزش اولیه در بدو خدمت | ۹ | ۲۱,۴ | ۱۸ | ۴۲,۹ | ۱۴ | ۳۳,۳ | ۱ | ۲,۴ | ۰ | ۰ | ۲۳,۱ | آسیب بالا |
| | آموزش حین خدمت | ۱۲ | ۲۸,۶ | ۱۶ | ۳۸,۱ | ۱۲ | ۲۸,۶ | ۱ | ۲,۴ | ۱ | ۲,۴ | ۲۵,۴ | آسیب بالا |
| آموزش متخصصین | التزام به داشتن اطلاعات اولیه در بدو استخدام یا هنگام ارائه مدرک علمی بالاتر | ۱۶ | ۳۸,۱ | ۱۴ | ۳۳,۳ | ۱۰ | ۲۳,۸ | ۲ | ۴,۸ | ۰ | ۰ | ۲۱,۰۴ | آسیب بالا |
| | آموزش اولیه در بدو استخدام | ۱۰ | ۲۳,۸ | ۱۵ | ۳۵,۷ | ۱۵ | ۳۵,۷ | ۱ | ۲,۴ | ۱ | ۲,۴ | ۲۷,۰۹ | آسیب بالا |
| | تداوم آموزش‌های تخصصی | ۹ | ۲۱,۴ | ۱۹ | ۴۵,۲ | ۱۱ | ۲۶,۲ | ۲ | ۴,۸ | ۱ | ۲,۴ | ۲۷,۹ | آسیب بالا |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| آموزش مدیران | آشنایی مدیران با کلیات فناوری‌های موجود در سازمان و مسائل و مشکلات و مزایا و معایب آن‌ها | ۶ | ۱۴,۳ | ۲۰ | ۴۷,۶ | ۱۵ | ۳۵,۷ | ۱ | ۲,۴ | ۰ | ۰ | ۲۶,۷ | آسیب بالا |
| | آشنایی مدیران با فناوری‌های جدید و روز دنیا و کشور و مزایا و معایب آن‌ها در تأمین و پیشبرد اهداف سازمان | ۱۱ | ۲۶,۲ | ۱۵ | ۳۵,۷ | ۱۲ | ۲۸,۶ | ۳ | ۷,۱ | ۱ | ۲,۴ | ۲۵,۶ | آسیب بالا |

**جدول شمارهٔ ۱۷: میانگین، فراوانی و درصد متغیرهای آموزش برای بررسی میزان آسیب‌پذیری در آینده**

| مؤلفه | متغیر | آسیب‌پذیری خیلی کم | | آسیب‌پذیری کم | | آسیب‌پذیری متوسط | | آسیب‌پذیری بالا | | آسیب‌پذیری خیلی بالا | | میانگین | وضعیت آسیب‌پذیری |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | فراوانی | درصد | فراوانی | درصد | فراوانی | درصد | فراوانی | درصد | فراوانی | درصد | | |
| آموزش عمومی فضای سایبر | التزام به داشتن اطلاعات اولیه در بدو استخدام یا هنگام ارائه مدرک علمی بالاتر | ۱۲ | ۲۸,۶ | ۱۴ | ۳۳,۳ | ۷ | ۱۶,۷ | ۶ | ۱۴,۳ | ۳ | ۷,۱ | ۲۹,۹ | خیلی کم |
| | آموزش اولیه در بدو خدمت | ۱ | ۲,۴ | ۸ | ۱۹ | ۱۸ | ۴۲,۹ | ۹ | ۲۱,۴ | ۶ | ۱۴,۳ | ۴۴,۸ | متوسط |
| | آموزش حین خدمت | ۱ | ۲,۴ | ۲ | ۴,۸ | ۱۳ | ۳۱ | ۸ | ۱۹ | ۸ | ۴۲,۹ | ۵۸,۹ | بالا |
| متخصصین | التزام به داشتن اطلاعات اولیه در بدو استخدام یا هنگام ارائه مدرک علمی بالاتر | ۸ | ۱۹ | ۶ | ۱۴,۳ | ۱۴ | ۳۳,۳ | ۱۰ | ۲۳,۸ | ۴ | ۹,۵ | ۳۹,۵ | متوسط |
| | آموزش اولیه در بدو استخدام | ۱ | ۲,۴ | ۷ | ۱۶,۷ | ۲۰ | ۴۷,۶ | ۳ | ۷,۱ | ۱۱ | ۲۶,۲ | ۴۹,۸ | متوسط |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | تداوم آموزش‌های تخصصی | ۲ | ۴,۸ | ۱ | ۲,۴ | ۱۰ | ۲۳,۸ | ۶ | ۱۴,۳ | ۲۳ | ۵۴,۸ | ۶۳,۳ | بالا |
| مدیران | آشنایی مدیران با کلیات فناوری‌های موجود در سازمان و مسائل و مشکلات و مزایا و معایب آن‌ها | ۱ | ۲,۴ | ۳ | ۷,۱ | ۵ | ۱۱,۹ | ۱۵ | ۳۵,۷ | ۱۸ | ۴۲,۹ | ۶۳,۱ | بالا |
| | آشنایی مدیران با فناوری‌های جدید و روز دنیا و کشور و مزایا و معایب آن‌ها در تأمین و پیشبرد اهداف سازمان | ۱ | ۲,۴ | ۳ | ۷,۱ | ۷ | ۱۶,۷ | ۱۲ | ۲۸,۶ | ۱۹ | ۴۵,۲ | ۶۲,۵ | بالا |

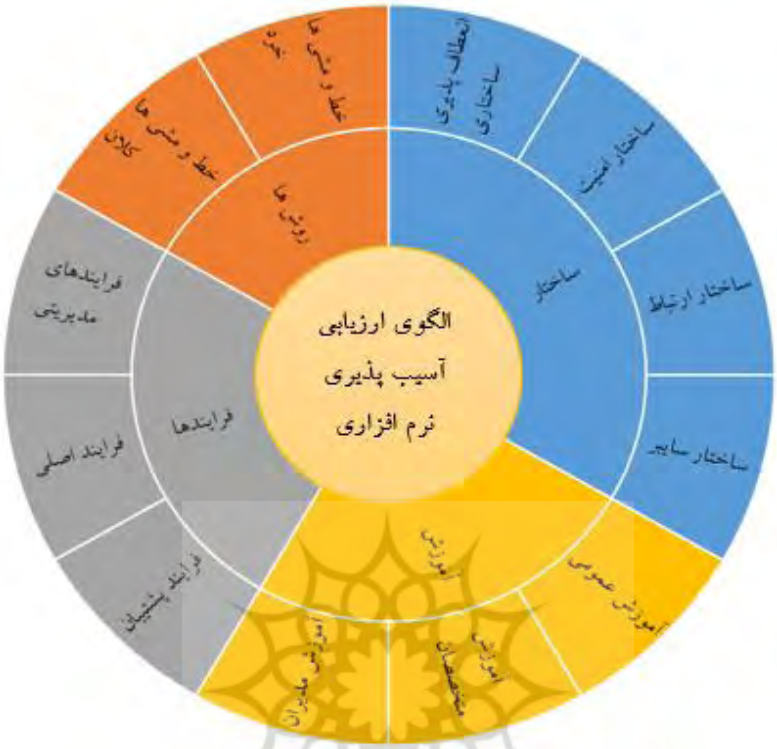
## بحث و نتیجه‌گیری

بر اساس مفاهیم حاصل از مطالعه منابع تحقیق، مقولات به‌دست‌آمده از تحلیل محتوای مصاحبه با صاحب‌نظران و همچنین نتایج تحقیقات پیشین مرتبط با موضوع آسیب‌پذیری نرم‌افزارهای نهاجا در فضای سایبری، به پرسش‌های تحقیق پاسخ داده شد.

در راستای پاسخ به سؤال اول و دوم در زمینهٔ آسیب‌پذیری نرم‌افزاری نهاجا و ابعاد و مؤلفه‌های آن، چهار بعد زیر به عنوان زمینه‌های آسیب‌پذیری نرم‌افزاری نهاجا شناسایی گردید. این یافته‌ها با نتایج سایر پژوهشگران (داد[1]، ۲۰۱۱: ۱۵) در زمینهٔ انواع آسیب‌پذیری‌های نرم‌افزاری مطابقت دارد.

- ✓ فرآیند
- ✓ روش‌ها
- ✓ ساختار
- ✓ آموزش

۱. Dod




**شکل شمارهٔ ۳: ابعاد و مؤلفه‌های الگوی ارزیابی آسیب‌پذیری نرم‌افزاری سازمان‌های نظامی**

نتایج حاصله از یافته‌های تحلیل یافته‌ها در راستای اهداف تحقیق را می‌توان به‌صورت زیر بیان نمود: فرآیند فضای سایبر در حوزه نرم‌افزار با تأکید ۵۹ موردی بیش‌ترین توجه صاحب‌نظران را به خود جلب نموده است که نشان می‌دهد این بعد هم می‌تواند دارای آسیب در شرایط کنونی بوده و هم در آینده دارای بیش‌ترین آسیب‌پذیری باشد. در بعد فرآیندها بیش‌ترین توجه معطوف متغیر امنیت با ۱۹ مورد تأکید در فرآیندهای پشتیبان است که مسلماً نشان از آسیب‌پذیری آن دارد و در برنامه‌ریزی‌های می‌بایست موردتوجه قرار گیرد. متغیر ساختار سازمانی امنیت با ۲۴ مورد تأکید در بعد ساختار از سوی صاحب‌نظران نیز بیش‌ترین توجه را در کل متغیرها به خود جلب کرده است.

نتیجه حاصل اینکه ساختار موجود امنیت سایبری سازمان‌های نظامی متناسب با رشد فناوری و انتقال آن به این سازمان‌ها نیست و این خود زمینه‌ساز آسیب‌پذیری شده است.

آموزش کمترین تأکید را از نظر صاحب‌نظران با تکرار متوسط دو مورد داشته است. نتیجه‌ای که می‌توان گرفت این است که آن‌ها معتقد به آسیب‌پذیری در این بعد نیستند.

**توصیه برای پژوهش‌های بعدی**

۱) ارائه راهبردهای پدافند غیرعامل در پیشگیری از آسیب‌پذیری‌های فاوا در آجا.

۲) بررسی نقش عامل انسانی در آسیب‌پذیری سیستم‌های رایانه‌ای در سازمان‌های نظامی

۳) بررسی آسیب‌پذیری‌های بهره‌برداری از زیرساخت فناوری‌های غیربومی در شبکه‌های رایانه‌ای آجا.

**محدودیت‌های تحقیق**

۱) کمبود متخصصان و خبرگان آشنا به ابعاد فضای سایبر.

۲) عدم امکان الگوگیری از تحقیقات انجام‌گرفته در سازمان‌های دیگر به خاطر متفاوت بودن جایگاه فناوری اطلاعات در سازمان‌های نظامی.

**پیشنهادها**

۱) معاونت فاوا نهاجا با هماهنگی معاونت فاوا آجا یک سند جامع جهت فضا سایبر نهاجا را تهیه نماید.

۲) معاونت فاوا بر اساس سند جامع با هماهنگی فرماندهی آماد و پشتیبانی نهاجا، مرکز خدمات فناوری اطلاعات و فرماندهی گروه فاوا نهاجا زیرساخت‌های و نیازمندی‌های لازم را مشخص و جهت اجرا اعلام نمایند.

۳) معاونت طرح و برنامه نهاجا با هماهنگی با معاونت طرح و برنامه و بودجه آجا در خصوص تسریع در تهیه راهبردها و برنامه‌های اجرایی فضای سایبر اقدام نماید.

۴) معاونت تربیت و آموزش نهاجا با همراهی معاونت فاوا، دوره‌ها و سرفصل‌های آموزشی موردنیاز و به‌روز را تعیین و جهت اجرا به مبادی زی ربط اعلام نمایند.

**فهرست منابع:**

اصلانی، مصطفی، سایبر، *جنگ اطلاعات و آینده*، همایش سراسری سرباز آینده، تهران، ۱۳۸۸.

اصلانی، مصطفی، *هدایت شبکه پنهان در فضای سایبر*، همایش سراسری، تهران،۱۳۹۱.

آقایی، محسن. معینی. علی.(۱۳۹۷). ارائه مدل مفهومی منطقی طبقه بندی تهدیدات سایبری زیرساخت های حیاتی. فصلنامه امنیت ملی. سال نهم. شماره دوم. تابستان ۹۸.

امیدیان، علیرضا، *رده‌بندی و مدل‌سازی آسیب‌پذیری‌های شناخته‌شده شبکه‌های رایانه‌ای*، پایان‌نامه کارشناسی ارشد، گرایش نرم‌افزار، دانشگاه صنعتی شریف، دانشکده مهندسی رایانه، تهران، ۱۳۸۴.

*آینده‌پژوهی، مفاهیم و روش‌ها*، موسسه آموزشی و تحقیقاتی صنایع دفاعی، تهران، ۱۳۸۸.

بلومنتال، مار جوری، کلارک، دیوید، کرامر، در*آینده‌ی اینترنت و جنگ سایبری*، ۲۰۰۸.

پل، دیوید. *درآمدی بر فرهنگ سایبر(۲۰۰۱)*. ترجمه مسعود کوثری. حسین حسنی. چاپ اول انتشارات جامعه شناسان ۱۳۸۹.

حافظنیا، محمدرضا، *مقدمه‌ای بر روش تحقیق در علوم انسانی*، انتشارات سمت، تهران، ۱۳۸۰.

خلج، رضا، باصفا، مهدی، *شناخت آسیب‌پذیری‌ها و امنیت شبکه*، واحد مجازی دانشگاه آزاد اسلامی، ۱۳۹۰.

خلیلی شَورَینی، سیاوش، *روش‌های تحقیق در علوم انسانی*، انتشارات یادوارهٔ کتاب، تهران، ۱۳۸۶.

ذوقی، محمودرضا، "*حمله هکرها*"، انتشارات سیمین دخت، تهران، ۱۳۸۱.

سازمان پدافند غیرعامل کشور، مرکز پدافند غیرعامل، پدافند غیرعامل- *پایگاه دانش مخاطرات امنیتی* ICT، تهران، ۱۳۸۷.

سازمان پدافند غیرعامل کشور، مرکز پدافند غیرعامل، پدافند غیرعامل- *تیم پاسخگویی به رویداد امنیتی رایانه*، تهران، ۱۳۸۷.

شاپوری، مهدی، باقری، اکرم، *عصر اطلاعات و تحول مفاهیم جنگ و امنیت در روابط بین‌الملل، چگونه دفاع کنیم*، نخستین همایش دفاع سایبری، تهران،۱۳۹۰.

کیلکرس، جورجیا و همکاران، *مدل‌های سازمانی برای پاسخگویی به حوادث رایانه‌ای*، ترجمه رضا انتظار شبستری، حسن‌زاده جعفر زاده جعفر اسدی، امیر صمدی، انستیتو ایز ایران، ۱۳۹۰.

فریدون زاده، یوسف، *تهدیدهای جامعه سایبر و روش‌های امن سازی و دفاع در برابر این تهدیدها*، نخستین همایش ملی دفاع سایبری، تهران، ۱۳۹۰.

قوچانی خراسانی. محمد مهدی. جسین پور. داود (۱۳۹۶). جاکمیت شبکه ای در نهادهای پژوهشی امنیت سایبری. دانشکده مدیریت و حسابداری دانشگاه علامه طباطبایی. فرایند مدیریت توسعه. دوره ۳۰، شماره ۱.

مشهدی، حسن. امینی، سعید. تدوین و ارائه الکوی ارزیابی تهدیدات، آسیب‌پذیریو تحلیل خطر پذیری زیرساخت های خیاتی با تاکید بر پدافند غیر عامل. دوفصلنامه مدیریت بحران. بهر و تابستان ۱۳۹۴.

محمدی،محمود، سلیمانی فر، اکبر و همکاران، *تکنولوژی‌های نو در حوزه الکترونیک (نقش فناوری اطلاعات در جنگ‌های آینده)*،تهران، ۱۳۸۱.

محمودزاده، ابراهیم. اسماعیلی، کیوان. الگوی راهبردی صیانت امنیتی فضای سایبری نیروهای مسلح. فصلنامه امنیت ملی. سال هشتم، شماره سی ام. زمستان ۱۳۹۷.

مؤسسه‌ی آموزشی و تحقیقاتی صنایع دفاعی، مرکز آینده‌پژوهی علوم و فناوری دفاعی، *رهنگاشت علم و فناوری*، تهران، ۱۳۸۸.

وزارت ارتباطات و فناوری اطلاعات، موسسه توسعه و گسترش افتا، سازمان فناوری اطلاعات ایران، *کتاب سال افتا(مرجع حوزه امنیت فضای تولید و تبادل اطلاعات)*، تهران، دوره اول، ۱۳۹۰.

Al-khawaldeh. Igried. Hssan Al. Washat. Bashar Igried. (۲۰۱۹). Risk and Vulnerability analyses for the protection of information for future communication security Based Neural networks.. Journal of advanced Science and engineering technologies.

Ammann. Paul. Wijesekera .Duminda. Kaushis. Sakket. (۲۰۰۲). Scalable, Graph-Based Network Vulnerability Analysis. Computer security Conference

Bishop. Matt. (۲۰۰۳). Computer security': art and scince. Boston, Mass, London : Addison- Wesley.

Cresweel , ۲۰۰۳, Cresswell , pallano , Gatman, Halson۲۰۰۳, tashakori & teddi,۱۹۹۸)

FEMA(۲۰۰۳), Risk Management Series, Risk asscessment FEMA ۴۲۶. WWW.fema.gov.

GibsonWilliam,۱۹۸۴, Neuromancer, US : Ace Book.

Dod, (۲۰۱۱), Department of Defence Strategy for Operating in Cyberspace, http://www.defence.gov.

O.H.Alhazmi, Y.K.Malaiya, and I.Ray, "Measuring, analyzing and predicting security vulnerabilities in software systems," computers & security, ۲۰۰۷,۴.Ghassan Kbar, "Security Risk Analysis based on probability of system failure, attacks andVulnerabilities," ۲۰۰۹.

Ramakrishnan, C.R., Sekar, R.: Model-Based Vulnerability Analysis of Computer Systems. In: Proceedings of the Second International Workshop on Verification, Model Checking and Abstract Interpretation (۱۹۹۸)

S. Liu, R. Kuhn, H. Rossmn, "Surviving Insecure IT: Effective Patch Management." Published by the IEEE Computer Society, ۲۰۰۹