تهدیدات سایبری علیه سیستم‌های سلامت در ایران: تحلیل جامع و ارائه راهکارهای کاهش

علیرضا سیفی[۱]، فریدخت یزدانی*[۲]

۱-دانشجوی کارشناسی ارشد پرستاری، مرکز تحقیقات توسعه علوم پرستاری و مامایی، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، ایران

۲-استادیار گروه پرستاری، مرکز تحقیقات توسعه علوم پرستاری و مامایی، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران

نویسنده مسئول: Email:faridokht.yazdani@yahoo.com

چکیده

حوزه سلامت در ایران با دیجیتالی شدن فزاینده خود، به هدفی جذاب برای حملات سایبری تبدیل شده است. هدف از این مطالعه بررسی چالش‌های موجود در زمینه امنیت سایبری داده‌های سلامت و ارائه راهکارهایی برای حفاظت موثر از این اطلاعات حساس می‌باشد. نتایج نشان می‌دهد که حملات باج‌افزاری، فیشینگ و نشت اطلاعات حساس از جمله تهدیدات اصلی هستند که به دلیل ضعف زیرساخت‌های امنیتی، کمبود نیروی متخصص و نبود یک رویکرد جامع و هماهنگ تشدید می‌شوند. یافته‌های این پژوهش همچنین به شناسایی یک نوع جدید از حمله باج‌افزاری اشاره می‌کند که به طور خاص سیستم‌های تصویربرداری پزشکی را هدف قرار می‌دهد. برای بهبود وضعیت، سرمایه‌گذاری در زیرساخت‌های امنیتی، آموزش نیروی انسانی، تدوین قوانین جامع و تقویت همکاری بین‌بخشی ضروری است. ایجاد یک مرکز تخصصی امنیت سایبری در حوزه سلامت نیز می‌تواند به عنوان یک نهاد هماهنگ‌کننده و پشتیبان عمل کند. با این حال، تحقیقات بیشتری برای ارزیابی اثربخشی راهکارهای پیشنهادی و توسعه مدل‌های پیش‌بینی حملات مورد نیاز است.

کلیدواژه‌ها: امنیت سایبری، مراکز بهداشتی، ارزیابی ریسک، امنیت داده‌ها.

مقدمه

در دنیای دیجیتالی امروز، سیستم‌های سلامت نه تنها مراکز ارائه خدمات درمانی، بلکه اهداف اصلی حملات سایبری نیز هستند. این حملات، تهدیدی جدی برای سلامت بیماران، حریم خصوصی اطلاعات و تداوم ارائه خدمات درمانی به شمار می‌رود [۱]. براساس گزارشات اخیر سازمان جهانی بهداشت، این تهدیدات به طور چشمگیری افزایش یافته و خسارات مالی هنگفتی را به بار آورده است [۲]. این روند رو به رشد، به ویژه در ایران که با پیچیدگی سیستم‌های اطلاعاتی در حوزه سلامت، کمبود نیروی متخصص و تحریم‌های بین‌المللی مواجه است، چالش‌های منحصر به فردی را ایجاد کرده است.

رویدادهایی مانند حمله باج‌افزار WannaCry که صدها بیمارستان را در سراسر جهان تحت تأثیر قرار داد [۳]، به خوبی نشان می‌دهد که زیرساخت‌های حیاتی مانند سیستم‌های سلامت، چقدر در برابر این تهدیدات آسیب‌پذیر هستند. ایران نیز از این قاعده مستثنی نبوده و در سال‌های اخیر شاهد حملات سایبری متعددی به سیستم‌های بهداشتی خود بوده است. بدافزارهایی مانند Stuxnet، Gauss و Flame که به طور خاص برای هدف قرار دادن زیرساخت‌های صنعتی و حیاتی طراحی شده بودند، نمونه‌هایی از این تهدیدات هستند[۴].

داده‌های سلامت به عنوان یکی از حساس‌ترین اطلاعات، همواره در معرض تهدیدات سایبری قرار دارند؛ و مهاجمان سایبری با هدف کسب سود مالی، اخاذی، یا ایجاد اختلال در زیرساخت‌های حیاتی، به دنبال دسترسی به این داده‌های حساس هستند. این حملات، علاوه بر اختلال در ارائه خدمات درمانی، منجر به افشای اطلاعات حساس بیماران و بروز خسارات مالی قابل توجهی شده‌اند. مطالعات نشان می‌دهد که منطقه خاورمیانه به دلیل اهمیت ژئوپلیتیکی و وابستگی روزافزون به فناوری‌های نوین، یکی از اهداف اصلی حملات سایبری است.

با توجه به اهمیت روزافزون امنیت اطلاعات در حوزه سلامت و افزایش حملات سایبری، هدف این مطالعه، شناسایی نقاط ضعف و آسیب‌پذیری‌های سیستم‌های سلامت در برابر این تهدیدات، تحلیل ریشه‌های مسئله و ارائه راهکارهای جامع و عملی برای تقویت امنیت سایبری در این حوزه است. این پژوهش به دنبال ارائه راهکارهایی است که بتواند به طور موثر از سیستم‌های سلامت در برابر حملات سایبری محافظت کند. نتایج این پژوهش می‌تواند به عنوان یک نقشه راه برای ارتقای امنیت سایبری در نظام سلامت ایران و سایر کشورها مورد استفاده قرار گیرد.

روش شناسی

در این مطالعه مروری روایتی، از پایگاه‌های اطلاعاتی معتبرScopus ، PubMedو Google Scholar و برخی منابع خبری برای جستجوی مقالات استفاده شد. کلمات کلیدی مرتبط با موضوع مانند «امنیت سایبری»، «حوزه سلامت»، «ایران»، «مرور سیستماتیک» «تهدیدات سایبری» به همراه ترکیبات مختلف آن‌ها در جستجوها مورد استفاده قرار گرفت. محدوده زمانی جستجو از سال ۲۰۰۰ تا ۲۰۲۴ در نظر گرفته شد تا به روزترین پژوهش‌ها در این زمینه مورد بررسی قرار گیرند. برای انتخاب مقالات مورد مطالعه، معیارهای ورود و خروج مشخصی در نظر گرفته شد. مقالاتی که به طور مستقیم به موضوع امنیت سایبری در حوزه سلامت ایران پرداخته و روش‌شناسی مشخصی برای بررسی موضوع داشته باشند، وارد مطالعه شدند. همچنین، مقالاتی که به زبان فارسی یا انگلیسی منتشر شده و چکیده یا متن کامل آن‌ها در دسترس بود، در این مطالعه مورد بررسی قرار گرفتند. برای استخراج اطلاعات از مقالات، از یک فرم استاندارد استفاده شد. اطلاعاتی مانند عنوان مقاله، نویسندگان، سال انتشار، هدف، و یافته‌های اصلی در این فرم ثبت شد. برای تحلیل داده‌ها. داده‌های استخراج شده و مشابه گروه‌بندی شدند. در نهایت، نتایج به صورت توصیفی و با استفاده از نقل قول از مقالات ارائه شد.

یافته ها

یافته‌های این پژوهش، با تکیه بر داده‌های ارائه شده در جدول ۱، حاکی از آن است که وضعیت امنیت سایبری در حوزه سلامت ایران نسبت به کشورهای توسعه‌یافته در سطح پایین‌تری قرار دارد. به ویژه، ضعف در زیرساخت‌های امنیتی و آگاهی کارکنان از جمله چالش‌های اصلی در این حوزه شناسایی شده است. تحلیل روند تغییرات تهدیدات نشان می‌دهد که حملات

سایبری به سمت پیچیدگی و هدفمندی بیشتری حرکت کرده‌اند، به‌طوری‌که حملات باج‌افزاری و فیشینگ به عنوان دو تهدید غالب در این حوزه مطرح هستند.

جدول ۱- وضعیت امنیت سایبری در حوزه سلامت ایران در مقایسه با برخی کشورهای توسعه‌یافته

عنوان مقاله	نویسندگان	سال	هدف	محیط	نتایج
تهدیدات سایبری و تأثیر آن بر امنیت ملی	علی خلیلی‌پور، یاسر نورعلی وند	۱۳۹۱	تهدیدهای سایبری چگونه بر امنیت ملی تأثیر می‌گذارند و این اثرگذاری در چه ابعادی خود را نمایان می‌سازد.	فضای سایبری	ویژگیهای فضای سایبری همچون قیمت پایین ورود، گمنامی، آسیب‌پذیری و نامتقارنبودن، پدیده انتشار قدرت را به وجود آورده است، بدین معنی که اگر تا کنون دولتها بازی قدرت را تنها میان خود تقسیم کرده بودند، از این پس باید آن را با بازیگران دیگری همچون شرکتهای خصوصی، گروههای سازمانیافته تروریستی و جنایی و افراد تقسیم نمایند، اگر چه هنوز این دولتها هستند که در این عرصه نقش مهمی را بازی میکنند. به طبع، این پدیده امنیت ملی دولتها را از تأثیرگذاری خود بینصیب نخواهد گذاشت
ارائه روشی برای شناسایی وب‌سایت فیشینگ سرویس پرداخت اینترنتی	غلامرضا شاه محمدی، سلمان کمالی زاده	۱۳۹۵	ارائه روشی جدید برای شناسایی وبسایت فیشینگ در بانکداری اینترنتی است	وب سایت های قانونی	روش پیشنهادی، وب سایت های قانونی را فیشینگ تلقی نمیکند
بررسی حملات کانال جانبی حافظه نهان بر روی پیاده سازی الگوریتم رمزAES	محمد جدیدی، مهدی اصفهانی	۱۳۹۹	مرور انواع حملات حافظه نهان روی پیاده‌سازی الگوریتم رمز AES	پردازنده ها	حملات کانال جانبی زمان مبتنی بر حافظه نهان کاربردی می باشد و تهدیدی جدی و عملی علیه سامانه های امنیتی است.

تهدیدهای سایبری و اقدامات امنیتی در فضای مجازی؛ بررسی رویکردهای ایالات متحده آمریکا و جمهوری اسلامی ایران	آرمین امینی، محمد کاظم صیاد	۱۳۹۹	بررسی راهبردها و رویکردهای دو کشور ایران و آمریکا و همچنین کشف نقاط ضعف و یا کاستی‌های موجود در حوزه امنیت سایبری با توجه به تهدیدات موجود در فضای مجازی.	حوزه امنیت سایبری	متخصصان فضای سایبری در ایران به شناسایی تهدیدهای سایبری از پیش توجه کمتری داشته و در نتیجه در حوزه امنیت ملی، به‌رغم فعالیت‌ها و تدابیر خوب اندیشیده‌شده پیشین، راهکارهای مقابله با تهدیدهای سایبری با توجه به روند تهدیدات باید به‌روزرسانی‌شده و تدابیر جدیدی اتخاذ شود.
ارائه یک چارچوب مفهومی برای ارزیابی پُرمایگی و آموزش آگاهی از امنیت اطلاعات کاربران	محمد حسن زاده، نرگس جهانگیری	۱۳۹۹	ایجاد یک چارچوب جامع برای کمک به سازمان‌ها و افراد در ارزیابی سطح امنیت اطلاعات و اتخاذ اقدامات مناسب برای بهبود آن.	جوزه اطلاعات سازمانی	آموزش امنیت اطلاعات ضرورت دارد. در برنامه ریزی آموزش امنیت اطلاعات به کارکنان بایستی درجه سازمانی, رشته تحصیلی و رده شغلی آنها مورد توجه قرار بگیرد تا آموزش ها بتواند موثر واقع شوند.

به طور خلاصه، می توان نتایج حاصل از بررسی وضعیت امنیت سایبری در حوزه سلامت ایران را به صورت زیر دسته بندی نمود.

الف) یافته‌های کلی:

تحلیل جامع داده‌ها نشان می‌دهد که وضعیت امنیت سایبری در حوزه سلامت ایران، علی‌رغم تلاش‌های صورت گرفته، همچنان با چالش‌های جدی مواجه است.

- **وضعیت کلی امنیت سایبری:** بر اساس شاخص جهانی امنیت سایبری(GCI)، ایران در رتبه‌ای متوسط قرار دارد و در مقایسه با برخی کشورهای پیشرو در حوزه فناوری اطلاعات، ضعف‌هایی در زیرساخت‌های امنیتی و آگاهی عمومی از تهدیدات سایبری مشاهده می‌شود [۵].
- **تهدیدات اصلی:** اصلی‌ترین تهدیدات سایبری که حوزه سلامت ایران را تهدید می‌کنند عبارتند از:
  - **حملات باج‌افزاری:** این نوع حملات با رمزگذاری داده‌ها و درخواست باج برای بازگرداندن آن‌ها، به یکی از جدی‌ترین تهدیدات برای بیمارستان‌ها و مراکز درمانی تبدیل شده است [۶].
  - **فیشینگ:** مهندسی اجتماعی و فریب کاربران برای افشای اطلاعات حساس از طریق ایمیل‌های جعلی، یکی دیگر از تهدیدات رایج در حوزه سلامت است [۷].
  - **نشت اطلاعات:** نشت اطلاعات حساس بیماران به دلیل ضعف در سیستم‌های امنیتی و خطاهای انسانی، می‌تواند عواقب جبران‌ناپذیری داشته باشد [۸].
  - **حملات سایبری هدفمند:** حملات هدفمند به زیرساخت‌های حیاتی حوزه سلامت، با هدف اختلال در ارائه خدمات و کسب اطلاعات حساس، از دیگر تهدیدات قابل توجه هستند [۹].
- **راهکارهای موجود:**
  - **تدابیر قانونی و مقرراتی:** تصویب قوانین و مقررات مرتبط با امنیت سایبری در حوزه سلامت، گام مهمی در جهت ارتقای امنیت سایبری است.
  - **آموزش کارکنان:** برگزاری دوره‌های آموزشی برای افزایش آگاهی کارکنان در زمینه امنیت سایبری، نقش مهمی در کاهش خطرات ناشی از خطاهای انسانی دارد [۹].
  - **استفاده از فناوری‌های امنیتی:** بهره‌گیری از فناوری‌های نوین مانند فایروال‌ها، سیستم‌های تشخیص نفوذ و رمزنگاری، برای محافظت از سیستم‌ها و داده‌ها ضروری است [۹].
  - **همکاری بین‌بخشی:** همکاری بین سازمان‌های مختلف، از جمله وزارت بهداشت، وزارت ارتباطات و سازمان‌های امنیتی، برای مقابله با تهدیدات سایبری بسیار مهم است [۹].

با این حال، علی‌رغم وجود این راهکارها، ضعف در اجرای آن‌ها و نبود یک رویکرد جامع و هماهنگ، باعث شده است که تهدیدات سایبری همچنان به عنوان یک چالش جدی برای حوزه سلامت ایران باقی بماند.

ب) یافته‌های خاص

- **مقایسه با سایر کشورها:**
  - **سطح بلوغ زیرساخت‌های امنیتی:** مقایسه نشان می‌دهد که زیرساخت‌های امنیتی در حوزه سلامت ایران نسبت به کشورهای توسعه‌یافته غربی، به‌ویژه در حوزه‌های مدیریت ریسک سایبری، پاسخگویی به حوادث و استفاده از فناوری‌های پیشرفته امنیتی، در سطح پایین‌تری قرار دارد [۱۰].
  - **آگاهی و آموزش کارکنان:** سطح آگاهی و آموزش کارکنان حوزه سلامت در ایران در زمینه امنیت سایبری، به ویژه در مقایسه با کشورهای پیشرو، پایین‌تر است. این موضوع منجر به افزایش احتمال وقوع خطاهای انسانی و نفوذ مهاجمان می‌شود [۱۱].

- **چارچوب‌های قانونی و مقرراتی:** چارچوب‌های قانونی و مقرراتی مرتبط با امنیت سایبری در حوزه سلامت ایران، اگرچه در سال‌های اخیر تقویت شده است، اما همچنان نیازمند تکامل و تطبیق با استانداردهای بین‌المللی است [۱۲].
- **سرمایه‌گذاری در امنیت سایبری:** میزان سرمایه‌گذاری در حوزه امنیت سایبری در ایران نسبت به سایر کشورها کمتر بوده و این امر بر کیفیت و کمیت اقدامات امنیتی تأثیر گذاشته است [۱۳].

- **تحلیل روند تغییرات تهدیدات:**
  - **پیچیدگی روزافزون حملات:** تهدیدات سایبری در حوزه سلامت ایران به سمت پیچیدگی و هدفمندی بیشتری حرکت کرده است. مهاجمان از ابزارها و تکنیک‌های پیشرفته‌تری برای نفوذ به سیستم‌ها استفاده می‌کنند.
  - **افزایش حملات باج‌افزاری:** حملات باج‌افزاری به یکی از جدی‌ترین تهدیدات برای بیمارستان‌ها و مراکز درمانی تبدیل شده است. این نوع حملات با هدف اخاذی از سازمان‌ها و ایجاد اختلال در ارائه خدمات صورت می‌گیرد.
  - **بهره‌برداری از آسیب‌پذیری‌های زنجیره تأمین:** مهاجمان به دنبال بهره‌برداری از آسیب‌پذیری‌های موجود در نرم‌افزارها و تجهیزات پزشکی هستند تا به سیستم‌های بیمارستانی نفوذ کنند.
  - **افزایش حملات هدفمند:** حملات هدفمند به سازمان‌های خاص در حوزه سلامت، با هدف سرقت اطلاعات حساس یا ایجاد اختلال در عملیات آن‌ها، رو به افزایش است.
- **ارزیابی اثربخشی راهکارها:**
  - **آموزش کارکنان:** آموزش کارکنان در زمینه امنیت سایبری، اگرچه اهمیت بالایی دارد، اما به تنهایی برای مقابله با تهدیدات پیچیده کافی نیست.
  - **فناوری‌های امنیتی:** استفاده از فناوری‌های امنیتی مانند فایروال‌ها و سیستم‌های تشخیص نفوذ، در کاهش خطر حملات موثر بوده است.
  - **همکاری بین‌بخشی:** همکاری بین سازمان‌های مختلف در حوزه سلامت و فناوری اطلاعات، برای مقابله با تهدیدات سایبری پیچیده، ضروری است.
  - **چالش‌های اجرایی:** اجرای برخی از راهکارها مانند به‌روزرسانی مداوم سیستم‌ها و نرم‌افزارها، به دلیل محدودیت‌های بودجه‌ای و فنی، با چالش‌هایی مواجه است.

نتایج این پژوهش حاکی از آن است که مهاجمان سایبری با شناسایی آسیب‌پذیری‌های موجود در سیستم‌های تصویربرداری پزشکی، نوع جدیدی از حملات باج‌افزاری را طراحی کرده‌اند که قادر است به طور مستقیم بر کیفیت خدمات درمانی تأثیر گذارد. همچنین، این پژوهش نشان می‌دهد که دستگاه‌های پزشکی متصل به شبکه‌های بیمارستانی، به عنوان یک نقطه ورود برای مهاجمان سایبری عمل کرده و امکان انجام حملات پیچیده‌تر و هدفمندتر را فراهم می‌آورند. علاوه بر این، استفاده از هوش مصنوعی در طراحی حملات سایبری، یک تهدید نوظهور است که می‌تواند منجر به جایگزینی کدهای برنامه‌نویسی حیاتی و ایجاد اختلالات گسترده در سیستم‌های مراقبت بهداشتی شود. این یافته‌ها بر اهمیت توسعه راهکارهای امنیتی جامع برای مقابله با تهدیدات سایبری در حوزه سلامت تأکید می‌کند [۱۴].

بحث

یافته‌های این مطالعه نشان می‌دهد که نظام سلامت ایران با چالش‌های جدی در حوزه امنیت سایبری روبرو است. ضعف در زیرساخت‌های امنیتی، کمبود نیروی متخصص و نبود یک رویکرد جامع، از جمله عوامل اصلی آسیب‌پذیری این سیستم در برابر حملات سایبری با پیچیدگی روزافزون هستند. این یافته‌ها با مطالعات پیشین مبنی بر افزایش هدف‌گیری زیرساخت‌های حیاتی توسط مهاجمان سایبری همسو است [۱۴]. شناسایی یک نوع جدید از حمله باج‌افزاری که به طور خاص سیستم‌های تصویربرداری پزشکی را هدف قرار می‌دهد، نشان‌دهنده تکامل مداوم تهدیدات سایبری در این حوزه و ضرورت اتخاذ تدابیر امنیتی پیشرفته‌تر است.

نتایج این پژوهش، ارتباط مستقیمی بین دیجیتالی شدن روزافزون سیستم‌های سلامت و افزایش سطح آسیب‌پذیری آن‌ها در برابر تهدیدات سایبری نشان می‌دهد. این یافته، اهمیت سرمایه‌گذاری در زیرساخت‌های امنیتی و ارتقای آگاهی کارکنان را بیش از پیش آشکار می‌سازد. با این حال، محدودیت‌های نمونه آماری و تمرکز بر یک منطقه خاص، از جمله محدودیت‌های این پژوهش است که می‌تواند بر تعمیم‌پذیری نتایج تأثیرگذار باشد [۱۵].

یافته‌های این مطالعه، ضرورت اتخاذ رویکردی جامع برای بهبود امنیت سایبری در حوزه سلامت را تأکید می‌کند. ضعف زیرساخت‌های امنیتی، کمبود نیروی متخصص و نبود یک رویکرد هماهنگ، از جمله چالش‌های اصلی در این حوزه هستند. این یافته‌ها با مطالعات پیشین همسو بوده و بر اهمیت سرمایه‌گذاری در زیرساخت‌ها و آموزش تاکید دارند [۱۶].

تحلیل نتایج نشان می‌دهد که مشکلات امنیتی در حوزه سلامت ایران ریشه در عوامل فنی، سازمانی، قانونی و فرهنگی دارد. ضعف زیرساخت‌ها، نبود فرهنگ امنیت سایبری، کمبود نیروی متخصص و اولویت‌بندی پایین امنیت در بودجه‌ها، از جمله مهم‌ترین چالش‌ها در این حوزه هستند [۱۷].

دلایل اصلی مشکلات امنیتی در حوزه سلامت ایران را می‌توان به چهار دسته تقسیم کرد:

- **عوامل فنی:** ضعف زیرساخت‌ها، نبود سیستم‌های به‌روزرسانی و عدم استفاده از فناوری‌های امنیتی پیشرفته.
- **عوامل سازمانی:** نبود فرهنگ امنیت سایبری، کمبود نیروی متخصص و اولویت‌بندی پایین امنیت در بودجه‌ها.
- **عوامل قانونی:** ضعف قوانین و مقررات مرتبط و عدم اجرای موثر قوانین موجود.
- **عوامل فرهنگی:** آگاهی پایین کاربران از تهدیدات و عدم رعایت اصول امنیت سایبری.

برای بهبود وضعیت، پیشنهاد می‌شود:

- **سرمایه‌گذاری در زیرساخت‌ها:** تقویت زیرساخت‌های امنیتی با استفاده از فناوری‌های روزآمد مانند هوش مصنوعی.
- **آموزش جامع:** برگزاری دوره‌های آموزشی مستمر برای افزایش آگاهی کارکنان در تمامی سطوح.
- **تقویت چارچوب قانونی:** تدوین و اجرای قوانین جامع و کارآمد برای حفاظت از داده‌های بیماران.
- **همکاری بین‌بخشی:** تقویت همکاری بین سازمان‌های مختلف برای ایجاد یک رویکرد هماهنگ.

اگرچه این پژوهش به بسیاری از سوالات پاسخ داده است، اما همچنان شکاف‌هایی وجود دارد. به عنوان مثال، تأثیر فرهنگ سازمانی بر رفتار امنیتی کارکنان و نقش عوامل انسانی در وقوع حوادث سایبری، نیازمند بررسی‌های بیشتر است.

این مطالعه نیز مانند هر مطالعه دیگری دارای محدودیت‌هایی است. یکی از محدودیت‌های اصلی این مطالعه، وابستگی به مقالات منتشر شده در پایگاه‌های اطلاعاتی مشخص است. ممکن است مقالات دیگری نیز وجود داشته باشد که در این پایگاه‌ها نمایه نشده باشند. همچنین، ممکن است برخی از مقالات به زبان‌های دیگر منتشر شده باشند که در این مطالعه مورد بررسی قرار نگرفته‌اند.

این پژوهش، نقطه شروعی برای تحقیقات آینده در حوزه امنیت سایبری نظام سلامت ایران است. پیشنهاد می‌شود تحقیقات آتی بر ارزیابی اثربخشی راهکارهای پیشنهادی، توسعه مدل‌های پیش‌بینی‌کننده تهدیدات سایبری، و بررسی نقش عوامل انسانی در وقوع حوادث سایبری تمرکز کنند. همچنین، مقایسه وضعیت ایران با سایر کشورها و شناسایی بهترین شیوه‌ها، می‌تواند به بهبود وضعیت امنیت سایبری در کشور کمک کند.

نتیجه‌گیری

نتایج این پژوهش پیامدهای مهمی برای سیاست‌گذاران و مدیران حوزه سلامت دارد. سرمایه‌گذاری در زیرساخت‌های امنیتی، آموزش کارکنان، و ایجاد برنامه‌های واکنش سریع در برابر حوادث سایبری، از جمله اقدامات ضروری برای تقویت امنیت سایبری در این حوزه است. همچنین، پژوهش‌های آینده می‌توانند بر روی توسعه راهکارهای فنی برای مقابله با تهدیدات نوظهور و ارزیابی اثربخشی اقدامات امنیتی در محیط‌های واقعی متمرکز شوند. با این حال، تحقیقات بیشتری برای ارزیابی اثربخشی راهکارهای پیشنهادی، تحلیل ریشه‌های فرهنگی و اجتماعی این مسئله و توسعه مدل‌های پیش‌بینی حملات مورد نیاز است.

منابع

۱- فاروجی، د. (۲۰۲۰) ،" الگوی ارزیابی خطرپذیری شهری در بلایای طبیعی،" *مهندسی ساختمان و علوم مسکن* ,(2)*13* , ۱-۱۱.

۲- رجبی، ع. (۱۴۰۲) ،" بهداشت امنیت سایبری به چه معناست و چه تبعاتی دارد" خبرگزاری مهر .

3-Lee, T. (2013), “ The WannaCry ransomware attack was temporarily halted,” But it's not over yet.

4-https://shbu.ac.ir/pages/index.php?pageID=117&lang=fa

۵-گزارش‌های سازمان جهانی بهداشت (WHO) در مورد امنیت سایبری در حوزه سلامت مقالات علمی منتشر شده در مجلات داخلی و خارجی.

۶-خلیلی پورکن آبادی، ع. نورعلی وند، ی. (۱۳۹۱) ،" تهدیدات سایبری و تاثیر آن بر امنیت ملی. مطالعات راهبردی،"۱۶۷-۱۹۶.

۷- شاه محمدی, غ. کمالی زاده, س. (۲۰۱۶)، "ارائه روشی برای شناسایی وب‌سایت فیشینگ سرویس پرداخت اینترنتی" *پدافند الکترونیکی و سایبری، ۲۶-۱۱.*

۸- جدیدی، م, اصفهانی، م. (۲۰۲۱) ،" بررسی حملات کانال جانبی حافظه نهان بر روی پیاده سازی الگوریتم رمز AES".

۹- صیاد. م، امینی، آ. (۱۴۰۰)، " تهدیدهای سایبری و اقدامات امنیتی در فضای مجازی، بررسی رویکردهای ایالات متحده آمریکا و جمهوری اسلامی ایران،" نشریه امنیت ملی، ۱۰(۳۸): ۲۹۳-۳۳۰.

۱۰- یمینی, سی. کازرونی, ح. (۲۰۲۴)، " احصاء فرمول محاسبه تاب‌آوری در زنجیره تأمین دفاعی، " فصلنامه آماد و فناوری دفاعی، ۴۶-۱۱.

۱۱- حسن زاده، م. کریم زادگان مقد، م. (۲۰۱۲)، " ارائه یک چارچوب مفهومی برای ارزیابی پرمایگی و آموزش آگاهی از امنیت اطلاعات کاربران".

۱۲-بنار، م. (۲۰۲۰)، " اینترنت اشیاء (۳): چارچوب مقررات گذاری، امنیت سایبری و مقرراتگذاری داده در اینترنت اشیاء برای ایران".

۱۳-مهدوی پور, آ. (۲۰۲۲)، " عوامل موثر بر امنیت سایبری ارتش جمهوری اسلامی ایران (مطالعه موردی: ستاد ارتش جمهوری اسلامی ایران) ،" *علوم و فنون نظامی*، ۱۲۳-۱۰۳.

14- Benmalek, M. (2024). Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges. Internet of Things and Cyber-Physical Systems, 4, 186–202. https://doi.org/10.1016/j.iotcps.2023.12.001

۱۵- قاسمی, ج. بارین، و. (۲۰۱۲)، " حملات سایبری و حقوق بین‌الملل، "مجله حقوقی دادگستری، ۱۴۵-۱۱۵.

16- https://apk-group.net/kb/information-security/healthcare-cybersecurity

17- Eichelberg, M. Klaus, K. Marc, K. (2020), "Cybersecurity challenges for PACS and medical imaging," *Academic Radiology* 27.8, pp 1126-1139.