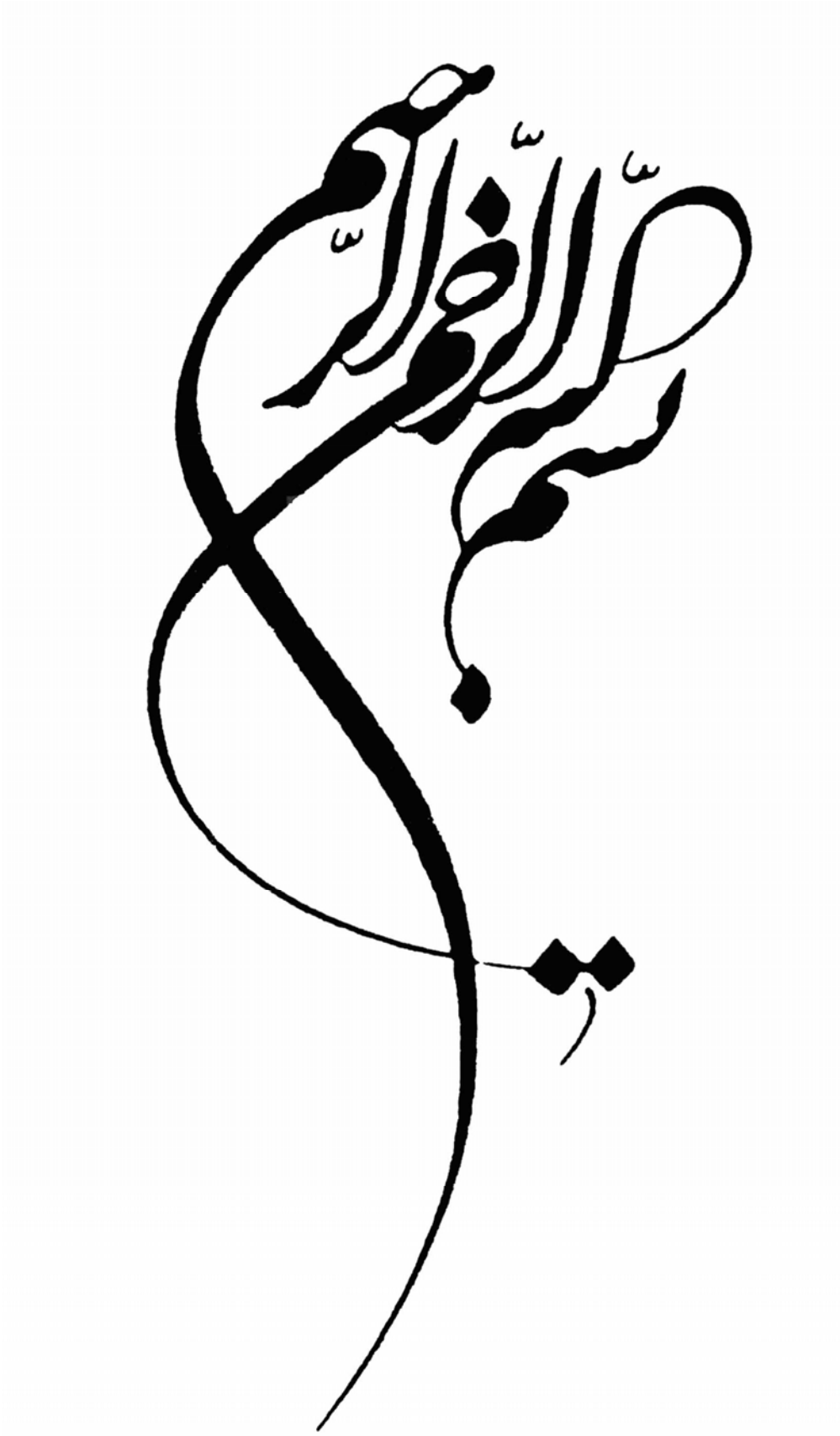


بسمه تعالی

تاییدیه اعضای هیات داوران حاضر در جلسه دفاع از پایان نامه

آقای محمدامیر ثابت حاجیونی پایان نامه ٦ واحدی خود را **با عنوان ارزیابی کمی مخاطرات امنیتی موجود در شبکه فیبر نوری کشور** در تاریخ ۱۳۸۹/۳/۲۲ ارائه کردند.

اعضای هیات داوران نسخه نهایی این پایان نامه را از نظر فرم و محتوا تایید کرده و پذیرش آنرا برای تکمیل درجه کارشناسی ارشد مهندسی صنایع - مهندسی فناوری اطلاعات-سیستمهای اطلاعاتی پیشنهاد می کنند.

عضو هیات داوران	نام و نام خانوادگی	رتبه علمی	امضا
استاد راهنما	دکتر پرستو محمدی	استادیار	
استاد راهنمای دوم	دکتر عباس آسوشه	استادیار	
استاد ناظر	دکتر محمد اقدسی	دانشیار	
استاد ناظر	دکتر نسیم نهاوندی	استادیار	
استاد ناظر	دکتر اسفندیار مهرشاهی	استادیار	
مدیر گروه (یا نماینده گروه تخصصی)	دکتر نسیم نهاوندی	استادیار	

این نسخه به عنوان نسخه نهایی پایان نامه/رساله مورد تأیید است.

امضای استاد راهنما:

آیین‌نامه حق مالکیت مادی و معنوی در مورد نتایج پژوهشهای علمی دانشگاه تربیت مدرس

مقدمه: با عنایت به سیاست‌های پژوهشی و فناوری دانشگاه در راستای تحقق عدالت و کرامت انسانها که لازمه شکوفایی علمی و فنی است و رعایت حقوق مادی و معنوی دانشگاه و پژوهشگران، لازم است اعضای هیأت علمی، دانشجویان، دانش‌آموختگان و دیگر همکاران طرح، در مورد نتایج پژوهشهای علمی که تحت عناوین پایان‌نامه، رساله و طرحهای تحقیقاتی با هماهنگی دانشگاه انجام شده است، موارد زیر را رعایت نمایند:

ماده ۱- حق نشر و تکثیر پایان نامه/ رساله و درآمدهای حاصل از آنها متعلق به دانشگاه می باشد ولی حقوق معنوی پدید آورندگان محفوظ خواهد بود.

ماده ۲- انتشار مقاله یا مقالات مستخرج از پایان‌نامه/ رساله به صورت چاپ در نشریات علمی و یا ارائه در مجامع علمی باید به نام دانشگاه بوده و با تایید استاد راهنمای اصلی، یکی از اساتید راهنما، مشاور و یا دانشجو مسئول مکاتبات مقاله باشد. ولی مسئولیت علمی مقاله مستخرج از پایان نامه و رساله به عهده اساتید راهنما و دانشجو می باشد.

تبصره: در مقالاتی که پس از دانش‌آموختگی بصورت ترکیبی از اطلاعات جدید و نتایج حاصل از پایان‌نامه/ رساله نیز منتشر می‌شود نیز باید نام دانشگاه درج شود.

ماده ۳- انتشار کتاب، نرم افزار و یا آثار ویژه (اثری هنری مانند فیلم، عکس، نقاشی و نمایشنامه) حاصل از نتایج پایان‌نامه/ رساله و تمامی طرحهای تحقیقاتی کلیه واحدهای دانشگاه اعم از دانشکده ها، مراکز تحقیقاتی، پژوهشکده ها، پارک علم و فناوری و دیگر واحدها باید با مجوز کتبی صادره از معاونت پژوهشی دانشگاه و براساس آئین نامه های مصوب انجام شود.

ماده ۴- ثبت اختراع و تدوین دانش فنی و یا ارائه یافته ها در جشنواره‌های ملی، منطقه‌ای و بین‌المللی که حاصل نتایج مستخرج از پایان‌نامه/ رساله و تمامی طرح‌های تحقیقاتی دانشگاه باید با هماهنگی استاد راهنما یا مجری طرح از طریق معاونت پژوهشی دانشگاه انجام گیرد.

ماده ۵- این آیین‌نامه در ۵ ماده و یک تبصره در تاریخ ۸۷/۴/۱ در شورای پژوهشی و در تاریخ ۸۷/۴/۲۳ در هیأت رئیسه دانشگاه به تایید رسید و در جلسه مورخ ۸۷/۷/۱۵ شورای دانشگاه به تصویب رسیده و از تاریخ تصویب در شورای دانشگاه لازم‌الاجرا است.

«اینجانب محمد امیر ثابت حاجیونی دانشجوی رشته مهندسی فناوری اطلاعات ورودی سال تحصیلی۱۳۸۶ مقطع کارشناسی ارشد دانشکده فنی و مهندسی متعهد می شوم کلیه نکات مندرج در آئین نامه حق مالکیت مادی و معنوی در مورد نتایج پژوهش های علمی دانشگاه تربیت مدرس را در انتشار یافته های علمی مستخرج از پایان نامه / رساله تحصیلی خود رعایت نمایم. در صورت تخلف از مفاد آئین نامه فوق الاشعار به دانشگاه وکالت و نمایندگی می دهم که از طرف اینجانب نسبت به لغو امتیاز اختراع بنام بنده و یا هر گونه امتیاز دیگر و تغییر آن به نام دانشگاه اقدام نماید. ضمناً نسبت به جبران فوری ضرر و زیان حاصله بر اساس برآورد دانشگاه اقدام خواهم نمود و بدینوسیله حق هر گونه اعتراض را از خود سلب نمودم»

امضا:

تاریخ:۱۳۸۹/۰۳/۲۲

آیین نامه چاپ پایان‌نامه (رساله)های دانشجویان دانشگاه تربیت مدرس

نظر به اینکه چاپ و انتشار پایان نامه (رساله)های تحصیلی دانشجویان دانشگاه تربیت مدرس، مبین بخشی از فعالیتهای علمی - پژوهشی دانشگاه است بنابراین به منظور آگاهی و رعایت حقوق دانشگاه،دانش آموختگان این دانشگاه نسبت به رعایت موارد ذیل متعهد می‌شوند:

ماده ۱: در صورت اقدام به چاپ پایان نامه (رساله)ی خود، مراتب را قبلاً به طور کتبی به «دفتر نشر آثارعلمی» دانشگاه اطلاع دهد.

ماده ۲: در صفحه سوم کتاب (پس از برگ شناسنامه) عبارت ذیل را چاپ کند:

«کتاب حاضر، حاصل پایان نامه کارشناسی ارشد نگارنده در رشته مهندسی فنآوری اطلاعات است که در سال ۱۳۸۹ در دانشکده فنی و مهندسی دانشگاه تربیت مدرس به راهنمایی سرکار خانم دکتر پرستو محمدی و استاد راهنما دوم جناب آقای دکتر عباس آسوشه از آن دفاع شده است.»

ماده ۳: به منظور جبران بخشی از هزینه‌های انتشارات دانشگاه، تعداد یک درصد شمارگان کتاب (در هر نوبت‌چاپ) را به «دفتر نشر آثارعلمی» دانشگاه اهدا کند. دانشگاه می‌تواند مازاد نیاز خود را به نفع مرکز نشر درمعرض فروش قرار دهد.

ماده ۴: در صورت عدم رعایت ماده ۳، ۵۰٪ بهای شمارگان چاپ شده را به عنوان خسارت به دانشگاه تربیت‌مدرس، تأدیه کند.

ماده ۵: دانشجو تعهد و قبول می کند در صورت خودداری از پرداخت بهای خسارت، دانشگاه می‌تواند خسارت مذکور را از طریق مراجع قضایی مطالبه و وصول کند؛ به علاوه به دانشگاه حق می‌دهد به منظور استیفای حقوق خود، از طریق دادگاه، معادل وجه مذکور در ماده ۴ را از محل توقیف کتابهای عرضه شده نگارنده برای فروش، تامین نماید.

ماده ۶: اینجانب محمد امیر ثابت حاجیونی دانشجوی رشته مهندسی فناوری اطلاعات – سیستمهای اطلاعاتی مقطع‌کارشناسی ارشد تعهد فوق وضمانت اجرایی آن را قبول کرده، به آن ملتزم می شوم.

نام و نام خانوادگی: محمد امیر ثابت حاجیونی

تاریخ و امضا: ۸۹/۰۳/۲۲

دانشگاه تربیت مدرس

دانشکده فنی مهندسی

پایان نامه برای دریافت درجه کارشناسی ارشد

رشته مهندسی فنآوری اطلاعات گرایش سیستم ها

ارزیابی کمی مخاطرات امنیتی موجود در شبکه فیبر نوری کشور

نگارنده

محمد امیر ثابت حاجیونی

استاد راهنما اول

دکتر پرستو محمدی

استاد راهنما دوم

دکتر عباس آسوشه

ماه و سال دانش آموختگی

۱۳۸۹/۰۳/۲۲

تشکر و قدردانی:

سپاس خدای یکتا را که هرچه هست از اوست.

سپاس خدایی را که توفیق تحصیل علم به ما ارزانی داشت.

به مصداق کلام شریف من لم یشکر المخلوق لم یشکر الخالق وظیفه خود می دانم سپاسگذار تمام آنهایی باشم که در این راه ارزشمند، بودنشان و امیدشان راهگشای من بود؛ خانواده عزیزم که همانند تمامی روزهای گذشته با صبر و حوصله در کنارم بودند. و همچنین از استادان گرامی سرکار خانم دکتر پرستو محمدی و جناب آقای دکتر عباس آسوشه که با تلاش های خود در انجام این پایان نامه مرا یاری نمودند، صمیمانه متشکرم و برای ایشان آرزوی سلامتی، موفقیت و سر بلندی دارم.

چکیده

شبکه فیبر نوری کشور بعنوان یکی از مهمترین زیرساخت های ارتباطی از اهمیت بسیار بالائی برخوردار است. لذا اطمینان یافتن از امنیت مناسب شبکه و اطلاعات موجود در آن بسیار ضروری است. در مورد ارزیابی امنیتی شبکه فیبر نوری کشور تا به حال کار تحقیقاتی خاصی صورت نگرفته است. و همچنین براساس آمار رسمی شرکت ارتباطات زیرساخت، بروز قطعی‌های ناخواسته شبکه فیبرنوری و اختلالات ایجاد شده در ارتباطات داخلی و بین‌المللی تاکنون خسارات اقتصادی، اجتماعی، سیاسی و امنیتی زیادی به کشور وارد کرده است.لذا در این تحقیق سعی شده است با روشی اصولی و بر اساس استانداردهای ارزیابی امنیتی معتبر بتوان شبکه موجود را مورد تحلیل و ارزیابی امنیتی قرار داده و آسیب پذیری ها و نقاط ضعف آنرا استخراج کرده و بر اساس آنها ریسک های قابل اعمال بر پارامترهای کلیدی شبکه را بصورت کمی تحلیل نموده و بصورت گرافیکی نیز وضعیت امنیتی موجود و مطلوب را ارائه کرد. از ابزارهای موجود در این متدولوژی بعنوان ابزارهای اصلی ارزیابی کمی ریسک شبکه فیبر نوری کشور استفاده شده است. روش استفاده شده در این متدولوژی بر اساس استانداردهای امنیتی معتبر از قبیل ISO27001 و BS7799 می باشد. برای انجام روند تحلیل ریسک های امنیتی، ابزار تحلیل ریسک مبتنی بر اکسل بر مبنای متدولوژی Infotech طراحی گردیده و با استفاده از آن روند ارزیابی و تحلیل ریسک های امنیتی شبکه فیبر نوری کشور انجام گردید.

پارامترهای کلیدی شبکه فیبر نوری در شش دسته : مدیریت شبکه، شناسایی وتصدیق هویت، کنترل دسترسی، صحت ودرستی پیام و تاریخ، سخت افزار شبکه و مجموع روترها ، سوئیچ‌ها و هاب‌ها، طبقه بندی می شوند. LYNN, S. (2009)

نتیجه ارزیابی بدین شرح بدست می آید: مدیریت بسیار ضعیف شبکه 11.0%، شناسائی و تصدیق هویت ضعیف20.0%، کنترل دسترسی ناکافی25.0%، صحت داده ها پیام به طور خیلی ضعیف10.0%، سخت افزار شبکه 15.0% و نتایج هاب،روترها و سوئیچ ها35.0% و بر اساس درصد مشخص شده برای هر کدام از شش دسته ، خارج قسمت ریسک کسب و کاری آن طبق فرمول

$$BRQ = \frac{\text{(احتمال وقوع} \times \text{آسیب پذیری)} + \text{میزان تاثیر کسب و کار}}{}$$

محاسبه، سپس BRQ شبکه برای هر کدام استخراج گردیده که عبارتند از مدیریت شبکه 1.1 ، شناسائی و تصدیق 1.3، کنترل دسترسی1.5، صحت داده ها1.2، سخت افزار شبکه1.3 و نتایج هاب،روترها و سوئیچ ها1.6 که بیانگر وضعیت امنیتی موجود شبکه فیبر نوری است. لذا شبکه مورد نظر دارای نقاط ضعف و ریسک های امنیتی متعددی می باشد که در صورت عدم رفع آنها می تواند صدمات جبران ناپذیری به سیستم های ارتباطی و تجهیزات استفاده کننده از این زیرساخت وارد آورند.در واقع طراحان شبکه فیبر نوری کشور در هنگام طراحی و پیاده سازی شبکه فیبر نوری ملاحظات امنیتی لازم را مد نظر قرار نداده اند.

کلید واژه: ارزیابی ، آسیب پذیری ، ریسک، امنیت، شبکه فیبر نوری

فصل اول

۱-۱ مقدمه

شبکه فیبر نوری کشور، بعنوان یکی از مهمترین زیرساختهای ارتباطی موجود، نقش بسیار بالائی در روند انتقال اطلاعات و ارتباطات در سطح ملی ایفا می نماید و در رشد و پیشرفت دانش و فن آوری در تمامی حوزه ها تاثیرگذار است.

با توجه به جدید بودن تکنولوژی ساخت تجهیزات فیبر نوری در مقایسه با سایر تجهیزات انتقال اطلاعات و داده ها از قبیل کابل های مسی و مخابرات بی سیم و رویکرد عمومی به استفاده از آنها و حجم بالای داده های در حال انتقال توسط آنها، مساله امنیت اطلاعات و داده های در حال انتقال بسیار مهم بوده و می تواند تاثیر بسیار زیادی بر روی بخشهای مختلف استفاده کننده از این امکانات بگذارد. همچنین براساس آمار رسمی شرکت ارتباطات زیرساخت، بروز قطعی‌های ناخواسته شبکه فیبرنوری و اختلالات ایجاد شده در ارتباطات داخلی و بین‌المللی تاکنون خسارات اقتصادی، اجتماعی، سیاسی و امنیتی زیادی به کشور وارد کرده است. هر چند آمار دقیقی از میزان قطعی فیبرنوری در منطقه در دسترس نیست اما به اعتقاد کارشناسان این حوزه و بر حسب شواهد موجود، هیچ کشوری در منطقه به اندازه ایران قطعی ندارد. آمار ۱۹۰ بار قطعی منطقه‌ای در برخی مسیرهای شبکه ملی فیبرنوری یا به عبارتی قطعی یک روز در میان اینترنت کشور طی یک سال در نوع خود یک رکورد به حساب می‌آید .درسال گذشته ۱۹۰ قطعی و در سال جاری تاکنون ۷۹قطعی در شبکه ملی فیبرنوری رخ داده است. یعنی به طور متوسط هر دو روز یک بار قطعی، اما این آمار بیانگر همین تعداد اختلال درارتباطات بین شهری وبین الملل طی سال های گذشته و سال جاری نیست، اگر هرقطعی درمسیرهای فیبرنوری به اختلال در ارتباطات اینترنتی ، تلفن ثابت وهمراه در شبکه بین شهری و بین الملل منجر شود دیگر موضوعی تحت عنوان تأمین ارتباطات درشبکه زیرساخت کشور مفهومی نخواهد داشت، لذا با توجه به اینکه تا کنون در کشور چنین تحقیقی صورت نگرفته است، در

این پایان نامه سعی شده است با استفاده از روش های ارزیابی ریسک مناسب، میزان امنیت شبکه فیبر نوری کشور بررسی گردد.

هدف از امنیت اطلاعات، استفاده از مجموعه ای از سیاست ها، راه کارها، ابزارها، سخت افزارها و نرم افزارها، برای فراهم آوردن یک محیط عاری از تهدید (یک حد قابل قبول از ریسک) در تولید، پالایش، انتقال، و توزیع اطلاعات است. فراهم آوردن چنین محیطی مستلزم انجام یک سری موارد است که می توان از آنها به نیازهای امنیتی اطلاعات نام برد.

شبکه یکپارچه فیبرنوری که سریعترین، مطمئن‌ترین شبکه زیرساختی در جهان و از جمله برای ایران و پانزده کشور همسایه (جهت برقراری ارتباط حدود ۴۰۰ میلیون نفر جمعیت این منطقه با یکدیگر) است و نیز فرصتی برای ترانزیت ارتباطات کشورهای منطقه است، می‌تواند محل درآمد ارزی قابل توجهی برای کشور باشد که همه این موارد در سایه شبکه‌ای ایمن و بدون نقص محقق خواهد شد.

۱-۲ بیان مسئله

وزارت ICT در راستای توسعه‌ی شبکه فیبرنوری و با توجه به ملزم بودن به ایجاد زیرساخت شبکه فیبر نوری(انتقال دیتا) کشور و بستری مناسب برای توسعه‌ی اقتصادی، فرهنگی و سیاسی کشور از جمله زیرساخت لازم برای کاربردهای الکترونیکی شامل، شبکه فناوری اطلاعات پیشرفته، دولت الکترونیکی، تجارت الکترونیکی، بانکداری الکترونیکی، آموزش الکترونیکی و بهداشت الکترونیکی و... اقدام کرده است. تا کنون بیش از ۴۰ هزار کیلومتر مسیر فرعی فیبرنوری در درون شهرها و نقاط فرعی بین‌شهری اجرا شده است. مجموع خطوط فیبرنوری شهری و بین‌شهری و بین‌الملل کشور به ۷۶ هزار کیلومتر رسیده است که امکان ارتباطات شهری، بین شهری و بین‌الملل را درانتقال صوت، تصویر و دیتا فراهم می کند.

بروز قطعی‌های ناخواسته‌ی شبکه‌ی فیبر نوری تاکنون خسارات اقتصادی ، اجتماعی ، سیاسی و امنیتی زیادی به کشور وارد و اختلالاتی در ارتباطات داخلی و بین‌المللی به وجود آورده است. که از آن جمله می توان به موارد زیر اشاره نمود:

- خسارات اقتصادی
- اختلال در مکالمات تجاری
- ضرر و زیان حاصله در زمان قطع ارتباط (ریالی از ارتباطات داخلی و ارزی از ترانزیت ارتباطات بین الملل)
- ضرر و زیان حاصله در اثر عدم توان هدایت هواپیماهای ترانزیت توسط برجهای مراقبت هوائی در زمان قطع ارتباط
- خسارات ناشی از عدم هماهنگی سازمانها و دستگاههای مختلف همچون : بانکها ، شرکتهای برق ، گاز، نفت ، کارت هوشمند سوخت و ...
- خسارات اجتماعی

نارضایتی عمومی و سلب اعتماد اجتماعی از عملکرد دستگاههای اجرائی و ...

عدم امکان برقراری ارتباط جامعه و اخلال در امور اجتماعی، فرهنگی و ...

- خسارات سیاسی و امنیتی

کاهش وجهه امنیتی و ثبات مسیرهای ایران (زمینی و هوائی) برای انتقال ترافیکهای بین‌المللی و عواقب مترتب و ...

با این که هزینه پیاده سازی یک سیستم امنیتی شبکه فیبر نوری اندک نمی باشد و هزینه های بسیار بالایی را بر دولت تحمیل می کند، ولی در مقابل هزینه های گزاف و غیر قابل جبران عدم امنیت شبکه ، این سرمایه گذاری لازم و ضروری است. دولت با پیاده سازی یک استراتژی امنیتی در شبکه فیبر نوری می تواند از مزایای زیر بهره مند گردد:

- کاهش احتمال غیرفعال شدن سیستم ها و برنامه ها (کاهش از دست دادن فرصت ها)
- کاهش زیانهای اقتصادی ناشی از اختلالات فیبرنوری
- کاهش هزینه از دست دادن داده توسط ویروس های مخرب و یا حفره های امنیتی (حفاظت از داده های ارزشمند)

- افزایش حفاظت از مالکیت معنوی (M. Krause & Harold F. Tipton,1998)

لذا با توجه به احتمال وقوع تهدیدات (اعم از عمدی ، غیر عمدی و محیطی)و در نتیجه ایجاد اختلال در ارتباطات موجود بر بستر شبکه فیبر نوری که منجر به خسارت فوق الذکر می گردد ، بایستی بستر شبکه فیبر نوری به لحاظ امنیتی مورد ارزیابی قرار گیرد.

۱-۳ اهمیت تحقیق

با توجه به اینکه در هر لحظه، اطلاعات بسیار زیادی از طریق شبکه فیبر نوری کشور در حال انتقال می باشد که اغلب آنها دارای ارزش فراوانی می باشند ،لذا اطمینان از امن بودن این مسیر ارتباطی و عدم دسترسی آسان به آنها برای عوامل تهدید از اهمیت خاصی برخوردار است. همچنین امن بودن این زیرساخت ارتباطی مهم در شرائط بحران، می تواند نقشی کلیدی در برابر تهاجمات دشمنان نسبت به تجهیزات ارتباطی و اطلاعاتی ایفا نماید.

متاسفانه تاکنون در مورد بررسی میزان امنیت شبکه فیبر نوری موجود و استخراج و دسته بندی ریسک های موجود در آن، تحقیق خاصی انجام نشده است و به اشتباه این تصور شکل گرفته است که شبکه فیبر نوری بطور ذاتی امن می باشد. در نتیجه در چند سال اخیر بطور فزاینده ای شبکه فیبر نوری گسترش یافته و در حال حاضر، بالغ بر دهها هزار کیلومتر شبکه فیبر نوری در نقاط مختلف نصب شده است. بدون اینکه مساله امنیت آن بررسی گردیده و راه کارهای مناسب امنیتی برای آن در نظر گرفته شود. در این پایان نامه سعی شده است به روشی کاملا علمی و با استفاده از روند تحلیل ریسک، نقاط ضعف و آسیب پذیری های موجود در شبکه فیبر نوری کشور بررسی گردیده و سعی شده با استفاده از استانداردهای امنیتی موجود در این زمینه ابزارهای مبتنی بر اکسلی جهت استخراج ریسک ها و رتبه بندی آنها طراحی و تولید گردد.

۱-۴ سوالات تحقیق

- آیا شبکه فیبر نوری کشور از لحاظ امنیتی وضعیت مطلوبی دارد؟

- آیا متدولوژی مناسبی را می توان برای انجام روند تحلیل ریسک شبکه فیبر نوری کشور، انتخاب یا بومی سازی نمود؟
- آیا می توان نقاط ضعف و آسیب پذیری های امنیتی شبکه فیبر نوری کشور را تعیین و استخراج نمود؟
- آیا می توان بر اساس نقاط ضعف و آسیب پذیری های امنیتی استخراج شده، ریسک های امنیتی شبکه فیبر نوری کشور را تعیین نمود؟
- آیا می توان ابزار یا ابزارهائی برای انجام روند تحلیل ریسک شبکه فیبر نوری کشور تولید نموده و توسط آن، ریسک های شبکه فیبر نوری کشور را تحلیل و ارزیابی نمود؟

۱-۵ فرضیه های تحقیق

- از میان مخاطرات شبکه، انواع دارایی های موجود در این شبکه فیبر نوری تحت تاثیر مخاطرات قرار می گیرند.
- جهت ایجاد بستر امن برای توسعه اقتصاد نوین مبتنی بر فنآوری اطلاعات و ارتباطات ، ارزیابی نمودن مخاطرات امنیتی شبکه فیبر نوری کشور ضروری می باشد.

۱-۷ متدولوژی تحقیق

با توجه به بررسی تطبیقی انواع استانداردهای امنیت اطلاعات و مطالعه و مقایسه انواع روشهای تحلیل ریسک و همچنین مقایسه انواع ابزار های ارزیابی کمی و کیفی ریسک در سیستم های اطلاعاتی به منظور انتخاب روش و ابزار مناسب تحلیل ریسک نسبت به دیگر روشها و ابزارها ، روش Infotech انتخاب و بر اساس ابزار طراحی شده مذکور ارزیابی کمی مخاطرات امنیتی شبکه فیبر نوری انجام گردید.

۱-۶ ساختار تحقیق

در ادامه این بخش ، نحوه چیدمان مطالب در بخشهای بعدی ذکر می گردد. در فصل دوم شبکه فیبر نوری کشور معرفی می گردد . سپس در فصل سوم، روش های مختلف تحلیل و ارزیابی ریسک های امنیتی مورد بررسی قرار گرفته و نقاط ضعف و قدرت هر کدام مشخص می گردد. سپس بر روی روند تحلیل ریسک مناسب یعنی متدلوژی Infotech که یکی از روندهای جدید و مبتنی بر استانداردهای امنیتی جهت تعیین و ارزیابی ریسک های موجود در شبکه های مبتنی بر فن آوری اطلاعات می باشد مورد بررسی قرار گرفته و با توجه به خصوصیات و مشخصات شبکه فیبر نوری کشور، اصلاحات مورد نیاز بر روی آن اعمال شده تا بتوان از این طریق روند تحیل ریسک مورد نظر را انجام داد. در ادامه در فصل چهارم ویژگیهای کلیدی امنیتی شبکه فیبر نوری کشور استخراج شده و پارامترها و شاخص های هر کدام از آنها تعیین می گردد. در نهایت در فصل پنجم با توجه به شاخص های کلیدی امنیتی استخراج شده ابزارهای تحلیل و ارزیابی ریسک های امنیتی قابل اعمال بر روی شبکه فیبر نوری کشور طراحی شده و بر اساس آنها شبکه فیبر نوری کشور تحلیل می گردد.

۱-۷ نتیجه گیری

با توجه به اطلاعات موجود در زمینه شبکه فیبر نوری کشور و گستردگی و اهمیت روزافزون آن، لازم است که توسط روشی علمی و بر مبنای استانداردهای امنیتی معتبر بتوان میزان امنیت این شبکه را مورد ارزیابی و تحلیل قرار داد. با توجه به اینکه از این نظر تا بحال کار تحقیقاتی خاصی در کشور صورت نگرفته است، اجرای این تحقیق می تواند نقطه شروع مناسبی برای محققین و کارشناسان امنیت اطلاعات که علاقه مند به انجام اینگونه تحقیقات باشند، قرار گیرد.

فصل دوم

بررسی انواع روش های تحلیل ریسک و انتخاب روش مناسب

۲-۱ مقدمه

اصولا جهت تعیین میزان امنیت یک شبکه نیازمند بکارگیری روش و متدولوژی ارزیابی امنیتی معتبری می باشیم. در حقیقت پس از مشخص شدن نحوه روش ارزیابی و تعیین ملاک های امنیتی مناسب، می توان بر اساس آنها هدف مورد نظر را ارزیابی و میزان امنیت آن را تعیین نمود. از آنجائیکه شناخت نقاط ضعف و آسیب پذیری های امنیتی و تعیین راه کارهای کنترلی مناسب جهت کاهش آنها بعنوان یکی از مراحل اساسی در تمامی روشهای تحلیل و ارزیابی امنیتی می باشد، ما نیز بر همین اساس روش ارزیابی خود را بر مبنای تحلیل آسیب پذیری ها و ریسک های موجود قرار می دهیم. در ادامه روش های مختلف تحلیل و مدیریت ریسک بصورت کلی بررسی می گردد. سعی شده است در این بررسی نقاط ضعف و قوت هر کدام از این روش ها استخراج شده و سپس با توجه به خصوصیات شبکه فیبر نوری کشور و نبود داده ها و اطلاعات کافی و مناسب در مورد حوادث و رویدادهای امنیتی رخ داده در شبکه مورد نظر، نقاط ضعف و آسیب پذیری های امنیتی شبکه فیبر نوری کشور بر اساس متدلوژی تحلیل ریسک مناسبی ، تعیین شده و سپس ریسک های متناسب با آنها استخراج می گردد.

در ادامه ابتدا روش مدیریت ریسک استاندارد ،تعریف شده و بطور مختصر شرح داده می شود. سپس بطور مختصر روشهای تحلیل و مدیریت ریسک های امنیتی مختلف مورد بررسی قرار می گیرد. بعلت اینکه در مراجع مختلف تعاریف مختلفی از عناصر تشکیل دهنده ریسک و مدیریت ریسک ارائه شده است در ادامه ابتدا عناصر مهم موجود در روش مدیریت و تحلیل ریسک تعریف می گردند.

۲-۲ مبنای کلی تحلیل ریسک در سیستم‌های مبتنی بر IT

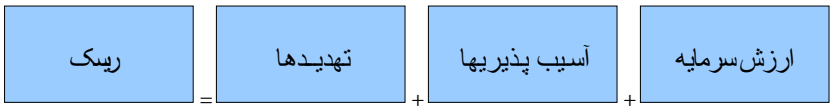
قبل از معرفی انواع روش‌های تحلیل ریسک لازم است مفاهیم پایه‌ای تحلیل ریسک توضیح داده شود .البته لازم به ذکر است که در مقوله امنیت اطلاعات و تحلیل ریسک، تعاریف مختلفی توسط محققین و

متخصصین این رشته برای عناصر مختلف موجود در تحلیل ریسک بیان شده است .ولی به طور کلی هدف تمامی این روش‌ها یکسان بوده و عبارت است از بین بردن یا به حداقل رساندن ریسک‌های امنیتی شناسایی شده در مجموعه تحت بررسی .

به دلیل پیچیدگی و گستردگی مفاهیم امنیت اطلاعات، تا بحال روش یکسان و قانونمندی برای انجام تحلیل ریسک امنیت اطلاعات به وجود نیامده است و روش‌های گوناگون و نظریه‌های مختلفی توسط کارشناسان این رشته، ارائه گردیده است .لذا هر سازمان باید با توجه به نیازمندی‌های امنیتی خاص خود و استفاده از افراد متخصص در این زمینه، بتواند با ترکیب روش‌های گوناگون موجود در زمینه تحلیل ریسک، روش تحلیل ریسکی که برآورده کننده نیازمندی‌های امنیتی خاص آن سازمان بوده را به وجود آورده و بر اساس آن روند تحلیل ریسک امنیت اطلاعات را در سازمان خود انجام دهد.

مفاهیم پایه‌ای زیر در تمامی روش‌های مختلف تحلیل ریسک، به عنوان مبنا و اساس روند در نظر گرفته می شوند:

ریسک : احتمال اینکه یک تهدید مشخص، بتواند از یک نقطه ضعف خاص موجود در سیستم استفاده نماید ریسک گفته میشود .تعریف دیگری از ریسک :ریسک به علت عدم قطعیت و وجود تردید به وجود می‌آید و به عنوان یکی از جنبه‌های کوشش افراد برای تخمین زدن و کنترل آینده می‌باشد و زندگی انسان‌ها شامل انواع تحلیل‌های ریسک کوچک و بزرگ می‌باشد . همچنین تعریف دیگری از ریسک عبارت است از :ریسک در هر زمینه، شامل مجموعه تهدیدها ، آسیب‌پذیریها و ارزش سرمایه‌های سازمان می‌باشد .در حقیقت داریم :



هر کدام از این فاکتورها افزایش یابند، ریسک زیاد شده و هر کدام که کاهش یابد، باعث کاهش یافتن ریسک می شود .M. Krause & Harold F. Tipton,(1998)