ارائه رویکردی جهت استقرار مدیریت پروژه امنیت اطلاعات بر اساس استاندارد PMBOK

ن همراهی[۱] ، ن مدیری[۲]
nassermodiri@yahoo.com ، n.hamrahi@gmail.com

چکیده

مدیریت پروژه های فناوری اطلاعات یکی از بدیع ترین مدیریت ها در دنیای امروز است. در این نوع مدیریت عمده تلاش بر ۳ اصل اساسی استوار است : ۱ - گرد آوری و ذخیره سازی اطلاعات ۲ - پردازش و سازماندهی اطلاعات ۳ - انتقال و نمایش اطلاعات [۳] . از طرفی با بسط روز افزون فناوری در دنیا، مدیریت این نوع از پروژه های قرن ۲۱ به مهارتها و قابلیت های متمایزتری نسبت به دیگر محدوده های مدیریتی احتیاج دارد. هدف از این مقاله بر آن است تا بر اساس یکی از معتبرترین استانداردهای مدیریت پروژه، یعنی استاندارد PMBOK ۲۰۱۲ مدلی را برای مدیریت پروژه های امنیت اطلاعات در پروژه هایی که تحت چارچوب فناوری اطلاعات تعریف می‌شود ارائه نماید. چارچوب این مدل بر ۵ فرآیند اساسی استوار است : فرآیند تعیین نیازها و انتظارات مشتری - فرآیند طرح ریزی جریان های کاری - فرآیند کار گروهی - فرآیند ارزیابی و اختتام - مدیریت پروژه های امنیت اطلاعات [۱,۱۲] .

در فرآیند تعیین نیازها و انتظارات مشتری، عمده فعالیت بر روی شناخت هر چه بیشتر و بهتر نیاز مشتری از اجرای پروژه مورد نظر بر اساس جدیدترین فناوری دنیا، استوار است. در فرآیند دوم یعنی فرآیند طرح ریزی جریان های کاری، با آگاهی و شناخت از توانائی ها و قابلیت های فناوری موجود و در دسترس، سازماندهی کاری جهت نیل به اجرایی نمودن پروژه انجام می پذیرد. در فرآیند سوم این سازماندهی، قابلیت اجرایی پیدا می نماید که این فعالیت های اجرایی، با ارزیابی و کنترل مستمر همراه است. در فرآیند چهارم، ارزیابی نهائی و اختتام پروژه، با ارائه اقلام قابل تحویل مبتنی بر فناوری اطلاعات انجام می پذیرد و در فرایند پنجم، نه مورد امنیت اطلاعات که عبارت اند از : مدیریت محدوده، تدارکات، هزینه، زمان، ریسک، ارتباطات، یکپارچگی، کیفیت و مدیریت منابع انسانی را مورد بررسی قرار داده و فلوچارتی بر اساس آن ها ارائه خواهیم نمود. همچنین سعی نگارنده در این مقاله بر آن است تا در کلیه فرآیندهای مذکور، چارچوب سیستماتیک استاندارد PMBOK ، مشتمل بر ورودی، ابزار و تکنیک و نیز خروجی را رعایت نماید.

کلمات کلیدی : پروژه های امنیت اطلاعات - مدیریت پروژه IT – استاندارد PMBOK – ISO ۲۷۰۰۰ – فناوری اطلاعات

۱- مقدمه

اهمیت مدیریت پروژه بیش از پیش در بسیاری از سازمانها نمود پیدا کرده است این امر بنا به دلایلی که در ادامه به توضیح آن خواهیم پرداخت، در حوزه فناوری اطلاعات (IT)، نقشی استراتژیک یافته است. در طول سالهای ۱۹۶۰ تا ۱۹۷۰ در صنعت کامپیوتر، القاب متفاوتی مانند برنامه ریز، متصدی یا مدیر وجود داشته است. اما، به مرور زمان، شرکت ها و سازمان ها در یافتند که به فردی نیازمند هستند تا قادر باشد با کاربران ارتباط بر قرار کند، زبانشان را بفهمد و سپس با ایجاد ارتباط با گروه فنی، نیازمندی های تجاری را به مشخصات فنی تبدیل کند. در تحقیقی که در سال ۱۹۹۵ و ۲۰۰۱ بطور جداگانه توسط مؤسسه تحقیقاتی استندیش گراپ انجام شد، نتایج جدول زیر بدست آمده است [۵] :

---

۱) * نوید همراهی – دانشجوی کارشناسی ارشد مهندسی نرم افزار – دانشگاه آزاد اسلامی واحد زنجان – دانشکده برق ، کامپیوتر و IT

۲) ناصر مدیری – استادیار دانشگاه آزاد اسلامی

جدول ۱ : مقایسه نتایج پروژه های فناوری اطلاعات در سال های ۱۹۹۵ و ۲۰۰۰

شرح	۱۹۹۵	۲۰۰۱
میزان پروژه های لغو شده قبل از انتهای کار	٪۳۱	بررسی نشد
میزان پروژه های موفق IT	٪۲،۱۶	٪۲۸
درصد تخطی از هزینه مصوب، زمان مصوب و یا هر دو	٪۸۸	بررسی نشد
درصد تخطی از هزینه مصوب، زمان مصوب و یا هر دو	۵۹ بیلیون$	۲۲ بیلیون$
هزینه پروژه های شکست خورده در IT	۸۱ بیلیون$	۷۵ بیلیون$
درصد پروژه های باز آغاز شده	٪۹۴	٪۶۷
درصد تخطی کلی از زمان مصوب	٪۲۲۲	٪۶۳
درصد تخطی کلی از هزینه مصوب	٪۱۸۹	٪۴۵

با توجه به نتایج فوق میتوان فهمید که مدیریت مناسب در این نوع پروژه ها تا چه میزان می تواند در کاهش مشکلات پروژه نقش داشته باشد !؟ در این مقاله نیز تلاش شده است تا با توجه به اهمیت موضوع، مدلی جهت مدیریت پروژه های امنیت اطلاعات طبق چهار چوب مدیریت پروژه های فناوری اطلاعات که اساس آن استاندارد مؤسسه PMI یعنی استاندارد PMBOK می باشد، ارائه گردد. در این راستا لازم است تا با چارچوب کاری این استاندارد که بعنوان بستر اصلی این مقاله انتخاب شده است، آشنا شویم.

۲- مدیریت پروژه ها بر اساس استاندارد PMBOK

مؤسسه مدیریت پروژه یا (PMI)، در سال ۱۹۶۹و با هدف جمع آوری سوابق و تجربیات محیط های مختلف مدیریتی تأسیس شد. این انجمن طی سمیناری در سال ۱۹۷۶ در مونترال، ایده مستندسازی تجربیات را در قالب استاندارد مطرح و سرآغازی برای تبیین « مدیریت پروژه» بعنوان یک حرفه می گردد. با شروع دهه هشتاد، پروژه ای توسط این انجمن برای ایجاد رویه ها و مفاهیم مورد نیاز حرفه مدیریت پروژه با سه محور عمده «تعیین مشخصه های علمی حرفه ای- اخلاقیات»، «مفاهیم و ساختار مدیریت پروژه – استاندارد»، «تعیین نحوه حرفه ای شدن- گواهینامه» تبیین گردید.

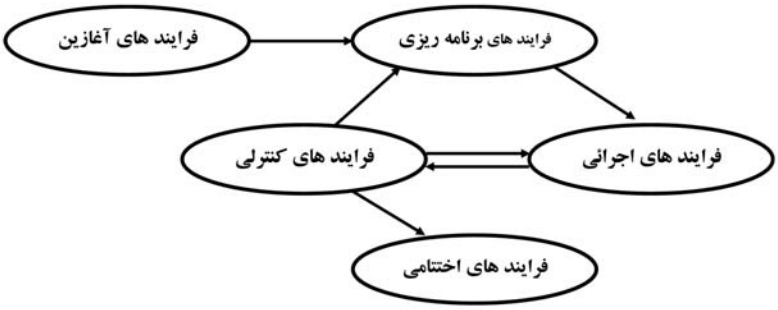
۲-۱ مفهوم پروژه : پروژه عبارت است از مجموعه تلاش های موقتی برای تحقق یک تعهد و تقبل در ایجاد یک محصول یا ارائه خدمات مشخص می باشد. اصطلاح "موقتی" بدین معنی است که پروژه ها در زمان های معین شروع و خاتمه می یابند. اصطلاح "مشخص" نیز به مفهوم این است که خدمت یا محصول مورد نظر کاملاً تعریف شده و روشن بوده و از نتایج حاصل از اجرای پروژه های دیگر متمایز می باشد[۱].

۲-۲- مفهوم مدیریت پروژه : مدیریت پروژه بکارگیری دانش، مهارت، ابزار و تکنیک های لازم در اداره جریان اجرای فعالیت ها، به منظور رفع نیازهای پروژه از طریق تحقق فرآیندهای آغازین، برنامه ریزی، اجرائی، کنترلی و اختتامی است.

۲-۳- فرآیندهای مدیریت پروژه : مدیریت پروژه، فرآیند مجموعه فعالیت های یکپارچه و بهم مرتبط می باشد و لذا کسب نتیجه هر یک از محدوده های مدیریت پروژه، معمولاً در سایر فعالیت ها نیز مؤثر است. تعامل بین محدوده ها دارای نتایج مثبت و منفی برای هر یک از آنان است.

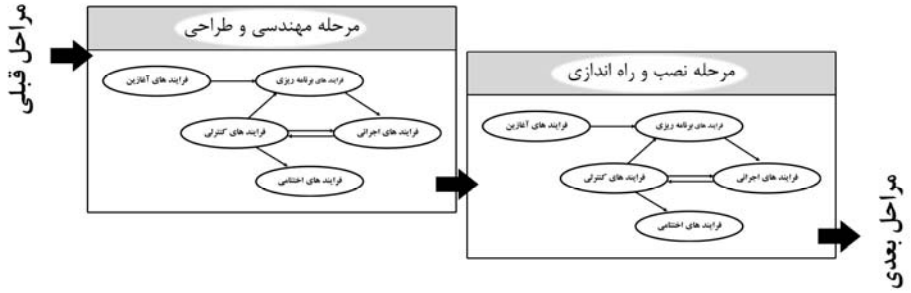
۲-۳-۱- ساختار فرآیندهای مدیریت پروژه : برای اجرای هر پروژه، مجموعه ای از فرآیندهای مختلف صورت می گیرد. شامل مجموعه فعالیت های لازم الاجرا برای حصول به یک نتیجه مشخص است. این فرآیندها توسط مجریان پروژه انجام می شود.

۲-۳-۲- گروه های فرآیندی : فرآیندهای مدیریت پروژه در قالب یکی از پنج گروه ذیل انجام می شوند : فرآیندهای آغازین فرآیندهای برنامه ریزی - فرآیندهای اجرائی - فرآیندهای کنترلی - فرآیندهای اختتامی. گروه های فرآیندی فوق از طریق نتایج حاصله از اجرای هر یک به یکدیگر مرتبط می شوند. این نتایج بصورت خروجی برخی و بعوانی ورودی برخی دیگر، مورد استفاده قرار می گیرد. این ارتباطات که از ابتدا تا انتهای پروژه بطور مداوم و چند سویه می باشد، در شکل یک ارائه شده است.



شکل ۱ : تعامل بین گروه های فرایندی مدیریت پروژه

در یک مرحله از اجرای پروژه، نهایتاً پس از تعامل کافی بین فرآیندهای مختلف، نتایج در قالب خروجی آن مرحله بطور کامل مشخص می شود تا بعنوان ورودی مرحله بعد مورد استفاده قرار گیرد. این مجموعه ارتباطات در شکل ۲ ارائه شده است.



شکل ۲ : تعامل بین مراحل اجرای پروژه

در ابتدای شروع هر یک از مراحل پروژه، توجه کافی به برخی از فرآیندهای آغازین در حفظ اهداف پروژه و تعهدات مجریان بسیار مؤثر است. اگر چه در شکل ۲ مراحل اجرای پروژه و فرآیندهای مدیریت پروژه بطور گسسته ارائه شده است. اما در اجرای پروژه به واقع این مراحل و فرآیندهای آنها از یکدیگر جدا نیستند.

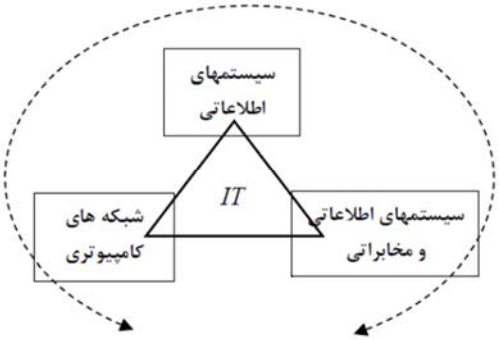
۲-۳-۲- تعامل بین فرآیندها : هر یک از گروه های فرآیندی (پنجگانه) نیز از مجموعه فرآیندهای کاملاًمشخصی تشکیل شده اند، که با یکدیگر مرتبط هستند. این ارتباط بصورت خروجی هر یک ورودی دیگری می باشد. هر یک از فرآیندها از سه بخش مجزای زیر تشکیل شده اند : ورودی ها - ابزار و تکنیک ها -خروجی ها .

۳- فناوری اطلاعات

فناوری ارتباطات‌واطلاعات تکنولوژی است که توسط آن داده‌های خام که دارای معنی و مفهوم قابل درک نیست در فرآیند تجزیه و تحلیل قرار گرفته و پس از آنکه دارای معانی قابل درک شده و به اطلاعات تبدیل شدند [۷].

۴ - مولفه ها و تعاریف بنیادین در فناوری اطلاعات (IT)

فناوری اطلاعات متکی بر مولفه ها و توانائی های سه بخش اصلی بنا شده است : سیستم های اطلاعاتی IS (Information System) - شبکه های کامپیوتری CN (Computer Networks) - سیستم های ارتباطی و مخابراتی CS (Communication System) - این سه بخش سه راس مثلث IT را تشکیل می دهند[۳] :

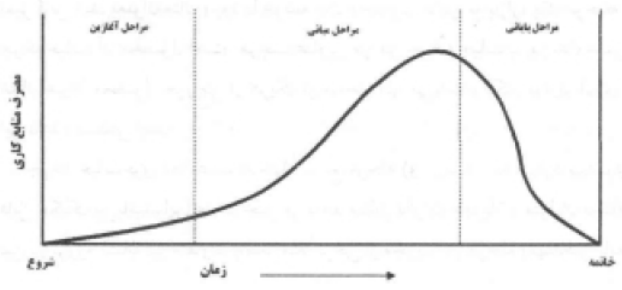


شکل ۳ : مولفه های بنیادین در فناوری اطلاعات

۵ - مشخصات مدیران پروژه های IT

مدیریت پروژه های فناوری اطلاعات ، بکارگیری دانش، مهارت، ابزار و تکنیک های لازمی است که مدیران پروژه ها با کمک آنها قادر به برنامه ریزی، سازماندهی، تخمین زنی و مدیریت پروژه های فناوری اطلاعات از طریق تحقق فرآیندهای آغازین،برنامه ریزی، اجرائی،کنترلی و اختتامی هستند. این مدیریت، هر نوع پروژه ای که هدف آن تکمیل، توسعه یا اجرای سخت افزاری و نرم افزاری کامپیوتری و نیز ارتباطات ویدئویی، صوتی و داده ای باشد را شامل است. تلاش عمده در این نوع پروژه ها بر روی یادگیری مفاهیم موجود در مدیریت محدوده، ریسک، هزینه، زمان و کیفیت پروژه استوار است. همچنین لازم است تا ضمن تعریف دقیق چرخه حیات پروژه، نسبت به مدیریت مراحل مختلف آن تدبیر مناسب اندیشیده شود. در این راه لازم است تا مدیر پروژه خصوصیات ذیل را داشته باشد : توانایی‌های فردی، توانایی‌های فنی، توانائی های مدیریتی، توانائی های تکمیلی .

۵-۱- چرخه حیات پروژه : چرخه حیات، نمایانگر مراحل اصلی و قدم های عمده در اجرای پروژه، از شروع تا خاتمه آن می باشد. اغلب چرخه های حیات پروژه دارای مشخصه های کلی به شرح ذیل می باشند : ۱ - میزان انجام هزینه ها و استفاده از نیروی انسانی در مراحل اولیه اجرای پروژه ها عموماًکمتر بوده، بمرور افزایش یافته و هنگامیکه پروژه به خاتمه نزدیک می شود، این میزان سریعاًکاهش می یابد. ۲ - در مراحل آغاز پروژه، احتمال موفقیت در انجام تعهدات و حصول کامل به نتایج از پیش تعیین شده کمتر است و بدین لحاظ میزان ریسک و عدم قطعیت بیشتر می باشد[۱].



شکل ۴ : چرخه حیات پروژه

۶ - مدل مدیریت پروژه‌های فناوری اطلاعات

در مدل تهیه شده جهت مدیریت پروژه های IT بر اساس استاندارد PMBOK با توجه به مشخصات پروژه ها و فرآیندهای وابسته به این نوع پروژه ها، چهار فرآیند تعیین نیازها و انتظارات مشتری، طرح ریزی جریان های کاری، کار گروهی و در نهایت ارزیابی و اختتام کار در نظر گرفته شده است که در این قسمت به تشریح هر کدام از این فرآیندها و مشخصات ورودی ها، تکنیک ها و خروجی های درگیر در هر کدام می پردازیم. کلیه این فرآیندها با یکدیگر مرتبط می باشند. این ارتباطات، نه تنها منحصر به حیطه هر یک از محدوده های مدیریت پروژه ها IT می باشد[۶].

جدول ۲ : فرایند مدیریت پروژه های فناوری اطلاعات

مدیریت پروژه فناوری اطلاعات (IT)			
مرحله اول	**مرحله دوم**	**مرحله سوم**	**مرحله چهارم**
فرایند تعیین نیاز ها و انتظارات مشتری	**فرایند طرح ریزی جریان های کاری**	**فرایند کار گروهی**	**ارزیابی و اختتام کار**
۱ – ورودی ها	**۱ – ورودی ها**	**۱ – ورودی ها**	**۱ – ورودی ها**
۱ – شرح محصول خروجی پروژه ۲ – برنامه استراتژیک ۳ – اطلاعات و سوابق مرتبط ۴ – شناسایی نیاز های مشتری	۱ – منشور پروژه ۲ – ساختار شکست کار ۳ – شرح محصول پروژه ۴ – فرضیات عمده ۵ – محدودیت های کاری و محیطی ۶ – اطلاعات و سوابق مرتبط	۱ – برنامه گذار پروژه ۲ – ساختار شکست کار ۳ – مشخصات کارکنان ۴ – بازتاب خارجی ۵ – الگوی کاری ۶– محدودیت های کاری و محیطی	۱ – مستندات اندازه گیری عملکرد ۲ – مستندات نتایج کار ۳ – سایر مستندات پروژه
۲ – تکنیک ها و ابزارها	**۲ – تکنیک ها و ابزارها**	**۲ – تکنیک ها و ابزارها**	**۲ – تکنیک ها و ابزارها**
۱ – برگزاری جلسات مشترک ۲ – آراء و نظرات خبرگان	۱ - آراء و نظرات خبرگان ۲ – بررسی مشخصه های انتخاب ممکن ۳ – الگو ها ۴ – روش ها و رویه های کاری ۵ – تئوری سازمانی ۶ – معماری اطلاعات سازمان	۱ – کار گروهی ۲ – فرم های کنترلی ۳ – مهارت های عمومی مدیریت ۴ – آموزش ۵ – نظارت ۶ – ارزیابی عملکرد	۱ – ممیزی نتایج ۲ – ارزیابی عملکرد
۳ – خروجی ها	**۳ – خروجی ها**	**۳ – خروجی ها**	**۳ – خروجی ها**
۱ – منشور پروژه ۲ – انتخاب مدیر پروژه ۳ – شناسایی محدودیت های کاری و محیطی ۴ – شناسایی فرضیات عمده	۱ – برنامه گذار پروژه ۲ – مستندات تفصیلی ۳ – شناسایی رویدادهای بالقوه مخاطره آمیز	۱ – نتایج کار ۲ – برنامه گذار بهنگام شده ۳ – اقدامات اصلاحی ۴ – مستند سازی تجربیات	۱ – بایگانی پروژه ۲ – صدور تائیدات

۶-۱- فرآیند تعیین نیازها و انتظارات مشتری : در فرآیند تعیین نیازهای مشتری، با انجام بررسی و مطالعات لازم، در خواست مشتری کاملاًمشخص میگردد تا مشخصه محصول خروجی پروژه (سخت افزاری و نرم افزاری) دقیقاً منطبق با این درخواست باشد.

۶-۲- فرآیند طرح ریزی جریان های کاری : در فرآیند طرح ریزی جریانهای کاری، بعد از انجام بررسی و مطالعات لازم در مورد درخواست مشتری، برنامه ریزی اجرایی کار مشخص می شود. در این راستا نتایج سایر فرآیندهای برنامه ریزی در یک مجموعه منسجم و واحد یکجا گرد هم می آیند.

۶-۳- فرآیند کار گروهی : با توجه به اینکه در پروژه های IT متخصصین مختلفی از جمله برنامه نویسان، مهندسان،تکنسین‌ها و... وجود دارند، لذا استفاده موثر از این نیروها اجتناب ناپذیر می باشد. فرآیند کار گروهی، فرآیندی است که با بکارگیری نیروی انسانی مورد نیاز (بصورت گروهی) و واگذاری مسئولیت برای انجام فعالیت های پروژه، این مهم را به انجام می رساند.

۶-۴- فرآیند ارزیابی و اختتام کار : فرآیند ارزیابی و اختتام کار، فرآیند پایان بخشیدن به پروژه یا یک مرحله پروژه، پس از تحقق اهداف و نتایج پیش بینی شده و یا حتی به دلایل دیگر می باشد. این فرآیند شامل بازرسی نتایج پروژه، توسط متولیان و دست اندرکاران کلیدی صاحبان و حتی مشتریان و همچنین مستند سازی می باشد.

۷ - ارائه مدل مدیریت پروژه های امنیت اطلاعات بر اساس استاندارد PMBOK

در حال حاظر فلوچارت مدیریت پروژه های IT را مورد بررسی قرار دادیم . حال طبق بررسی های بعمل آمده فرایند مدیریت پروژه های امنیت اطلاعات را مطابق با ISO ۲۷۰۰۰ به فلوچارت مذکور اضافه نموده و به شرح آن می‌پردازیم [۱۳,۴]:

جدول ۳ : فرایند مدیریت پروژه های امنیت اطلاعات

مدیریت پروژه امنیت اطلاعات بر اساس استاندارد PMBOK			
مرحله اول	**مرحله دوم**	**مرحله سوم**	**مرحله چهارم**
فرایند تعیین نیاز ها و انتظارات مشتری	**فرایند طرح ریزی جریان های کاری**	**فرایند کار گروهی**	**ارزیابی و اختتام کار**
فرایند مدیریت امنیتی تدارکات و محدوده پروژه	**فرایند مدیریت امنیتی هزینه و زمان پروژه**	**فرایند مدیریت امنیتی ریسک و ارتباطات پروژه و منابع انسانی**	**فرایند مدیریت امنیتی یکپارچگی و کیفیت پروژه**
۱ – مدیریت تدارکات پروژه امنیتی ۲ –مدیریت محدوده پروژه های امنیتی	۱ – مدیریت هزینه پروژه امنیتی ۲ – مدیریت زمان پروژه امنیتی	۱ – مدیریت ریسک پروژه امنیتی ۲ – مدیریت ارتباطات پروژه امنیتی ۳ – مدیریت منابع انسانی پروژه	۱ – مدیریت یکپارچگی پروژه امنیتی ۲ – مدیریت کیفیت پروژه امنیتی

۷-۱ – مرحله اول :

۷-۱-۱- مدیریت تدارکات پروژه امنیتی : مدیریت تدارکات در هر پروژه ای، کالا و خدمات مورد نیاز جهت انجام آن پروژه را از خارج از آن سازمان تامین می کند. در خصوص پروژه های امنیتی نکته در این است که این موضوع دلیلی برای ارتباط نفرات دخیل در پروژه امنیتی با خارج از سازمان است. لذا شناخت و اعتماد سازمان مجری، به افراد تدارکات بسیار ضروری است. چرا که از همین ارتباطات ساده، اطلاعات یک پروژه امنیتی می تواند فاش شود و بر سرنوشت آن پروژه تاثیر بگذارد. در گام اول باید نیازهایی از پروژه که می توان آنها را از خارج سازمان پروژه تامین کرد شناسائی شده و تعیین شود که آیا این تدارک انجام شود یا خیر؟، در صورت پاسخ مثبت چگونگی انجام باید مشخص شود، مقدار تدارک و زمان آن نیز باید معین شود. پس از آن باید برای پشتیبانی از این درخواست

تدارکات، اسناد آن آماده سازی شوند. در گام بعدی باید از فروشندگان آتی تدارکات پیشنهادهای بهاء و طرحهای پیشنهادی در مورد چگونگی تحقق نیازهای پروژه اخذ شود. پس از این کار باید برای انجام امور تدارکات یک منبع تدارکات در خارج از سازمان را انتخاب نمود، که برای این انتخاب باید بر اساس معیارهای مهم برای سازمان پروژه ارزیابی از منبع انجام شده و انتخاب آن صورت پذیرد. در پروژه های امنیتی یا پروژه های غیر امنیتی که کاربرد امنیتی دارند اینکه سازمان پروژه از منبع تدارکات در خارج از سازمان چه میزان شناخت دارد و چه میزان به آن اعتماد دارد یکی از اصلی ترین ملاکهای ارزیابی منابع تدارکات در پروژه های امنیتی است. در گام نهائی باید طی روشی، اطمینان حاصل نمود که عملکرد فروشنده(منبع تدارکات) الزامات پیمان را محقق می سازد. و با صحت سنجی محصول و ثبت و بروز آوری سوابق به منظور انعکاس بهتر نتایج نهائی، فرآیند اجرای تدارکات را خاتمه داد[۱۵].

۷-۱-۲- مدیریت محدوه پروژه امنیتی : مدیریت محدوده پروژه های امنیتی در واقع یعنی تعیین مرز اینکه چه کاری را می توان به شرکت های اقماری داد و چه کاری باید حتما در انحصار تیم خود مجموعه امنیتی باشد. پس از اینکه با کار کارشناسی دقیق و گسترده محدوده امور مربوط به تیم خود مجموعه و شرکت های اقماری مشخص شد گام بعدی تصویب رسمی پروژه است که شروع کار در اینجاست. در گام بعدی، این پروژه تصویب شده باید مستند سازی شود و هر یک از بخش های آن به تفصیل شرح داده شود. نکته اینکه هر بخش از این مستند فقط باید در اختیار کسی قرار گیرد که باید آن کار را انجام دهد و کل آن فقط باید در اختیار تیم مدیریت پروژه باشد. در تدوین بخش ها باید تا حد ممکن هر بخش مستقل از دیگری باشد لیکن بخش ها از محدوده اصلی کار خارج نشوند تا قابل کنترل و مدیریت باشند. پس از شفاف شدن حد و مرزهای اصل پروژه و بخش های آن، گام بعدی پذیرفتن رسمی این محدوده ها توسط سازمانها یا اشخاص حقوقی ذینفع در پروژه است. نتیجه این گام آن است که هر یک از بخش های این کار امنیتی از نگاه مسئولیتهای مختلف مورد بازبینی امنیتی قرار می گیرد و در صورت عدم مشکل تایید می شود. در گام پایانی نوبت به اتفاقاتی می رسد که محدوده پروژه امنیتی را تغییر می دهند و آنهایی که این محدوده را تغییر نمی دهند. اگر یک اتفاق رخ دهد که تیم مدیریت پروژه امنیتی تایید کند که در محدوده پروژه اثر گذار است، آنچه که تا کنون بیان شد باید از ابتدا مورد بازبینی قرار گیرد. در گام پایانی باید افرادی در جلسه تصمیم گیری حضور داشته باشند که در آن سازمان از مقام بالایی برخوردار باشند تا بتوانند مسئولیت و تبعات تصمیمات متخذه را بر عهده بگیرند[۱۵].

۷-۲ – مرحله دوم :

۷-۲-۱- مدیریت هزینه پروژه امنیتی : مدیریت هزینه پروژه ها در بر گیرنده فرآیندهای مورد نیاز برای حصول اطمینان از تکمیل پروژه با بودجه مصوب است. حال با توجه به اینکه در تمام سازمانها علاقه زیادی به کاهش هزینه های تمام شده هر پروژه وجود دارد، ممکن است دشمنان به روشهای مختلف حاضر باشند حتی بخش از یک پروژه امنیتی را رایگان انجام دهند، فقط برای اینکه درون تیم نفوذ کرده و اطلاعات کسب کنند. در مدیریت هزینه پروژه های امنیتی توجه به این نکته بسیار ضروری است. در این راستا باید برنامه ریزی کرد که چه منابعی و از هر منبع چه میزان و در چه زمانی برای انجام فعالیت های پروژه مورد نیاز است. در گام بعدی برای منابع مورد نیاز باید یک برآورد هزینه انجام داد تا بتوان یک تخمین از هزینه کل پروژه را بدست آورد. سپس باید این هزنیه را به تک تک فعالیت ها یا بسته های کاری جهت تشکیل مبنای هزینه برای اندازه گیری عملکرد پروژه شکست و به هر

یک تخصیص داد و پس از آن در صورت وقوع هر نوع تغییر احتمالی، باید این تغییر توسط ذی نفعان پروژه مورد توافق قرار گیرد و هزینه مبنای تغییر یافته تشخیص داده شود. و این تغییرات واقعا در لحظه وقوع مدیریت و کنترل شوند[۲,۱۵].

۷-۲-۲- مدیریت زمان پروژه امنیتی : همان طور که می دانید هر کاری که در عمل به طولانی شدن زمان اجرا برخورد کرد، در حاشیه قرار خواهد گرفت و کارهای مهم تر از آن برای آن سازمان به وجود خواهد آمد. در این بین احتمال فاش شدن اطلاعات و اسناد پروژه به علت طولانی شدن زمان اجرا بسیار زیاد می شود. پس در مدیریت زمان پروژه های امنیتی باید از به وقوع پیوستن تعلل در کار جلوگیری کرد. مدیریت زمان در هر پروژه ای دربرگیرنده فرآیندهای مورد نیاز جهت حصول اطمینان از تکمیل به موقع پروژه است. برای انجام این مدیریت باید بدانیم کل پروژه شامل چه کارهائی است و هر کار نیز شامل چه بخش هائی است. تمام این موارد باید شناسائی شوند و مستندات آنها تولید گردد که بهترین منبع برای این کار ساختار شکست کار (WBS) است.

۷-۳ – مرحله سوم :

۷-۳-۱- مدیریت ریسک پروژه امنیتی : این نوع مدیریت بر پروژه ها تضمین می کند که آثار مثبت رویدادها به میزان حداکثر، و آثار منفی آن به میزان حداقل بر پروژه تاثیر بگذارد و در آن فرآیندهایی وجود دارد تا ریسکهای پروژه شناسائی، تحلیل و نسبت به آنها واکنش مناسب اتخاذ شود. لیکن در پروژه های امنیتی رویدادهایی که تاثیرگذار هستند ویژگیهای خاصی دارند که از جمله آنها می توان به این مطلب اشاره کرد که باید خیلی سریع به آن رویدادها پاسخ داد و در صورت از دست دادن زمان و طولانی شدن فرآیند پاسخ دهی، پاسخ قبلی در زمان فعلی راه حل مناسبی نخواهد بود. پس سرعت عمل در واکنش مناسب به ریسکی که شناسائی شده و تحلیل مناسب روی آن انجام شده است مطلب بسیار مهمی است. شناسائی ریسک فرآیندی تکرارپذیر است که در مقاطع زمانی مختلف باید انجام شود. سپس باید ریسکهای شناسائی شده را تحلیل کنیم تا تاثیر و شانس وقوع آنها سنجیده شود. به این وسیله ریسکها را بر اساس آثار بالقوه آنها بر اهداف پروژه اولویت بندی می کنیم. سپس باید تحلیل عددی احتمال هر ریسک و پیامدهای آن بر اهداف پروژه را برای داشتن تحلیل کمی ریسک استخراج کنیم. در گام بعدی باید اقداماتی انجام داد تا فرصتها افزایش، و تهدیدها کاهش یابد و برای انجام این کار باید افراد یا قسمتهایی به منظور پذیرش مسئولیت هر واکنش به ریسک شناسائی و تعیین گردند. با این کار در واقع برنامه ریزی واکنش به ریسک را انجام داده ایم. این برنامه باید با شدت ریسک متناسب باشد، در مواجهه با چالشها از نظر هزینه ای اثر بخش باشد، برای موفقیت آمیز بودن به هنگام باشد، با توجه به شرایط پروژه واقع بینانه باشد، مورد توافق همه قسمتهای درگیر باشد و توسط یک شخص مسئول پذیرفته شده باشد. در گام آخر باید یک کنترل و نظارت بر ریسکها داشت که شامل فرآیند پیگیری ریسکهای شناسائی شده، نظارت بر ریسکهای باقیمانده و شناسائی ریسکهای جدید، اطمینان از اجرای برنامه های ریسک و ارزیابی اثر بخشی آنها در کاهش ریسک می باشد. آنچه واضح است اینکه حوزه مدیریت ریسک حساس ترین حوزه مدیریت یک پروژه امنیتی است که در صورت مدیریت صحیح نتایج مثبت پروژه و در صورت سهل انگاری لغو پروژه را در پی دارد[۱۰].

۷-۳-۲- مدیریت ارتباطات پروژه امنیتی : مدیریت ارتباطات در پروژه ها تنظیم کننده روابط بین افراد، نظرات و اطلاعاتی است که برای موفقیت پروژه لازم هستند. حال در پروژه های امنیتی آنچه از این موضوع اهمیت دارد این است که اگر پازل اطلاعات ذهنی افراد پروژه در کنار یکدیگر قابلیت تکمیل شدن داشته باشد، آنگاه احتمال فاش

شدن ماهیت پروژه وجود دارد که باید از وقوع آن جلوگیری کرد. در گام اول باید برای این ارتباطات برنامه ریزی کنیم. در گام بعدی برای آگاهی از نحوه مصرف منابع در راستای اهداف پروژه باید اطلاعات عملکردی پروژه به منظور گزارش دهی، گردآوری شود. و در نهایت باید نتایج پروژه مستندسازی شده تا محصول پروژه توسط سرمایه گذار پذیرش رسمی گردد[۴,۱۴].

۷-۳-۳- مدیریت منابع انسانی پروژه امنیتی : در پروژه ها معمولا مدیریت منابع انسانی دربرگیرنده فرآیندهایی است که برای دست یابی به اثربخش ترین کاربری از افراد درگیر در پروژه لازم می باشد. آنچه که در مورد پروژه های امنیتی در این بخش اهمیت دارد این است که تمام تیم نیروی انسانی پروژه باید کارمندان رسمی آن سازمانی باشند که قصد اجرای یک پروژه امنیتی را دارد و در صورت ضعف در دانش فنی برای این تیم کلاس آموزشی درنظر گرفته شود. زیرا دانش فنی کار را می توان با کلاس آموزشی به یک نفر انتقال داد لیکن اعتماد و اطمینان به یک نیروی سازمانی، با برگزاری کلاس آموزشی تامین نمی شود. برای انجام این مهم در گام اول باید اقدام به شناسائی، مستندسازی و واگذاری نقش ها و مسئولیتها در پروژه کرد که هر کدام از آنها می تواند به افراد یا گروه های کاری واگذار گردد.

۷-۴ – مرحله چهارم :

۷-۴-۱- مدیریت یکپارچگی پروژه امنیتی : در این بخش فرآیندهایی از استاندارد PMBOK مطرح است که اطمینان می دهد هماهنگی مناسبی بین عناصر مختلف پروژه امنیتی اتفاق می افتد. برای کنترل این هماهنگی کار را در سه بخش انجام می دهیم: ۱- تدوین برنامه ای برای این کنترل: برنامه ای که بتواند عناصر مختلف پروژه امنیتی را کنترل و هماهنگ کند. ۲- اجرای این برنامه: در اجرای برنامه های تدوین شده، دقت در اجرا ضامن کیفیت خروجی کار است. ۳- کنترل تغییرات احتمالی: در کنترل تغییرات قدم نخست تشخیص و تعیین این مطلب است که یک تغییر رخ داده است. پس از آن کنترل و مدیریت آن تغییر دارای اهمیت است و در نهایت حصول اطمینان از اینکه آن تغییر پذیرفته شده است یا خیر.

۷-۴-۲- مدیریت کیفیت پروژه امنیتی : مدیریت کیفیت پروژه ها دربرگیرنده فرآیندهایی است برای تامین اطمینان اینکه نیازهایی که پروژه به خاطر آنها تعهد شده است حتما حاصل می شوند. نکته مهم برای پروژه های امنیتی در این است که اگر کیفیت کار پائین بیاید نمی گوئیم کار با کیفیت پائینی انجام شده. بلکه ممکن است کاهش کیفیت، کل اصل کار پروژه را لغو کند، آن هم به دلیل مسائل امنیتی. پس تامین کیفیت پروژه در پروژه های امنیتی اهمیتی دو چندان دارد[۸].

۸- نتیجه گیری و فعالیت های آتی

هدف از این مقاله بررسی مدیریت پروژه های امنیت اطلاعات در حوزه فناوری اطلاعات (IT) بر اساس استاندارد PMBOK بوده است. در این راستا، لزوم مدیریت خاص در این نوع پروژه های ، بر اساس یک استاندارد معتبر، مورد توجه قرار گرفت. لذا استاندارد موسسه PMI ، به عنوان بستر اصلی مورد توجه قرار گرفت. لذا ضمن مروری کلی بر سابقه این استاندارد، مباحث مهم مدیریت پروژه فناوری اطلاعات از جمله تعاریف پروژه و مدیریت پروژه، فرآیندهای مختلف پروژه و نحوه تقابل آنها از دیدگاه این استاندارد مورد بررسی قرار گرفت.

در ادامه نیز ضمن بررسی تاریخچه IT، مدل مدیریتی این نوع پروژه ها براساس استاندارد PMBOK مشتمل بر چهار فرآیند تعیین نیازها و انتظارات مشتری، فرآیند طرح ریزی جریان های کاری، فرآیند کار گروهی و نیز فرآیند ارزیابی و اختتام کار تدوین و بسط داده شد. سپس با وارد نمودن مراحل امنیت اطلاعات طبق استاندارد ISO ۲۷۰۰۰ مدلی جهت مدیریت این نوع پروژه ها مشتمل بر نه فرایند جزئی بیان گردید.

از جمله فعالیت های آتی که در این زمینه می توان انجام داد، میتوان به موارد ذیل اشاره کرد :

- بسط و توسعه مدل فوق در جهت بهینه کردن فاکتورهای اساسی پروژه (زمان- هزینه – ریسک).
- بررسی عملی مدل فوق در محیط های اجرائی
- تحلیل و بررسی مدل فوق بر اساس استانداردهای دیگر مدیریت پروژه

۹- منابع و مأخذ

۱ - راهنمای مدیریت پروژه / تالیف انجمن مدیریت پروژه PMI / مترجم : مترجمین سیدحسین اصولی، نجابت، علی بیاتی، حسین ناصری، علی افخمی تهران/شرکت ملی صنایع پتروشیمی،۱۳۸۴ /

۲ - بهترین ها در امنیت اطلاعات / جرج ال استفانک / ترجمه و نگارش دکتر علیرضا پورابراهیمی ، دکتر عباس طلوعی اشلقی / انتشارات دانشگاه آزاد اسلامی واحد الکترونیکی / چاپ اول تابستان ۱۳۸۹ /

۳ - فناوری اطلاعات ، فنون امنیتی – آیین کار مدیریت امنیت اطلاعات / استاندارد ایران – ایزو – آی ای سی ۲۷۰۰۲ / موسسه استاندارد و تحقیقات صنعتی ایران / چاپ اول ۱۳۸۶ /

۴ - آشنائی با ISMS و استانداردهای امنیتی ISO ۲۷۰۰۱ و ISO ۲۷۰۰۲ / نوشته حیدر علی کورنگی / دیماه ۱۳۸۶ / کتاب جهت استفاده در سمینارهای شبکه علمی مجاز می باشد /

۵ - مدیریت و کنترل پروژه های فناوری اطلاعات/ جک تی . مارچوکا / ترجمه مهندس رامین مولاناپور ، مهندس فرزاد حبیبی پور رودسری / چاپ دوم اسفند ۱۳۸۸ /

۶- مقاله ارائه مدلی جهت مدیریت پروژه های فناوری اطلاعات / احمد زاده قاسم آبادی /

۷ - راهنمای امنیت فناوری اطلاعات / دبیرخانه شورای عالی انفورماتیک / تیر ۱۳۸۴ /

۸ - Information Security Management Metrics : A Definitive Guide to Effective Security Monitoring and Measurement / by W.Krag Brotby , CISM / CRC Press , Taylor & Francis Group , an informa business , ۲۰۰۹

۹- IT Security Metrics : A Practical Framework for Measuring Security & Protecting Data / by Lance Hayden , Ph.D. / Mc Graw Hill , ۲۰۱۰

۱۰- Risk Analysis and Security Countermeasure Selection / by Thomas L.Norman, cpp/psp/csc / CRC Press , Taylor & Francis Group , an informa business , ۲۰۱۰ / ISBN ۹۷۸-۱-٤۲۰۰-۷۸۷۰-۱

۱۱- Security Strategy : From Requirements to Reality / by Bill Stackpole and Eric Oksendahl / CRC Press . Taylor & Francis Group , an informa business , ۲۰۱۱

۱۲- Management Information Systems : James A.O´ Brien , George M.Markas / Ninth edition / Mc Grow Hill / ۲۰۰۹

۱۳- ISO/IEC ۲۷۰۰۱ & ۲۷۰۰۲ implementation guidance and metrics / Prepared by the international community of ISO ۲۷k implementers at ISO۲۷۰۰۱security.com/ Version ۱ ۲۸$_{th}$ June ۲۰۰۷

۱٤- ITIL V۳ and Information Security / by : Jim Clinch / White Paper , May ۲۰۰۹

۱۵- http://www.۲۷۰۰۰.ir