نگاهی به استانداردهای حوزه امنیت اطلاعات

جواد منزوی بزرگی، مجتبی انصاریان

تاریخ دریافت : ۱۳۹۰/۰۸/۲۹
تاریخ پذیرش : ۱۳۹۰/۱۱/۰۳

چکیده:

با شکل‌گیری اندیشه‌ی ایجاد یک استاندارد در حوزه امنیت اطلاعات در کشور انگلستان و انتشار اولین نسخه ی استاندارد در سال ۱۹۹۵م و تقویت نگاه سیستمی به مقوله امنیت اطلاعات، تحولات گسترده ای در این بخش صورت گرفته است. در این زمینه، موسسه بین المللی استاندارد (ISO) با همکاری و پیشگامی موسسه استاندارد انگلستان (BSI) تا کنون چندین استاندارد و گزارش فنی منتشر نموده است. این مقاله ضمن اشاره به سیر پیدایش و تکامل استانداردهای حوزه امنیت اطلاعات به معرفی اجمالی استانداردها و همچنین ترسیم وضعیت فعلی اسناد بالادستی کشور در این بخش و لزوم حرکت پر شتاب تر آن خصوصاً در بخش دفاعی پرداخته است.

واژگان کلیدی:

استانـــــدارد، امنیـــت، امنـــیت اطلاعات، فناوری اطلاعات، ارتباطات

۱- مقدمه

با مطرح شدن موضوع مدیریت امنیت اطلاعات در دهه ۹۰ م، نگاه تک بعدی فنی به مقوله امنیت کمرنگ شد و جای خود را به نگرش سیستمی(چند بعدی) در این بخش داد. امنیت اطلاعات در این دهه منوط به وجود خطی مشی امنیت اطلاعات، ساختارهای سازمانی و هم‌چنین تعریف و تبیین استراتژی‌ها و اتخاذ سیاست‌های امنیتی بر اساس نیازهای اصلی سازمان و مدیریت آن گردید. در همین راستا مجموعه‌ای از استانداردهای مدیریتی و فنی در حوزه امنیت اطلاعات و ارتباطات ارایه شده‌اند که از آن جمله می‌توان به استانداردهای مدیریتی و هم چنین گزارش‌های فنی موسسه بین‌المللی استاندارد و موسسه استاندارد انگلستان که از پیشگامان این حوزه بوده است، اشاره نمود.

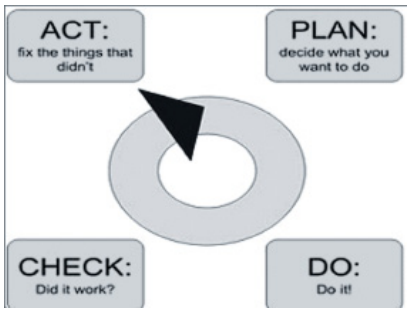
۲- تاریخچه ایجاد استانداردها در حوزه امنیت

منشاء اولین استاندارد در حوزه امنیت یعنی[1] BS۷۷۹۹ به زمان تاسیس مرکز امنیت رایانه‌های بازرگانی[2] و شکل‌گیری بخش صنعت و تجارت انگستان[3]در سال ۱۹۸۷م برمی‌گردد. این مرکز با هدف تعریف معیارهای بین المللی برای ارزیابی میزان امنیت تجهیزات تولید شده توسط سازندگان تجهیزات امنیتی تشکیل گردید تا از این طریق تاییدیه و گواهی نامه های مربوطه و آموزش لازم را به کاربران ارایه نماید. مرکز CCSC در سال ۱۹۸۹ اقدام به انتشار شناسه هایی(کدهایی) با عنوان Practice Users Code ofبرای سنجش میزان امنیت نمود. پس از آن اجرایی بودن شناسه‌ها از نگاه کاربران توسط مرکز محاسبات بین المللی[4]و کنسرسیوم کاربران صنایع انگلستان مورد بررسی قرار گرفت (دشتی، ۵۴:۱۳۸۴) .

در سال ۱۹۹۵ این استاندارد با عنوان BS۷۷۹۹ منتشر شد و

1- British Standard 7799
2- Commercial Computer Security Center(CCSC)
3- UK Department of Trade and Industry (DTI)
4.National Counting Center(NCC)
5. Information Security Management System(ISMS)

قسمت دوم آن نیز در اوایل سال ۱۹۹۸م به آن اضافه گردید. این قسمت مفهوم سیستم مدیریت امنیت اطلاعات[5] را به‌وجود آورد. نسخه بازنگری شده ی این استاندارد در سال ۱۹۹۵م به عنوان استاندارد پذیرفته شده ی سازمان بین المللی استاندارد[1] و تحت عنوان ISO/IEC ۲۷۰۰۱ یا همان ISMS به ثبت رسید. در سال ۲۰۰۰م با افزودن الحاقیه‌هایی به استاندارد BS۷۷۹۹ که به عنوان یک استاندارد ISO ثبت شده بود، این استاندارد تحت‌عنوان استاندارد ISO/IEC ۱۷۷۹۹ به ثبت رسید. نسخه جدید و قسمت دوم این استاندارد در سال ۲۰۰۲م به منظور ایجاد هماهنگی بین این استاندارد مدیریتی و سایر استانداردهای مدیریتی نظیر ISO ۹۰۰۱ و ISO ۱۴۰۰۱ تدوین گردید(Broderick . ۲۰۰۶,۲۶-۳۱). این قسمت برای ارزیابی میزان موثر بودن سیستم ISMS در یک سازمان مدل Plan-Do-Check-Act (PDCA) را همان‌گونه که در شکل ذیل نشان داده شده است، ارایه می‌نماید. به عبارت دیگر با شکل گیری نگاه سیستمی به مقوله امنیت اطلاعات، تامین امنیت اطلاعات در یک سازمان، به صورت آنی مقدور نبوده و لازم است این امر طی یک فرآیند مداوم و در یک چرخه ایمن سازی شامل مراحل طراحی[2] ، پیاده سازی[3] ، ارزیابی[4] و اصلاح[5] انجام گیرد. پس از آن مجموعه استانداردهای خانواده ISO ۲۷۰۰۰ از سال ۲۰۰۵م به بعد به صورت مستمر در حوزه‌ی مدیریت امنیت اطلاعات ارایه و منتشر گردید(دشتی، پیشین).



۱-۲- استاندارد BS۷۷۹۹

این استاندارد به چگونگی پیاده سازی امنیت در همه ی ابعاد در یک سازمان مربوط است و به معرفی روش های استانداردی می‌پردازد که از طریق آن ایمنی ساختار سازمان برای اجرا و پیاده‌سازی فناوری اطلاعات امکان پذیر باشد.BS۷۷۹۹ حفاظت از اطلاعات را در سه مفهوم محرمانگی و قابل اطمینان بودن اطلاعات[6] ، صحت و پیوستگی اطلاعات[7] و در دسترس بودن اطلاعات[8] تعریف می کند. این استاندارد جزییات و چگونگی‌ها را مطرح نمی کند بلکه سرفصل‌ها و موضوعات کلی را بیان می کند. نسخه اولیه این استاندارد متشکل از ۳۵ هدف امنیتی در ۱۰ گروه کنترلی و در مجموع ۱۲۷ اقدام بازدارنده جهت تامین اهداف تعیین شده برای استقرار یک سیستم مدیریت امنیت اطلاعات می‌باشد. گروه های ده گانه این استاندارد عبارتند از:

۱- سیاست های امنیتی؛
۲- تشکیلات امنیت سازمان؛
۳- کنترل و طبقه بندی دارایی ها؛
۴- امنیت فردی؛
۵- امنیت فیزیکی و پیرامونی؛
۶- مدیریت ارتباطات و بهره برداری؛
۷- کنترل دسترسی ها؛
۸- راه ها و روش ها ی نگهداری و بهبود اطلاعات؛
۹- مدیریت تداوم فعالیت سازمان؛
۱۰- سازگاری با موارد قانونی (www.iso.org, ۲۰۱۲-۰۴-۰۶)

گفتنی است که نسخه اولیه این استاندارد دارای دو بخش اصلی می باشد. بخش اول آن به ارایه سیاست ها و خط مشی‌ها در حوزه امنیت اطلاعات پرداخته و بخش دوم آن به دریافت و ارایه گواهی‌نامه مرتبط می باشد. در آخرین ویرایش صورت گرفته، این استاندارد در دو بخش دستورالعمل های اجرایی و مشخصات سیستم های مدیریت امنیت اطلاعات سازماندهی گردیده است. در این استاندارد تعیین مراحل ایمن سازی و نحوه ی شکل گیری چرخه امنیت، جزییات مراحل ایمن سازی و تکنیک‌های فنی مورد استفاده در هر مرحله، فهرست و محتوی طرح ها و برنامه‌های امنیت اطلاعات مورد نیاز سازمان، ضرورت و جزییات ایجاد تشکیلات سیاستگذاری، اجرایی و فنی تامین امنیت، کنترل‌های امنیتی مورد نیاز برای هر یک از سیستم های اطلاعاتی و ارتباطی، تعریف سیاست‌های امنیت اطلاعات، تعریف قلمروی سیستم مدیریت امنیت اطلاعات و مرزبندی آن متناسب با نوع نیازهای سازمان، انجام و پذیرش برآورد مخاطرات متناسب با نیازهای سازمان، پیش بینی زمینه ها و نوع مخاطرات بر اساس سیاست‌های امنیتی تدوین

1. International Standard Organization(ISO)
2. Plan
3. Do
4. Check
5. Act
6.Cofidentiality
7.Integrity
8.Availability

شده، انتخاب هدف‌های کنترل و کنترل‌های مناسب که قابل توجیه و تدوین دستورالعمل‌های عملیاتی از جمله سرفصل‌های مرتبط با نحوه‌ی پیاده‌سازی امنیت در یک سازمان می‌باشند. مراحل پیاده‌سازی امنیت در این استاندارد عبارتند از:

- برآورد نیازهای امنیتی؛
- اتخاذ سیاست‌های امنیتی لازم؛
- ارایه طرح امنیتی؛
- پیاده سازی و تست؛
- مدیریت امنیت (annekcM.۰۱۰۲,۸۱-۰۲).

۲-۲- استاندارد ISO/IEC ۱۷۷۹۹

همزمان با بکارگیری استاندارد BS۷۷۹۹ در برخی از سازمان‌ها و جلوگیری از گسترش آن در برخی از کشورها و همچنین افزایش تقاضا برای انتشار یک استاندارد امنیت اطلاعات تحت نظر یک موسسه بین‌المللی، بخش اول استاندارد BS۷۷۹۹ به سرعت توسط موسسه بین المللی استاندارد(ISO) پیگیری و بدون هیچ‌گونه تغییری و در ۱۰ سرفصل اشاره شده تحت عنوان استاندارد ISO/IEC ۱۷۷۹۹ در دسامبر سال ۲۰۰۰ م به ثبت‌رسید(www.inducon.to/bs۷۷۹۹-۱۷۷۹۹,۲۰۱۲-۰۴-۲۰).

این استاندارد بین المللی مرهون دو دهه تحقیق و فعالیت موسسه استاندارد انگلستان در حوزه امنیت اطلاعات می باشد. این استاندارد مجدداً در سال ۲۰۰۲م بازنویسی و منتشر گردید. سپس در سال ۲۰۰۵م دوباره بازنویسی و با دو نام ISO/IEC ۱۷۷۹۹:۲۰۰۵ BSو ۷۷۹۹-۱:۲۰۰۵ BSدر یک سند انتشار یافت. این نسخه متشکل از ۳۹ هدف امنیتی و ۱۳۴ اقدام بازدارنده است. تغییر برخی از فصول گذشته و افزایش یک فصل جدید، اضافه شدن۱۷کنترل جدید و حذف برخی از کنترل های قدیمی و افزایش تعداد اقدامات کنترلی از ۱۲۷به۱۳۴عدد از جمله تغییرات اصلی این استاندارد نسبت به‌نسخه‌اولیه آن می‌باشد(www.iso.org-۲۰۱۲-۰۵-۰۱).

۲-۳- استاندارد ISO/IEC ۲۷۰۰۱

این استاندارد نسخه بازنگری شده استاندارد BS۷۷۹۹ می باشد که در سال ۱۹۹۵م توسط سازمان بین المللی استاندارد به ثبت رسیده و ایجاد مفهوم ISMSرا به دنبال داشته است. سیستم مدیریت امنیت اطلاعات، مجموعه‌ای از سیاست‌ها، سیستم‌ها و روش‌هایی است که برای دستیابی به سطح قابل قبولی از امنیت اطلاعات در سازمان‌ها طراحی و پیاده‌سازی می‌شوند. در حال حاضر استاندارد ISO/IEC ۲۷۰۰۱ که به استاندارد سیستم مدیریت امنیت اطلاعات یا ISMSمشهور است، از جمله ی استانداردهای جهانی است که بسیاری از کشورها آن را به عنوان استاندارد ملی خود انتخاب و پذیرفته‌اند. این استاندارد کامل‌ترین ساختار را برای فرایند مدیریت امنیت اطلاعات در سازمان ها فراهم نموده و مدل کاملی برای ایجاد، بهره برداری و نگهداری سیستم های مدیریت اطلاعات ارایه می‌دهد. مسولیت‌های مدیریت، بازرسی داخلی، بهبود سیستم مدیریت امنیت اطلاعات و سه پیوست از بخش های اصلی ISO/IEC ۲۷۰۰۱ می باشند. ویرایش نهایی این نسخه در سال ۲۰۰۵م صورت گرفته است. اکثر بخش های این استاندارد از استاندارد BS۷۷۹۹ موسسه استاندارد ملی کشور انگلستان[1] اقتباس شده‌است(www.۲۷۰۰۱-online.com,۲۰۱۲-۰۴-۱۶).

با توجه به فراگیر شدن استاندارد مدیریت امنیت اطلاعات و گسترش دامنه و مفاهیم استانداردهای این حوزه، ارایه این استانداردها در قالب مجموعه‌ای از استانداردها با رویکردهای مختلف در دستور کار متخصصین موسسه بین المللی استاندارد قرار گرفته و مجموعه خانواده استاندارد ISO۲۷۰۰۰ در سال ۲۰۰۵ م ارایه گردید. سپس در سال۲۰۰۷ استاندارد, ISO/IEC ۲۷۰۰۲ و پس از آن سایر زیر مجموعه‌های استاندراد ISO۲۷۰۰۰ با عناوین مختلفی همچون راهنمای بکارگیری، شاخص‌ها ، الزامات، مدیریت خطر، آینده‌پژوهی و .... در حوزه امنیت اطلاعات هم چنان ادامه دارد. از جمله مزایای بکارگیری این استاندارد مبتنی بر استانداردهای سری ISO۲۷۰۰۰ ، می توان به موارد ذیل اشاره نمود:

- استاندارد مورد تایید و اجباری از سوی شورای عالی امنیت فضای تبادل اطلاعات کشور؛
- کمک به تهیه‌ی برنامه عملیاتی امنیت فضای تبادل اطلاعات سازمان‌ها؛
- تامین امنیت در همه ی سطوح شامل امنیت فیزیکی، پرسنلی و ارتباطات؛
- ایجاد چارچوب و ساختاری برای توسعه و نگه‌داری امنیت اطلاعات؛
- کاهش تبلیغات منفی علیه سازمان و افزایش وجهه و اعتبار سازمان؛
- جدید ترین استاندارد امنیت اطلاعات با رویکرد پیشگیرانه؛
- کاهش هزینه‌ها با رویکرد کاهش احتمال خطرات و تهدیدهای امنیتی
- سیستم های مدیریت امنیت پویا و مستمر با نگاه همه جانبه به امنیت؛
- آموزش کارکنان و ارتقای سطح آگاهی و دانش عمومی

1.British Standard Institute(BSI)

آن‌ها در زمینه امنیت .

لازم به ذکر است نسخه ISO/IEC ۲۷۰۰۲ این استاندارد در حالی که دارای سه مفهوم بنیادی مدنظر در استاندارد BS۷۷۹۹ یعنی محرمانگی، پیوستگی و در دسترس بودن اطلاعات دارد، تغییرات اندکی نسبت به نسخه قبلی داشته و دارای ۱۱ حوزه کنترلی می باشد(www.۲۷۰۰۰.org, ۲۰۱۲-۰۴-۱۶)

۲-٤- گزارش های فنی ISO/IEC TR

گزارش‌های فنی[1] از جمله‌ی اسناد و مدارکی است که توسط کمیته‌ی مشترک فنی موسسه بین‌المللی استاندارد و کمیسیون بین‌المللی فنی الکترونیک[2] در حوزه‌ی سیستم‌های مدیریت امنیت اطلاعات منتشر می‌گردد. اگر چه این گزارش‌ها به تنهایی استانداردی ارایه نمی‌دهند، لیکن دستورهای راهنما و مستندات فنی معتبری را برای ایجاد و استقرار استانداردهای معرفی شده‌ی موسسه بین المللی استاندارد در بخش های مختلف ارایه می‌دهند. راهنمای فنی، مدیریتی، کاربران و ارزیابان از جمله این گزارش‌ها می‌باشند.

اولین گزارش فنی با عنوان ISO/IEC TR۱۳۳۳۵ توسط موسسه بین المللی استاندارد و در قالب ۵ بخش در فواصل سال‌های ۱۹۹۶م تا ۲۰۰۱ م منتشر شده است(www.wikipedia.org,۲۰۱۲-۰۳-۲۰). اگر چه این گزارش فنی به عنوان استاندارد ISO منتشر نشد و عنوان آن گزارش فنی می‌باشد، لیکن تنها مستندات فنی معتبری است که جزییات و تکنیک های مورد نیاز مراحل ایمن‌سازی اطلاعات و ارتباطات را تشریح نموده و در واقع مکمل استانداردهای مدیریتی BS۷۷۹۹ و IEC/ ISO ۱۷۷۹۹ می باشد و در پیاده سازی سیستم مدیریت امنیت اطلاعات، کاربرد دارد(Farn,lin,fung.۲۰۰۹,۵۰۰-۵۰۶).

هشتمین گزارش موجود در سری استانداردهای TR۲۷۰۰۰ ISO/IEC با عنوان ISO/IEC TR۲۷۰۰۸:۲۰۱۱ در واقع دستورالعمل میزان کنترل امنیت اطلاعات می باشد که در سال ۲۰۱۱ ارایه شده است(Princely in edo.۲۰۱۲,۸۶).

۲-۵- سایر استانداردها

از جمله استانداردهای دیگر در فضای سایبر می‌توان به اسناد ۱۲-۸۰۰-۱۴۸، ۸۰۰-۲۶ و ۸۰۰-۲۶که توسط موسسه ملی استاندارد و تکنولوژی[3] منتشر شده است اشاره نمود. سند راهنمای امنیت اطلاعات، اصول پذیرفته شده برای امنیت فن‌آوری اطلاعات و راهنمای خود ارزیابی امنیتی سیستم های فناوری اطلاعات عناوین اسناد فوق می باشند. از آخرین استانداردهای منتشر شده خانواده ISO۲۷۰۰۰ می‌توان به استاندارد ۲۷۰۳۵:۲۰۱۱ ISO/IECاشاره نمود که با اجرای رویکرد مدیریت حوادث اطلاعات ارایه شده است. با اجرای این استاندارد می‌توان اقدامات تهدیدکننده امنیت اطلاعات همچون نفوذ هکرها و... را کاهش داد. این استاندارد دستورالعمل لازم به منظور چگونگی شناسایی، گزارش‌دهی و ارزیابی میزان آسیب‌پذیری و حوادث امنیت اطلاعات را ارایه می‌نماید. استاندارد۲۷۰۳۵:۲۰۱۱ /IEC ISO،که جایگزین گزارش فنی۱۸۰۴۴:۲۰۰۴ ISO/IEC TR شده‌است، متضمن مفاهیم کلی مندرج در استاندارد ۲۷۰۰۱:۲۰۰۵ /IEC ISOمی‌باشد(Saleh-Aflantookh.۲۰۱۱,۱۰۷-۱۱۸).

۳- استانداردها و امنیت اطلاعات در ایران

لزوم توجه جدی به موضوع امنیت و حفاظت از اطلاعات در حوزه فناوری اطلاعات از سال ۱۳۸۰ و در قالب "سیاست‌های کلی شبکه‌های اطلاع رسانی رایانه‌ای" مورد تاکید مقام معظم رهبری قرار گرفته است. در بند ۷ این سیاست ها که در مورخه ۸۰/۰۳/۰۹ابلاغ گردیده به موضوع " توسعه فناوری اطلاعات به ویژه حفاظت از اطلاعات و آینده نگری در خصوص تحولات فناوری اطلاعات در سطح ملی و جهانی" اشاره گردیده است(جهانگرد، سلجوقی. ۱۹:۱۳۸۳). با توجه به اهمیت موضوع و همچنین آسیب‌پذیری ها و تهدیدات متصور این بخش در نیروهای مسلح، "آیین نامه ی جامع امنیت فاوای نیروهای مسلح" در تیرماه ۱۳۸۷ از طریق ستاد کل ن.م ابلاغ گردیده است. در آیین نامه‌ی مذکور که مشتمل بر ۲۹۳ ماده و ۷۳ تبصره می باشد، به تعیین وظایف و مسوولیت های سازمان های ن.م در دو بخش دستورهای کلی و خاص در زمینه نرم افزار، سخت افزار، شبکه اطلاعات الکترونیکی، بسترهای ارتباطی و نیروی انسانی پرداخته است. پیش از آن و برابر بخشنامه ابلاغی معاون اول رییس جمهور در تاریخ ۱۳۸۶/۰۸/۱۰ کلیه دستگاه های دولتی و غیردولتی موظف به تهیه ی طرح سیستم مدیریت امنیت اطلاعات(ISMS) شده و هم چنین با توجه به اهمیت این سیستم مدیریتی در کشور طبق مصوبه هیات وزیران کلیه ی دستگاه‌های اجرایی مشمول ماده پنج قانون خدمات کشوری، ملزم به پیاده‌سازی سامانه‌ی مدیریت امنیت اطلاعات گردیدند. در حوزه ی قانونگذاری نیز قانون جرایم رایانه ای در خرداد ماه ۱۳۸۸ در دو بخش جرایم، مجازات ها و آیین دادرسی مشتمل بر ۵۶ ماده و ۲۵ تبصره به تصویب مجلس شورای اسلامی و تایید شورای نگهبان رسیده است. همچنین

1.Technical Report
2.International Electro technical Commission(IEC)
3.National Institute of Standard and Technology (NIST)

در ماده ی ۴۶ قانون برنامه‌ی پنجم توسعه و در فصل چهارم مبحث فناوری اطلاعات در نظام اداری و مدیریت به موضوع "موظف شدن دستگاه های اجرایی به توسعه و تکمیل پایگاه های اطلاعاتی و اتصال به شبکه ی ملی اطلاعات با رعایت مقررات امنیتی و بکارگیری استانداردهای لازم در راستای نگهداری و به روز رسانی آن‌ها" تاکید شده است. پس از آن و در تاریخ ۱۳۸۹/۱۱/۲۹ سیاست های کلی نظام در امور امنیت فضای تولید و تبادل اطلاعات و ارتباطات(افتا) توسط مقام معظم رهبری ابلاغ و در بند ۶ سیاست های ابلاغی به موضوع" تدوین استانداردهای لازم برای حفظ و توسعه ی امنیت فضای تولید و تبادل اطلاعات و ارتباطات و تهیه پیش نویس قوانین مورد نیاز" تاکید شده است و در نهایت در تاریخ۱۳۹۰/۱۲/۱۷ با دستور مقام معظم رهبری شورای عالی فضای مجازی با هدف راه اندازی مرکز ملی فضای مجازی کشور تشکیل و اعضای حقیقی و حقوقی آن به مدت سه سال از سوی معظم له منصوب گردیده اند.

٤- جمع بندی

با توجه به تحولات گسترده‌ی صورت گرفته در حوزه فناوری اطلاعات و ارتباطات طی دو دهه گذشته، موضوع امنیت اطلاعات به صورت عام و استانداردها در این حوزه به صورت خاص مورد توجه کشورهای پیشرو و پیشگام در این بخش قرار گرفته است. جایگاه ویژه‌ی این موضوع را می‌توان در ایجاد و شکل‌گیری خانواده ISO۲۷۰۰۰و هم‌چنین پیگیری مستمر سازمان‌ها و نهادهای دولتی و خصوصی برای استقرار الزامات استانداردهای پیش گفته و اخذ گواهی‌نامه‌های مربوط درک نمود. هرچند برقراری امنیت در یک سازمان می بایست در همه ابعاد آن صورت پذیرد، لیکن شناخت و پیاده سازی استانداردهای تدوین شده در این بخش، گامی موثر در راستای استقرار امنیت اطلاعات محسوب می‌گردد.

با وجود اینکه برخی معتقدند که استاندارد امنیتی تنها اعمال آیین‌نامه‌های امنیتی نیست و ضوابط امنیتی برای سازمان‌ها مجموعه ای از ابزارها و روش هایی را جهت بررسی و نقد، ارزیابی، اجرا، تقویت و گسترش سیاست ها و تدابیر فراهم می‌کند(۱۸-Blandford.۲۰۱۱,۱۵)، دیگر صاحب نظران حوزه امنیت اطلاعات، ضوابط و استانداردها را تضمین کننده ی نهایی امنیت در حوزه اطلاعات ندانسته و معتقدند کاربرانی که نسبت به امنیت رایانه اطلاعات کافی ندارند، خود از بزرگ ترین خطرات امنیت اطلاعات به شمار می روند(George sadowsky ۲۰۰۳:۴۵).

۵- نتیجه‌گیری

هرچند سابقه‌ی تشکیل سازمان استاندارد در کشور به سال ۱۳۰۴ و هم زمان با تصویب قانون اوزان و مقیاس ها برمی گردد و فعالیت‌های گسترده‌ای نیز در راستای عضویت و گسترش همکاری‌های مشترک با دفاتر، مجامع، اتحادیه و موسسه‌های استاندارد در سطح بین‌المللی در حوزه های فعالیت‌های تولیدی و خدماتی صورت گرفته است، به نظر می رسد اقدامات قابل ملاحظه‌ای در خصوص تدوین و انتشار استانداردها در حوزه فناوری اطلاعات با همکاری نهادهای مرتبط از جمله وزارت ارتباطات و فن‌آوری اطلاعات انجام نشده و سازمان ها، موسسات و شرکت های موفق به دریافت گواهینامه های استاندارد خانواده ISO۲۷۰۰۰ تا سال ۲۰۱۲م کمتر از ۱۰ مجموعه می باشند. اگرچه مواردی از جمله اهمیت کیفیت از نگاه مشتری، ارزان بودن و امکان اخذ مشاوره و ممیزی در حوزه استانداردهای سری ISO۹۰۰۰در حوزه کیفیت از جمله دلایل اصلی توسعه و گسترش این استاندارد در کشور ارزیابی می‌گردد و نقطه مقابل این محاسن- خصوصاً هزینه بالای تامین امنیت و عدم امکان اخذ مشاوره در این بخش که نقض امنیت را به دنبال دارد- در استقرار استانداردهای سری ISO۲۷۰۰۰ به عنوان موانع و حتی معایب کار تلقی می‌گردد، تدوین و ارایه استاندارد در حوزه ی امنیت اطلاعات در سطح ملی و به صورت تخصصی و ویژه در حوزه ی حساس و حاکمیتی دفاع ضروری ارزیابی می‌گردد.

منابع :

۱- جهانگرد، نصراله و سلجوقی،خسرو - « مجموعه قوانین و مقررات فناوری اطلاعات و ارتباطات ایران» - دبیرخانه شورای عالی اطلاع‌رسانی- ۱۳۸۳.

۲- دشتی، افسانه - " استانداردهای امنیت" - ماهنامه شبکه - شماره ۵۴-۱۳۸۴.

۳- قانون برنامه چهارم توسعه اقتصادی، اجتماعی و فرهنگی جمهوری اسلامی ایران؛ روزنامه رسمی کشور ج.ا.ا؛ ۱۳۸۳.

۴- قانون برنامه پنجم توسعه اقتصادی، اجتماعی و فرهنگی جمهوری اسلامی ایران؛ روزنامه رسمی کشور ج.ا.ا؛ ۱۳۸۹.

۵- معتمدی فر، مرتضی - «روش پیاده سازی استاندارد امنیت اطلاعات (ISO۲۷۰۰۱) در ادارات و سازمان ها (ISMS)» - مرکز آموزش و تحقیقات صنعتی ایران - ۱۳۹۰.

۶- آیین نامه جامع امنیت فاوای نیروهای مسلح، ۱۳۸۷.

۷- سیاست های کلی نظام در امور امنیت فضای تولید و تبادل اطلاعات و ارتباطات(افتا)، ۱۳۸۹.

8-Brian-Mckenna.2010."infoSecurity".March/Aprill-www.sciencedirect.com,2012.01.14.

9- Mikko Siponen, Robert Willison.2009.Information Security Management Standard: Problems and Solutions. Information & Management.www.elsevier.com/locate/im.

10Richard Blandford.2011. Information Security in the Cloud. Network Security. April,www.infosecurity-magazine.com/view/6157/gsm-2012-01-10.

11- Princely Ifinedo.2012.Understanding Information Systems Security Policy Compliance: An Integration of the theory of planned behavior And the Protection Motivation theoty. Shannon School of Business, Cape Breton University.

12- Mohamed S.Sale. Abdulkader Alfantookh.2011.A new comprehensive framework for enterprise information security risk management. Bradford University press.www.ksu.edu.sa.

13- Kwo-Jean Farn, Shu-Kuo Lin, Andrew Ren-Wei Fung.2009. A study on information security management system evaluation—assets, threat and vulnerability. Computer Standards & Interfaces 26 (2009) 501–513 www.elsevier.com/locate/csi.

14- J.Stuart Broderick.2006. ISMS, security standards and security regulations. Information Security Technical Report Strategic Consulting, Symantec Corporation United States. www.compseconline.com/publications/prodinf.htm.

15-, George sadowsky, jaes Dempsey, Alan Greenberg, Barbara j.mack, alansc hwartz . IT Security handbook. 2003. infodev,world bank

16- www.iso.org

17- www.27001-online.com

18- www.27000.org

19- www. khamenei.ir