ISIRI -ISO/IE

24759

1st. Edition

Identical with

ISO/IEC24759:2008

جمهوری اسلامی ایران

Islamic Republic of Iran

سازمان استاندارد و تحقیقات صنعتی ایران

Institute of Standards and Industrial Research of Iran

استاندارد ایران- ایزو/آی ای سی ۲۴۷۵۹

چاپ اول

فناوری اطلاعات- فنون امنیتی-

الزامات آزمون برای ماژول های پنهانی

Information technology — Security techniques — Test requirements for cryptographic modules

ICS: 35.040

به نام خدا

آشنایی با موسسه استاندارد وتحقیقات صنعتی ایران

موسسه استانداردوتحقیقات صنعتی ایران به موجب بندیک ماده ۳ قانون اصلاح قوانین ومقررات موسسه استاندارو تحقیقات صنعتی ایران،مصوب بهمن ماه ۱۳۷۱تنها مرجع رسمی کشور است که وظیفه تعین، تدوین ونشراستاندارد های ملی(رسمی) ایران را برعهده دارد .

تدوین استاندارد در حوزه های مختلف کمیسیون فنی مرکب ازکارشناسان موسسه* صاحب نظران مراکز وموسسات علمی، پژوهشی ، تولیدی واقتصادی آگاه ومرتبط انجام می شود وکوششی همگام بامصالح ملی و باتوجه به شرایط تولیدی، فناوری وتجاری است که از مشارکت اگاهانه ومنصفانه صاحبان حق ونفع ، شامل تولید کنندگان ، مصرف کنندگان ، صادرکنندگان ووارد‌کنندگان، مراکزعلمی وتخصصی، نهادها ، سازمان های دولتی وغیردولتی حاصل می شود.پیش نویس استاندارد های ملی برای نظر خواهی به مراجع ذی نفع و اعضاءکمسیون های فنی مربوطه ارسال می شود. وپس از دریافت نظرهاوپیشنهادها درکمیته ملی مرتبط با آن رشته طرح درصورت تصویب به عنوان استاندارد ملی(رسمی) ایران چاپ ومنتشر می شود .

پیش نویس استانداردهایی که موسسات وسازمانهای علاقه مند ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند در کمیته ملی طرح و بررسی ودر صورت تصویب، به عنوان استاندارد ملی (رسمی)چاپ ومنتشر می شود .بدین ترتیب، استانداردهایی ملی تلقی می شود که براساس مفاد نوشته شده در استاندارد ملی ایران شماره ۵ تدوین ودرکمیته ملی استاندارد مربوطه که موسسه استاندارد تشکیل می دهد به تصویب رسیده باشد .

موسسه استاندارد وتحقیقات صنعتی ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] کمیسیون بین المللی الکتروتکنیک(IEC)[2] وسازمان بین المللی اندازه شناسی قانونی(OIML)[3] است وبه عنوان تنهارابط[4] کمیسیون کدکس غذایی(CAC)[5] درکشورفعالیت می کند . درندوین استاندارد های ملی ایران ضمن توجه به شرایط کلی ونیاز مندی های خاص کشور ، از آخرین پیشرفت های علمی ، فنی وصنعتی جهان و استاندارد های بین المللی بهره گیری می شود.

موسسه استانداردوتحقیقات صنعتی ایران می تواندبارعایت موازین پیش بینی شده درقانون برای حمایت ازمصرف کنندگان،حفظ سلامت وایمنی فردی وعمومی،حصول اطمینان ازکیفیت محصولات وملاحظات زیست محیطی واقتصادی اجرای بعضی ازاستاندارد های ملی ایران را برای محصولات تولیدی داخل کشورو / یا اقلام وارداتی باتصویب شورای عالی استاندارد، اجباری نماید. موسسه می تواند به منظورحفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی ودرجه بندی آن را اجباری نماید.و همچنین برای اطمینان بخشیدن به استفاده کنندگان ازخدمات سازمان هاو موسسات فعال، در زمینه آموزش، مشاوره ، بازرسی، ممیزی وصدور گواهی سیستم های کیفیت ومدیریت زیست محیطی ، آزمایشگاه ها ومراکزکالیبراسیون(واسنجی) وسایل سنجش، موسسه استاندارد این گونه سازمان ها موسسات رابراساس ضوابط نظام تاییدصلاحیت ایران ارزیابی می کند ودرصورت احرازشرایط لازم،گواهی تایید صلاحیت با آنها اعطاء و برعملکرد آنها نظارت می کند. ترویج دستگاه بین المللی یکا های کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها وانجام تحقیقات کاربردی برای ارتقاع سطح استاندارد های ملی ایران از دیگر وظایف این موسسه است .

---

* موسسه استاندارد وتحقیقات صنعتی ایران

1- International Organization for standardization
2 -International Electrotechnical commission
3 - International Organization for Legal Metrology (Organization International de Metrology Legal)
4 – Contact point
5 – Codex Alimentarius commission

کمیسیون فنی تدوین استاندارد

" فناوری اطلاعات – فنون امنیتی – الزامات آزمون برای ماژول های پنهانی"

رئیس:	**سمت و/یا نمایندگی**
محمودزاده، مرتضی	شرکت سهامی عام کف
(دکترای مدیریت سیستم)	
دبیران:	
اعتمادی، محمود	بنیاد آموزش های فنی و حرفه ای ایرانیان
(فوق لیسانس مدیریت صنعتی)	
نوتاش، فاطمه	دانشگاه علمی کاربردی داروگر
(لیسانس مهندسی کامپیوتر)	
اعضاء (به ترتیب حروف الفباء) :	
اعتمادی، فرناز	وزارت آموزش و پرورش
(فوق لیسانس ریاضیات)	
جعفری، اکرم	وزارت تعاون
(لیسانس مهندسی کامپیوتر)	
خاوری، سیامک	وزارت ارتباطات و فناوری اطلاعات- سازمان تنظیم
(لیسانس مهندسی برق و الکترونیک)	مقررات و ارتباط رادیوئی
شاه محمودی، بهزاد	موسسه استاندارد و تحقیقات صنعتی ایران
(لیسانس فیزیک)	
صدیق زاده، وریا	شرکت توسعه شبکه خاورمیانه(MIDNET)

(لیسانس مهندسی برق و الکترونیک)

غیاثیان، علی — دانشگاه جامع علمی کاربردی
(فوق لیسانس ارتباطات)

فرحزادی، سیدهادی — شرکت مهاد صنعت
(لیسانس مهندسی برق و الکترونیک)

نوتاش، جواد — شرکت جهاد توسعه منابع آب
(لیسانس مهندسی مکانیک)

پیش گفتار

استاندارد " فناوری اطلاعات- فنون امنیتی- الزامات آزمون برای ماژول های پنهانی" که پیش نویس آن در کمیسیون فنی مربوط، توسط بنیاد آموزش های فنی و حرفه ای ایرانیان، بر مبنای روش تنفیذ مورد اشاره در راهنمای ISO/IEC Guide 21-1 (پذیرش منطقه ای یا ملی استانداردهای" بین المللی/ منطقه ای" و دیگر مدارک استاندارد) به عنوان استاندارد ملی ایران، تهیه و در یکصد و دهمین اجلاسیه کمیته ملی استاندارد رایانه و فراوری داده ها مورخ ۱۳۸۹/۹/۸ مورد تصویب قرار گرفته است، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین ومقررات سازمان استاندارد وتحقیقات صنعتی ایران مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می گردد.

برای حفظ همگامی وهماهنگی با تحولات و پیشرفت های ملی وجهانی در زمینه صنایع، علوم و خدمات، استاندارد های ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح یا تکمیل این استاندارد ها ارائه شود، در هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین همواره از آخرین تجدید نظر آن ها استفاده خواهد شد.

این استاندارد ملی براساس پذیرش استاندارد بین المللی به شرح زیراست:

ISO/IEC 24759: 2008 , Information technology — Security techniques — Test requirements for cryptographic modules

فناوری اطلاعات- فنون امنیتی- الزامات آزمون برای ماژول های پنهانی

۱ هدف و دامنه کاربرد

این استاندارد ملی، براساس پذیرش استاندارد بین المللی ISO/IEC 24759:2008 تدوین شده است.

هدف از تدوین این استاندارد، تعیین روش های مورد استفاده در آزمایشگاه های آزمون به منظور مطابقت دادن ماژول های پنهانی با الزامات مشخص شده در استاندارد ISO/IEC 19790: 2006 می باشد. این روش ها برای فراهم کردن درجه بالای واقعی بودن در طول فرایند های آزمون و به منظور اطمینان از آزمایشگاه های آزمون، تدوین شده اند.

این استاندارد هم چنین الزامات اطلاعاتی که فروشندگان برای آزمایشگاه های آزمون به عنوان گواهی پشتیبان فراهم می نمایند، را معین می کند. این الزامات مطابقت ماژول های پنهانی با الزامات مشخص شده در استاندارد ISO/IEC 19790 را مشخص می کند.

فروشندگان می توانند این استاندارد را به عنوان راهنما در بررسی صحت تطبیق ماژول های پنهانی با الزامات مشخص شده در استاندارد ISO/IEC 19790: 2006 ، قبل از آنکه برای آزمون به آزمایشگاه های آزمون اعمال شوند، به کار ببرند.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آن ها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد ملی ایران محسوب میشود.
در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه ها و تجدید نظرهای بعدی آن مورد نظر این استاندارد ملی نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن ها ارجاع داده شده است، همواره آخرین تجدید نظر و اصلاحیه های بعدی آن ها مورد نظر است.
استفاده از مراجع زیر برای کاربرد این استاندارد الزامی است :

2-1 ISO/IEC 15408 (all parts), Information technology — Security techniques — Evaluation criteria for IT security

2-2 ISO/IEC 18031:2005, Information technology — Security techniques — Random bit generation

2-3 ISO/IEC 19790:2006, Information technology — Security techniques — Security requirements for cryptographic modules

کلیه بندهای استاندارد بین المللی ISO/IEC 24759:2008 در مورد این استاندارد معتبر و الزامی است.