



حریم خصوصی و امنیت

اینترنت

مطابق با سرفصل وزارت علوم، تحقیقات و فناوری

مؤلف:

مهندس محمد علی ترکمانی

سرشناسه: ترکمانی، محمدعلی، ۱۳۵۴ -

عنوان و نام پدیدآور: حریم خصوصی و امنیت اینترنت/مؤلف محمدعلی ترکمانی.

مشخصات نشر: مشهد: ارسطو، ۱۳۹۵

مشخصات ظاهری: ۲۰۶ ص.؛ مصور.

شابک: ۹۷۸-۶۰۰-۷۹۴۰-۹۲-۱

وضعیت فهرست نویسی: فیا

موضوع: اینترنت -- تدابیر ایمنی

موضوع: شبکه‌های کامپیوتری -- تدابیر ایمنی

موضوع: کار، رفتارها -- ایمنی اطلاعات

موضوع: پایگاه‌های اطلاعاتی -- امنیت

رده بندی کنگره: ۴۴۰/۵۹/۵۱۰۵ TK

رده بندی دیویی: ۰۰۵/۱

شماره کتابشناسی ملی: ۴۱۱۱۱۱۱۱

نام کتاب: حریم خصوصی و امنیت اینترنت

مؤلف: محمد علی ترکمانی

ناشر: ارسطو (با همکاری سامانه اطلاع رسانی چاپ و نشر ایران)

صفحه آرایشی، تنظیم و طرح جلد: محمدعلی ترکمانی و علی بیات

تیراژ: ۱۰۰۰ جلد

نوبت چاپ: اول- ۱۳۹۵

چاپ: مدیران

قیمت: ۲۱۰۰۰ تومان

شابک: ۹۷۸-۶۰۰-۷۹۴۰-۹۲-۱

تلفن های مرکز پخش: ۳۵۰۹۶۱۴۵ - ۳۵۰۹۶۱۴۶ - ۰۵۱ - ۰۹۱۷۷۱۶۴۹۴۰

وب سایت: www.chaponashr.ir/Torkamani

این اثر مشمول قانون حمایت از مؤلفان و مصنفان و هنرمندان است. هر کس تمام یا قسمتی از

این اثر را بدون اجازه مؤلف نشر یا پخش یا عرضه کند، مورد پیگرد قانونی قرار خواهد گرفت.

فهرست مطالب

فصل اول: مفاهیم و اصول امنیت اطلاعات ۱۷

- ۱-۱- امنیت اطلاعات چیست؟ ۱۷
- ۱-۱-۱- خصوصیات سیستم امن ۱۷
- ۱-۲-۱- اطلاعات امنیتی ۱۸
- ۱-۲-۱- آسیب پذیری ۱۸
- ۱-۲-۱- حمل ۱۸
- ۱-۲-۱- تهدید ۱۸
- ۱-۲-۱- مفهوم AAA در امنیت اطلاعات ۱۸
- ۱-۲-۱- عدم انکار (سندیت) ۲۰
- ۱-۳- نفوذگر یا هکر ۲۰
- ۱-۴- دسته بندی کلی حملات ۲۰
- ۱-۴-۱- دسته بندی از نظر تغییر دادن اطلاعات ۲۰
- ۱-۴-۲- دسته بندی از نظر به چالش کشیدن اصول امنیت ۲۱
- ۱-۵- هک HACKER از چه راهی وارد سیستم می شود؟ ۲۲
- ۱-۶- سنوالات تشریحی ۲۲
- ۱-۷- سنوالات چهارگزینه ای ۲۳
- پاسخنامه: ۲۴

فصل دوم: انواع حملات در شبکه های کامپیوتری ۲۵

- ۲-۱- حمله تکرار یا استراق سمع یا شنود اطلاعات ۲۵
- ۲-۲- در پستی ۲۵
- ۲-۳- مصرف پهنای باند (حملات DOS) ۲۶

- ۲۶ ۲-۴ حمله مرد میانی
- ۲۷ ۲-۵ ویروس‌ها و کرم‌ها
- ۲۷ ۲-۶ اسب تروا
- ۲۷ ۲-۷ جاسوس افزار
- ۲۸ ۲-۸ وب سایت های تقلبی (فیشینگ)
- ۲۸ ۲-۹ حمله با استفاده از نرم افزار های ثبت کننده کلید
- ۲۸ ۲-۱۰ حملات جهت یافتن کلمات عبور
- ۲۹ ۲-۱۱ هرزنامه
- ۳۰ ۲-۱۲ رمز قمار (SPIT) یا VOIP SPAM
- ۳۰ ۲-۱۳ SPOOFING
- ۳۱ ۲-۱۳-۱ IP Spoofing یا IP Forger
- ۳۱ ۲-۱۳-۲ AP Spoofing
- ۳۲ ۲-۱۳-۳ Email spoofing
- ۳۲ ۲-۱۴ BOTNET
- ۳۴ ۲-۱۵ سنوالات تشریحی
- ۳۴ ۲-۱۶ سنوالات چهارگزینه‌ای
- ۳۶ پاسخنامه:

۳۷ فصل سوم: انتخاب و مدیریت کلمه عبور

- ۳۷ ۳-۱ مقدمه
- ۳۷ ۳-۲ برخی قوانین ساده و اولیه
- ۳۸ ۳-۳ هک کردن کلمات عبور شما
- ۳۹ ۳-۴ یک کلمه عبور خوب از چند کاراکتر تشکیل شده است؟
- ۴۰ ۳-۵ یک کلمه عبور خوب باید از چه کاراکترهایی تشکیل شده باشد؟
- ۴۱ ۳-۶ کلمات عبوری که به ندرت استفاده می شوند
- ۴۲ ۳-۷ مثالهایی از کلمات عبور خوب

- ۴۲..... ۱-۷-۳ مثالهایی از کلمات عبور چند کلمه ای
- ۴۲..... ۲-۷-۳ مثالهایی از کلمات عبور با استفاده از یک عبارت
- ۴۲..... ۸-۳ نرم افزارهای مدیریت رمز عبور
- ۴۲..... Efficient Password Manager Pro- ۱-۸-۳
- ۴۳..... Sticky Password Premium- ۲-۸-۳
- ۴۳..... LastPass Password Manager- ۱-۸-۳
- ۴۴..... Agilebits 1Password- ۴-۸-۳
- ۴۴..... Password- ۵-۸-۳
- ۴۴..... ۶-۸-۳ برخی دیگر از نرم افزارهای مدیریت رمز عبور
- ۴۴..... ۹-۳ صفحه کلید مجاز
- ۴۵..... ۹-۳ سنوالات تشریحی
- ۴۵..... ۱۰-۳ سنوالات چهارگزینه ای
- ۴۶..... پاسخنامه:

۴۷..... فصل چهارم: امنیت در خرید اینترنتی

- ۴۷..... ۱-۴ مقدمه
- ۴۷..... ۲-۴ نکات خرید آنلاین
- ۵۲..... ۳-۴ بررسی فروشگاه
- ۵۳..... ۴-۴ راه های مقابله با سرقت حساب
- ۵۵..... ۵-۴ مرورگر خود را تنظیم کنید
- ۵۸..... ۶-۴ توصیه هایی برای امنیت و جلوگیری از سرقت هویت
- ۶۱..... ۷-۴ سنوالات تشریحی
- ۶۲..... ۸-۴ سنوالات چهارگزینه ای
- ۶۲..... پاسخنامه

۶۳..... فصل پنجم: تورنت

- ۶۳ ۱-۵ تورنت (TORRENT) چیست؟
- ۶۳ ۲-۵ فایل‌های تورنت و پروتکل BITTORRENT
- ۶۴ ۳-۵ آیا دانلود از تورنت قانونی است؟
- ۶۴ ۴-۵ آیا دانلود از تورنت امن است؟
- ۶۵ ۵-۵ چگونه می‌توان از تورنت دانلود کرد؟
- ۶۵ ۶-۵ اصطلاحات BITTORRENT
- ۶۹ ۷-۵ BITTORRENT چگونه کار می‌کند؟
- ۷۰ ۸-۵ نرم افزارهای دانلود از تورنت
- ۷۰ ۱-۱۰ aTorrent PRO – Torrent App
- ۷۱ ۹-۵ سوالات تشریحی
- ۷۲ ۱۰-۵ سنوالات چهارگزینه‌ای
- ۷۲ پاسخنامه

۷۳ فصل ششم: ایمیل‌های شخصی و گمنامی ایمیل

- ۷۳ ۱-۶ ریمیلر چیست؟
- ۷۴ ۲-۶ انواع ریمیلرها
- ۷۵ ۳-۶ دسته‌بندی دیگر ریمیلرها
- ۷۶ ۴-۶ WEB BASED MAILER
- ۷۶ ۵-۶ چرا ریمیلرها توسط دولت‌ها بلاک میشوند؟
- ۷۶ ۶-۶ نرم افزارهای ریمیلر
- ۷۷ ۷-۶ سنوالات تشریحی
- ۷۷ ۸-۶ سنوالات چهارگزینه‌ای
- ۷۸ پاسخنامه

۷۹ فصل هفتم: امنیت فیزیکی و محیط

- ۷۹ ۱-۷ مقدمه
- ۷۹ ۲-۷ جلوگیری از دسترسی فیزیکی غیرمجاز، خسارت و توقف فعالیت‌های سازمان

۷۹	۱-۲-۷ ایجاد محیط امن فیزیکی برای اطلاعات و سیستم‌های اطلاعاتی
۸۰	۲-۲-۷ کنترل تردد فیزیکی (ورود و خروج)
۸۰	۳-۲-۷ امن‌سازی دفاتر اتاق‌ها و تاسیسات
۸۱	۴-۲-۷ محافظت در مقابل تهدیدات محیطی و خارج
۸۱	۵-۲-۷ کار در محیط امن
۸۱	۶-۲-۷ جداسازی فضاهای دسترسی عمومی تخلیه، بارگیری و ارسال و دریافت
۸۲	۷-۳ پیشگیری از صدمه خسارت دزدی یا لو رفتن دارایی‌های سازمان و توقف در فعالیت‌های سازمان
۸۲	۱-۳-۷ تجهیزات
۸۲	۱-۳-۷ ۱-۱-۳-۷
۸۲	۲-۳-۷ ۱-۲-۳-۷ ابزارهای قابل حمل (Portable)
۸۳	۲-۳-۷ ۲-۳-۷ امکانات پشتیبانی (منبع تغذیه)
۸۴	۳-۳-۷ ۳-۳-۷ امنیت کابل‌کشی
۸۵	۴-۳-۷ ۴-۳-۷ نگهداری از تجهیزات
۸۵	۵-۳-۷ ۵-۳-۷ امنیت تجهیزات خارج از محل‌های اصلی
۸۶	۶-۳-۷ ۶-۳-۷ اسقاط یا استفاده مجدد از تجهیزات
۸۶	۶-۳-۷ ۶-۳-۷ مخطومی اسقاط یا استفاده مجدد از تجهیزات
۸۷	۷-۳-۷ ۷-۳-۷ راه‌های خروج تجهیزات از سازمان
۸۷	۴-۷ ۴-۷ سنوالات تشریحی
۸۷	۵-۷ ۵-۷ سنوالات چهارگزینه‌ای
۸۸	پاسخنامه

فصل هشتم: امنیت در شبکه بی سیم ۸۹

۸۹	۱-۸ امنیت بی سیم
۹۰	۱-۱-۸ تهدیدهای شبکه بی سیم

- ۸-۱-۲- اقدامات امنیتی بی سیم ۹۲
- ۸-۲- امنیت دستگاه سیار ۹۴
- ۸-۳- سنوالات چهار گزینه ای ۱۰۱
- ۸-۴- سنوالات چهار گزینه ای ۱۰۱
- پاسخنامه: ۱۰۲

فصل نهم: حریم خصوصی ۱۰۳

- ۹-۱- حفاظت از حریم و قانون ۱۰۳
- ۹-۲- حریم، حریم در اساسنامه ایالات محته ۱۰۴
- ۹-۳- حریم اطلاعاتی ۱۰۴
- ۹-۴- قوانین حریم، داده ها و احکام دادگاه ۱۰۴
- ۹-۴-۱- داده های ۱۰۵
- ۹-۴-۱-۱- قانون حریم (اعتبار منصفانه (سال ۱۹۷۰) ۱۰۵
- ۹-۴-۱-۲- قانون Gramm-Leach-Bliley (GLBA) ۱۰۵
- ۹-۴-۲- اطلاعات سلامت ۱۰۷
- ۹-۴-۲-۱- قانون پاسخگویی و قابلیت افعال بیمه سلامت سال ۱۹۹۶ (HIPAA) ۱۰۷
- ۹-۴-۳- داده های شخصی کودکان ۱۰۸
- ۹-۴-۳-۱- قانون حفاظت حریم آنلاین کودکان (سال ۱۹۹۰) ۱۰۸
- ۹-۴-۴- نظارت الکترونیکی ۱۰۸
- ۹-۴-۴-۱- قانون ارتباطات سال ۱۹۳۴ ۱۰۹
- ۹-۴-۴-۲- قانون نظارت اطلاعات خارجی (سال ۱۹۷۸) ۱۰۹
- ۹-۴-۴-۳- قانون اصلاحیات اطلاعات خارجی (سال ۲۰۰۸) ۱۰۹
- ۹-۴-۴-۴- قانون USA PATRIOT (سال ۲۰۰۱) ۱۱۰
- ۹-۴-۵- صدور داده های شخصی ۱۱۰
- ۹-۵-۴-۱- سازمان همکاری اقتصادی و توسعه عملیات اطلاعات منصفانه (۱۹۸۰) ۱۱۰
- ۹-۵-۴-۲- دستور العمل حفاظت داده های اتحادیه اروپا (سال ۱۹۹۸) ۱۱۱
- ۹-۵-۴-۳- TRUSTe و BBBONLINE ۱۱۲

- ۱۱۳ ۶-۴-۹- دسترسی به رکوردهای دولت
- ۱۱۳ ۶-۴-۹- ۱- قانون آزادی اطلاعات (FOIA) سال ۱۹۶۶ در سال ۱۹۷۴ اصلاح شد
- ۱۱۳ ۶-۴-۹- ۲- قانون حریم سال ۱۹۷۴
- ۱۱۴ ۵-۹- مسائل کلیدی حریم و ناشناسی
- ۱۱۴ ۵-۹- ۱- سرقت هویت
- ۱۱۴ ۵-۹- ۱- ۱- رخنه به داده ها
- ۱۱۴ ۵-۹- ۲- ۱- نگهداری داده های شخصی
- ۱۱۵ ۵-۹- ۳- فیشینگ
- ۱۱۶ ۵-۹- ۴- ۱- نرم افزار جاسوسی (Sprow)
- ۱۱۶ ۵-۹- ۲- حریم مصرف کننده در تجارت الکترونیک
- ۱۱۶ ۵-۹- ۱- ۲- جمع آوری اطلاعات مصرف کننده
- ۱۱۶ ۵-۹- ۲- ۲- حریم داده های مصرف کننده
- ۱۱۷ ۵-۹- ۳- ۲- رفتار مسئولانه با داده های مصرف کننده
- ۱۱۷ ۵-۹- ۴- ۲- نظارت بر محل کار
- ۱۱۸ ۶-۹- سنوالات
- ۱۱۹ پاسخنامه

۱۲۱ فصل دهم: VPN

- ۱۲۱ ۱-۱- مقدمه
- ۱۲۲ ۱-۲- VPN چیست؟
- ۱۲۲ ۱-۳- چرا VPN؟
- ۱۲۲ ۱-۴- چه وقت از VPN استفاده می شود؟
- ۱۲۳ ۱-۵- تونلینگ (TUNNELING)
- ۱۲۳ ۱-۶- بررسی انواع VPN
- ۱۲۴ ۱-۷- بررسی امنیت VPN
- ۱۲۵ ۱-۸- سخن آخر
- ۱۲۶ ۱-۹- سنوالات تشریحی

۱۲۶	۱۰-۱۰ سوالات چهارگزینه ای
۱۲۷	پاسخنامه

فصل یازدهم: حریم شخصی در مرورگرها ۱۲۹

۱۲۹	۱-۱۱ مقدمه
۱۳۰	۲-۱۱ مرورگر TOR
۱۳۰	۳-۱۱ مرورگر EPIC
۱۳۱	۴-۱۱ مرورگر PIRATE BROWSER
۱۳۲	۵-۱۱ انتخاب مرورگر مناسب
۱۳۳	۶-۱۱ سوالات تشریحی
۱۳۳	۷-۱۱ سوالات چهارگزینه ای
۱۳۴	پاسخنامه

فصل دوازدهم: امکانات امنیتی در سیستم عامل ویندوز ۱۳۵

۱۳۵	۱-۱۲ مقدمه
۱۳۵	۲-۱۲ صفحه کلید مجازی
۱۳۵	۳-۱۲ فایروال سیستم عامل ویندوز
۱۳۹	۴-۱۲ WINDOWS DEFENDER
۱۳۹	۵-۱۲ رمزنگاری در ویندوز
۱۴۰	۱-۵-۱۲ EFS
۱۴۳	۲-۵-۱۲ Export نمودن گواهی با استفاده از wizard
۱۵۰	۳-۵-۱۲ Cipher دستور
۱۵۳	۴-۵-۱۲ دسترسی به فایل‌های رمز شده
۱۵۷	۵-۵-۱۲ موارد امنیتی EFS
۱۵۷	۶-۵-۱۲ تهیه Copy از فایل‌های Encrypt شده
۱۵۸	۷-۵-۱۲ Export نمودن گواهی با دستور Cipher

- ۱۵۸ Import کردن گواهی ۱۲-۵-۸
- ۱۵۹ استفاده از داده های رمز شده توسط کاربران دیگر ۱۲-۵-۱۰
- ۱۶۰ رمزگذاری درایوها با استفاده از BIT LOCKER ۱۲-۶-۶
- ۱۶۰ Bit locker چیست؟ ۱۲-۶-۱
- ۱۶۰ BitLocker و EFS مقایسه ۱۲-۶-۲
- ۱۶۱ فعالسازی BitLocker برای یک درایو ۱۲-۶-۳
- ۱۶۹ استورات BitLocker در خط فرمان (CMD) ۱۲-۶-۴
- ۱۷۰ سنوالات تشریحی ۱۲-۷
- ۱۷۰ سنوالات چهار گزینه ای ۱۲-۸
- ۱۷۱ پاسخنامه ۱۲-۹

فصل سیزدهم: محافظت از IP ۱۷۳

- ۱۷۳ ۱-۱۳ مقدمه ۱۳-۱
- ۱۷۳ ۲-۱۳ یافتن IP ۱۳-۲
- ۱۷۳ ۱-۲-۱۳ Ping فرمان ۱۳-۲-۱
- ۱۷۴ ۲-۲-۱۳ IP Config / All فرمان ۱۳-۲-۲
- ۱۷۴ ۳-۲-۱۳ Net stat فرمان ۱۳-۲-۳
- ۱۷۷ ۴-۲-۱۳ به دست آوردن IP طرف مقابل هنگام استفاده از یاهو مسنجر ۱۳-۲-۴
- ۱۷۷ ۳-۱۳ خرم افزارهای محافظت از IP ۱۳-۳
- ۱۷۷ SafeIP - ۱-۳-۱۳ ۱۳-۳-۱
- ۱۷۸ Easy Hide IP - ۲-۳-۱۳ ۱۳-۳-۲
- ۱۷۸ Real Hide IP - ۳-۳-۱۳ ۱۳-۳-۳
- ۱۷۹ ۴-۱۳ سنوالات تشریحی ۱۳-۴
- ۱۷۹ ۵-۱۳ سنوالات چهارگزینه ای ۱۳-۵
- ۱۸۰ پاسخنامه ۱۳-۹

فصل چهاردهم: فایروال ها و آنتی ویروسها ۱۸۱

- ۱۸۱ ۱-۱۴ مقدمه
- ۱۸۲ ۲-۱۴ چرا از فایروال استفاده می‌کنیم؟
- ۱۸۲ ۳-۱۴ فایروال ها چگونه کار می‌کنند؟
- ۱۸۳ ۴-۱۴ بسته های امنیتی اینترنت و آنتی ویروسها
- ۱۸۳ ESET Smart Security-۱-۴-۱۴
- ۱۸۳ ESET NOD32 Antivirus-۲-۴-۱۴
- ۱۸۳ ESET Endpoint Security ۳-۱-۱۴
- ۱۸۳ Norton 360-۴-۴-۱۴
- ۱۸۵ Norton Internet Security-۵-۴-۱۴
- ۱۸۶ Bitdefender Total Security-۶-۴-۱۴
- ۱۸۶ Symantec Endpoint Protection-۷-۴-۱۴
- ۱۸۷ Panda Global Protection-۸-۴-۱۴
- ۱۸۷ Kaspersky Internet Security-۹-۴-۱۴
- ۱۸۷ Kaspersky Internet Security-۱۰-۴-۱۴
- ۱۸۸ ZoneAlarm Pro-۱۱-۴-۱۴
- ۱۸۹ NSasoft BlueAuditor-۱۲-۴-۱۴
- ۱۸۹ ۵-۱۴ سنوالات تشریحی
- ۱۸۹ ۶-۱۴ سنوالات چهارگزینه ای
- ۱۹۰ پاسخنامه:

فصل پانزدهم: نرم افزارهای محافظت از اطلاعات ۱۹۱

- ۱۹۱ ۱-۱۵ مقدمه
- ۱۹۱ DISK DRIVE ADMINISTRATOR-۲-۱۵

۱۹۲	FOLDER LOCK-۳-۱۵
۱۹۲	FOLDER GUARD-۴-۱۵ حفاظت از پوشه ها
۱۹۳	O&O SAFEERASE PROFESSIONAL-۵-۱۵
۱۹۳	TENORSHARE DATA WIPE-۶-۱۵
۱۹۴	ACTIVE KILLDISK PROFESSIONAL SUITE-۷-۱۵
۱۹۴	COPY PROTECT-۸-۱۵
۱۹۴	GILISOFT PRIVACY PROTECTOR-۹-۱۵ حفظ حریم خصوصی
۱۹۵	SECRET DIARY-۱۰-۱۵
۱۹۵	HDD LOW LEVEL FORMAT TOOL-۱۱-۱۵
۱۹۵	TRACKS ERASER PRO-۱۲-۱۵
۱۹۶	POINTSTONE TOTAL PRIVACY-۱۳-۱۵
۱۹۷	۱۴-۱۵ سنوالات تشریحی
۱۹۷	۱۵-۱۵ سنوالات چهارگزینه‌ای
۱۹۸	پاسخنامه

فصل شانزدهم: مراقبت از فرزندان در فضای مجازی ۱۹۹

۱۹۹	۱-۱۶ مقدمه
۱۹۹	۲-۱۶ نرم افزار های فیلترینگ خانگی و نظارت بر عملکرد کودکان کاربران
۱۹۹	۱-۲-۱۶ kidlogger
۲۰۰	۲-۲-۱۶ I net
۲۰۰	۳-۲-۱۶ MM Guardian Parental Control
۲۰۰	۴-۲-۱۶ AppLock یا قفل کننده اپلیکیشن
۲۰۱	۵-۲-۱۶ selfeld Child Control
۲۰۲	۶-۲-۱۶ Kids PC Time Administrator
۲۰۳	۳-۱۶ افزونه های فایر فاکس
۲۰۵	۵-۱۶ سنوالات تشریحی

۶-۱۶. سنوالات چهارگزینه‌ای ۲۰۵

پاسخنامه: ۲۰۶

مراجع: ۲۰۶

www.ketab.ir



مقدمه مولف:

امروزه با گسترش روز افزون اینترنت، تجارت الکترونیک و بانکداری مبتنی بر اینترنت، سازمانها بسیاری از سرویسهای خود را از طریق اینترنت ارائه میدهند. همچنین تعداد فروشگاههای اینترنتی نیز به شدت افزایش یافته است. اما وجود آسیب پذیری در سیستمهای کامپیوتری باعث شده است که کاربران اینترنت با تهدیدهای زیادی روبرو باشند. نفوذگران از بد ابزارها و مکانیزمهای مهاجمی مختلفی برای نفوذ، آسیب رسانی یا سرقت اطلاعات استفاده می کنند. لذا همه کاربران اینترنت باید شش مورد نیاز در زمینه حریم خصوصی و امنیت اینترنت را کسب نمایند. با توجه به نیاز کاربران اینترنت به منبعی کاربردی و جامع این کتاب را تألیف نمودم. در این کتاب سعی شده است که مناسب، زیبا، ساده ارائه گردد که تمامی مخاطبین بتوانند از آن استفاده نمایند. همچنین این کتاب سر فصلهای وزارت علوم، تحقیقات و فناوری برای درس حریم خصوصی و امنیت اینترنت را پوشش میدهد. در پایان هر فصل نیز تعدادی سؤال تشریحی و چهارگزینه ای تألیفی وجود دارد تا دانشجویان گرامی بهتر بتوانند خود را برای آزمونهای پیش رو آماده نمایند. از مخاطبین گرامی تقاضا دارم نقطه نظرات خود را از طریق ایمیل m.a.torkamani@gmail.com با اینجانب در میان بگذارند تا انشأاً در ویرایشهای بعدی کتاب اشکالات یا کاستیهای احتمالی آن، مورد تجدید نظر قرار گیرد. در پایان وظیفه خود می دانم از زحمات همکار گرامی، آقای مهندس علی بیات به خاطر طراحی جلد کتاب و همچنین مدیریت انتشارات ارسطو جناب آقای حسین قنبری به خاطر مساعدت در کار چاپ تشکر و قدردانی نمایم.