بخش اول مقدمه‌ای بر تجارت ۲۹

فصل اول عصر اینترنت-تجارت‌الکترونیکی ۳۱

❖ تکامل تجارت ۳۲

○ تجارت‌الکترونیکی در مقابل تجارت سنتی ۳۳

○ کالاهای سخت در مقابل کالاهای دیجیتالی ۳۴

○ مزایای استفاده از تجارت‌الکترونیکی در مقابل تجارت سنتی ۳۵

❖ پرداخت ۳۸

○ پول ۳۸

○ نقش‌های اساسی پول ۳۹

○ انواع تقسیم‌بندی پول ۴۱

○ شبکه‌های مالی ۴۲

■ رایانش کارتی ۴۷

○ پرداخت و تجارت سیّار ۵۴

❖ رایانش توزیع‌شده-افزودن E (الکترونیکی) به تجارت ۵۸

○ سرویس‌دهنده/ مشتری ۵۸

○ رایانش شبکه‌ای ۶۱

○ رایانش ابری ۶۳

○ مشخصه‌های سازنده رایانش ابری ۶۹

○ امنیت ابر ۷۳

■ بازنگری معماری ۷۴

■ احرازهویت متمرکز ۷۵

■ ورود یکپارچه و تفویض‌اختیار ۷۵

■ کنترل‌دسترسی مبتنی بر نقش ۷۶

■ مخزن گواهی ۷۶

■ ارتباطات و ذخیره‌سازی امن ۷۷

■ مدیریت مجزا ۷۷

۷۷ ▪ مطابقت با مقررات (پیروی قانونی)
۷۸ ▪ اعتماد توزیع‌شده (توزیع اعتماد)
۷۸ ▪ تازگی
۷۸ ▪ اعتماد
۷۹ ▪ جداسازی امن
۸۱ ▪ تفویض‌اختیار
۸۳ ▪ تهدیدها
۸۹ ▪ جنبه‌های عملیاتی
۹۲ ▪ حاکمیت

۹۷ فصل دوم تجارت سیّار
۹۹ ❖ مفهوم و جایگاه تجارت‌سیّار
۱۰۰ ○ مشخصه‌های تجارت‌سیّار
۱۰۱ ○ حوزه‌های کاربرد تجارت‌سیّار
۱۰۲ ○ عوامل بازدارنده و محدودیت‌های تجارت‌سیّار
۱۰۴ ❖ دستگاه‌های الکترونیکی کاربری
۱۰۴ ❖ گوشی تلفن‌همراه و تجارت‌سیّار
۱۰۵ ○ چشم‌انداز
۱۰۹ ○ تجارت‌سیّار در مقابل تجارت‌الکترونیکی
۱۱۰ ▪ سخت‌افزار سیّار
۱۱۱ ▪ سازنده دستگاه
۱۱۲ ▪ سیستم‌عامل
۱۱۳ ▪ پشته
۱۱۴ ▪ مدل کاربرد
۱۱۸ ▪ حالت سیّار
۱۲۰ ❖ فن‌آوری‌های سیّار: پشته روی استروئیدها
۱۲۰ ○ شبکه‌های حامل

۱۲۴ ○ پشته‌های سیّار
۱۲۵ ■ نسخه میکروی جاوا
۱۳۱ ■ اندروید
۱۳۹ ■ بلک‌بری
۱۴۱ ■ آیفون
۱۴۶ ■ سیمبین
۱۴۸ ○ پشته‌های دیگر

۱۵۱ فصل سوم نقش قابلیت‌ها در امنیت تجارت‌الکترونیکی
۱۵۲ ❖ محرمانگی، صحت و دسترس‌پذیری
۱۵۲ ○ محرمانگی
۱۵۴ ○ صحت
۱۵۵ ○ دسترس‌پذیری
۱۵۶ ❖ توسعه‌پذیری
۱۵۷ ○ توسعه‌پذیری جعبه‌سیاه
۱۵۸ ○ توسعه‌پذیری جعبه‌سفید
۱۵۸ ○ توسعه‌پذیری جعبه شیشه‌ای
۱۶۰ ○ توسعه‌پذیری جعبه خاکستری
۱۶۱ ❖ قابلیت تحمل خطا
۱۶۱ ○ دسترس‌پذیری بالا
۱۶۲ ■ پرش الکترونیکی
۱۶۲ ■ رخدادنگاری از راه‌دور
۱۶۲ ■ ایجاد پایگاه‌داده سایه
۱۶۲ ■ سرویس‌دهنده افزونه
۱۶۳ ■ خوشه‌بندی سرویس‌دهنده
۱۶۳ ■ خطوط ارتباطی افزونه
۱۶۳ ○ تحمل خطا در شبکه ارتباطات از راه‌دور

۱۶۴ ❖ قابلیت تعامل‌پذیری
۱۶۴ ○ استانداردهای تعامل‌پذیری
۱۶۵ ○ آزمون قابلیت تعامل‌پذیری
۱۶۶ ❖ قابلیت نگهداری
۱۶۷ ❖ قابلیت اداره/ مدیریت‌پذیری
۱۶۸ ❖ ماژولار بودن/ پیمانه‌ای بودن
۱۶۸ ❖ قابلیت پایش
۱۷۰ ○ تشخیص نفوذ
۱۷۱ ○ آزمون نفوذپذیری
۱۷۱ ○ تحلیل انحراف/ تخلف
۱۷۳ ❖ قابلیت عملیاتی‌شدن
۱۷۳ ○ حفاظت از منابع و موجودیت‌های ممتاز
۱۷۴ ○ دسته‌بندی‌های کنترل‌های مربوط به قابلیت عملیاتی‌شدن تجارت‌الکترونیکی
۱۷۶ ❖ قابلیت حمل
۱۷۷ ❖ قابلیت پیش‌بینی
۱۷۸ ❖ قابلیت اطمینان
۱۸۰ ❖ همه‌جا حاضر
۱۸۱ ❖ قابلیت استفاده
۱۸۱ ❖ مقیاس‌پذیری
۱۸۳ ❖ پاسخگویی
۱۸۴ ❖ قابلیت ممیزی
۱۸۶ ❖ قابلیت ردیابی

۱۸۹ بخش دوم امنیت تجارت‌الکترونیکی

۱۹۱ فصل چهارم مبانی تجارت‌الکترونیکی

۱۹۳ ❖ چگونه یک سیستم امن می‌شود

۱۹۶ ❖ امنیت مخاطره‌محور (مبتنی بر مخاطره)

۱۹۹ ❖ امنیت و قابلیت استفاده

۱۹۹ ○ قابلیت استفاده از کلمه‌های عبور

۲۰۰ ○ نکات کاربردی

۲۰۰ ❖ امنیت مقیاس‌پذیر

۲۰۱ ❖ تراکنش‌های خود را امن کنید

۲۰۵ فصل پنجم بلوک‌های سازنده: ابزارهای امنیتی در اختیار شما

۲۰۶ ❖ رمزنگاری

۲۰۶ ○ نقش رمزنگاری

۲۰۷ ○ سیستم‌های رمزنگاری متقارن

۲۰۸ ■ اصول رمزنگاری با کلیدمتقارن

۲۰۹ ○ نمونه‌هایی از سیستم‌های رمزنگاری ساده

۲۰۹ ■ سیستم رمز سزار

۲۱۱ ■ سیستم رمز ویگنِر

۲۱۳ ■ رمزنگاری از طریق جابجایی (تبدیل)

۲۱۴ ■ سیستم رمز ورنام (کلید رمز یک‌بار مصرف)

۲۱۶ ■ رمزهای بلوکی

۲۱۹ ■ بردار مقداردهی اولیه

۲۲۰ ■ رمزهای دنباله‌ای

۲۲۱ • استاندارد رمزنگاری داده‌ها

۲۲۳ • استاندارد رمزنگاری سه‌گانه داده‌ها

۲۲۳ • استاندارد رمزنگاری پیشرفته

۲۲۵ • الگوریتم بین‌المللی رمزنگاری داده‌ها

۲۲۵ ○ سیستم‌های رمزنگاری نامتقارن
۲۲۶ ■ توابع رمزنگاری یک‌طرفه
۲۲۷ ■ الگوریتم‌های کلیدعمومی
۲۲۸ • الگوریتم آر.اِس.اِی
۲۲۸ • الگوریتم اِل.جَمال
۲۲۹ • الگوریتم منحنی بیضوی
۲۳۰ ■ مقایسه طول کلید در الگوریتم‌های رمزنگاری متقارن و نامتقارن
۲۳۰ ■ امضاء دیجیتالی
۲۳۱ ■ خلاصه پیام
۲۳۳ ■ ویژگی‌های تابع درهم‌ریزی
۲۳۴ ■ استانداردهای امضاءدیجیتالی و درهم‌ریزی امن
۲۳۶ ■ کد احرازهویت پیام درهم‌ریزی شده
۲۳۶ ○ تبادل کلید دفی-هِلمن
۲۳۸ ○ زیرساخت کلیدعمومی
۲۳۸ ■ گواهی دیجیتالی
۲۳۹ ■ دایرکتوری‌ها و X.500
۲۴۰ ■ پروتکل سبک‌وزن دسترسی به دایرکتوری
۲۴۰ ■ گواهی‌نامه‌های X.509
۲۴۲ ■ فهرست ابطال گواهی
۲۴۳ ■ الحاقیه‌های گواهی‌نامه X.509
۲۴۴ ○ تولید اعداد تصادفی
۲۴۶ ○ سیستم‌های صدورگواهی کلیدعمومی- گواهی‌نامه دیجیتالی
۲۴۷ ■ مدیریت کلید
۲۴۷ • توزیع کلید
۲۴۸ • ابطال کلید
۲۴۸ • بازیابی کلید

۲۴۹ • تجدید یا تغییر کلید
۲۴۹ • از بین بردن یا تخریب کلید
۲۵۰ • کلیدهای چندگانه
۲۵۰ • توزیع‌شدگی در مقابل مدیریت متمرکز کلید
۲۵۰ ○ حفاظت از داده‌ها
۲۵۰ ■ مقابله با از دست‌دادن داده‌ها
۲۵۲ ■ امنیت پایگاه‌داده
۲۵۴ ❖ کنترل‌دسترسی
۲۵۴ ○ کنترل‌ها
۲۵۵ ○ مدل‌های کنترل‌دسترسی
۲۵۵ ■ کنترل‌دسترسی اجباری
۲۵۷ ■ کنترل‌دسترسی اختیاری
۲۵۷ ■ کنترل‌دسترسی غیراختیاری (مبتنی بر نقش)
۲۵۸ ■ کنترل‌دسترسی وب
۲۵۹ ■ جایگاه کنترل‌دسترسی در امنیت تجارت‌الکترونیکی
۲۶۰ ❖ مقاوم‌سازی سیستم
۲۶۰ ○ امنیت سطح خدمت
۲۶۰ ■ سرویس‌دهنده‌های وب
۲۶۲ ■ امنیت سرویس‌دهنده وب
۲۷۱ ■ خدمات وب
۲۷۵ ■ کاربردهای تحت وب
۲۸۰ ○ امنیت در سطح میزبان
۲۸۰ ■ سیستم‌های عامل
۲۸۱ ■ مرورگر کاربران
۲۸۳ ■ کاربر محلی
۲۸۴ ○ امنیت شبکه

۲۸۴ ▪ دیواره‌آتش
۲۸۷ ▪ پروتکل‌ها
۲۹۹ ▪ پست‌الکترونیکی
۳۰۰ ▪ مشکل‌های بدافزاری

۳۰۷ **فصل ششم مؤلفه‌های سیستم: نحوه اجرا و پیاده‌سازی**
۳۰۸ ❖ احرازهویت
۳۰۸ ○ احرازهویت کاربر
۳۰۹ ▪ کلمه‌های عبور
۳۱۱ ▪ بایومتریک
۳۱۳ ○ احرازهویت شبکه
۳۱۶ ○ احرازهویت دستگاه
۳۱۸ ○ احرازهویت واسط برنامه‌کاربردی
۳۱۸ ▪ احرازهویت پایه HTTP
۳۱۸ ▪ احرازهویت دسترسی محدود HTTP
۳۱۹ ▪ الگوی احرازهویت درخواست- پاسخ سیستم‌عامل ویندوز
۳۲۰ ▪ احرازهویت براساس تابع AuthSub
۳۲۱ ○ احرازهویت فرآیند
۳۲۳ ❖ تفویض‌اختیار
۳۲۴ ❖ عدم انکار
۳۲۴ ❖ حریم‌خصوصی
۳۲۵ ○ خط‌مشی حریم‌خصوصی
۳۲۶ ○ قوانین و رهنمودهای مرتبط با حریم‌خصوصی
۳۲۷ ○ اصول اتحادیه اروپا
۳۲۸ ○ مسائل حریم‌خصوصی مرتبط با امور پزشکی
۳۲۹ ○ پلت‌فرمی برای توصیف اولویت‌های حریم‌خصوصی
۳۳۰ ○ پایش الکترونیکی

۳۳۲ ❖ امنیت اطلاعات
۳۳۲ ○ مفاهیم مدیریت امنیت
۳۳۳ ■ چرخه عمر امنیت سیستم
۳۳۳ ■ محرمانگی، صحت و دسترس‌پذیری
۳۳۵ ■ معماری امنیتی چندلایه
۳۳۶ ■ کنترل‌های امنیتی
۳۳۷ ❖ طبقه‌بندی داده‌ها و اطلاعات
۳۳۷ ○ مزایای طبقه‌بندی اطلاعات
۳۳۸ ○ مفاهیم طبقه‌بندی اطلاعات
۳۳۸ ■ اصطلاح‌های طبقه‌بندی
۳۴۰ ■ معیارهای طبقه‌بندی اطلاعات
۳۴۰ ■ روندهای طبقه‌بندی اطلاعات
۳۴۱ ■ توزیع اطلاعات طبقه‌بندی شده
۳۴۱ ■ نقش‌های مرتبط با طبقه‌بندی اطلاعات
۳۴۵ ○ دسته‌بندی داده
۳۴۶ ○ مدل Bell-LaPandula
۳۴۸ ❖ ممیزی داده‌ها و سیستم
۳۴۹ ○ پروتکل سیس‌لاگ
۳۵۲ ○ سامانه SIEM
۳۵۴ ❖ دفاع در عمق
۳۵۸ ❖ اصل حداقل حقوق‌دسترسی
۳۶۰ ❖ اعتماد
۳۶۲ ❖ جداسازی
۳۶۲ ○ مجازی‌سازی
۳۶۳ ○ جعبه‌شنی
۳۶۳ ○ جداسازی دامنه امنیتی پروتکل اینترنت

۳۶۴ ❖ خط‌مشی امنیتی
۳۶۵ ○ بیانیه خط‌مشی مدیریت ارشد
۳۶۵ ■ خط‌مشی‌های توصیه‌ای
۳۶۵ ■ خط‌مشی‌های مقرراتی
۳۶۵ ■ خط‌مشی‌های آگاهی‌رسانی
۳۶۶ ○ طبقه‌بندی خط‌مشی توسط مؤسسه استانداردها و فن‌آوری
۳۶۷ ❖ امنیت ارتباطات
۳۶۷ ○ امنیت بین‌شبکه‌ای
۳۶۹ ■ شبکه‌های همگن
۳۷۰ ■ شبکه‌های ناهمگن

۳۷۶ **فصل هفتم اعتماد کنید اما بررسی نمایید: شرایط امنیتی را کنترل نمایید**
۳۷۴ ❖ ابزارهای بررسی امنیت
۳۷۷ ○ ارزیابی آسیب‌پذیری و تحلیل تهدید
۳۷۸ ○ تشخیص و جلوگیری از نفوذ با استفاده از اِسنورت
۳۸۱ ○ پویش شبکه با استفاده از اِن‌مَپ
۳۸۲ ○ پویش آسیب‌پذیری
۳۸۲ ■ نِسوس
۳۸۴ ■ نیک‌تو
۳۸۴ ■ وایِرشارک
۳۸۵ ○ آزمون نفوذپذیری
۳۸۶ ■ مِتااِسپلویت
۳۸۷ ■ اِیرکِرَک-اِن‌جی
۳۸۹ ○ شناسایی شبکه‌های بی‌سیم
۳۸۹ ■ نِت اِستامبِلر
۳۹۰ ■ کیزمِت
۳۹۱ ■ تحلیل‌گر شبکه‌های وای‌فای شرکت اِیرمَگنِت

۳۹۳ ○ بررسی کاربردهای تحت‌وب
۳۹۳ ▪ لِینکس
۳۹۴ ▪ وی‌جِت
۳۹۶ ▪ تِلِپورت
۳۹۶ ▪ بِلَک‌ویندو
۳۹۸ ▪ بِراون‌ریکلیز

۴۰۱ **فصل هشتم تهدیدها و حمله‌ها: آنچه مهاجمان انجام می‌دهند**
۴۰۳ ❖ مفاهیم پایه
۴۰۳ ○ هدف
۴۰۴ ○ تهدید
۴۰۵ ○ حمله
۴۰۶ ○ کنترل
۴۰۷ ○ خط‌مشی یکسان و همسو برای منابع
۴۰۸ ❖ حمله‌های رایج در حوزه تجارت‌الکترونیکی
۴۰۸ ○ حمله دورزدن سازوکارهای احرازهویت و مدیریت نشست
۴۱۰ ○ جعل درخواست/ کلاهبرداری از طریق ارسال درخواست کد بین‌سایتی
۴۱۵ ○ حمله ارسال کد بین‌سایتی
۴۱۶ ▪ ارسال کد دایمی/ ذخیره‌شده بین‌سایتی
۴۱۶ ▪ ارسال کد غیردائمی/ انعکاسی بین‌سایتی
۴۱۷ ▪ ارسال کد بین‌سایتی مبتنی بر مدل شیء مستند
۴۲۱ ○ حمله سرقت از سیستم نام دامنه
۴۲۲ ○ حمله نقض محدودیت دسترسی به URL
۴۲۳ ○ رخنه‌های تزریقی
۴۲۸ ○ حفاظت نامناسب از لایه انتقال
۴۲۸ ○ حمله ذخیره‌سایز ناامن رمزنگاری
۴۳۰ ○ حمله ارجاع ناامن مستقیم به شیء

۴۳۱ ○ حمل‌های کلاهبرداری و ارسال هرزنامه
۴۳۲ ○ رخنه‌افزار و حمله‌های مرتبط با آن
۴۳۳ ○ حمله‌های مرتبط با پیکربندی ضعیف امنیتی
۴۳۳ ○ حمله راهبری و هدایت غیرمعتبر

۴۳۷ فصل نهم صدورگواهی: تضمین
۴۳۸ ❖ صدورگواهی و اعتباردهی
۴۳۸ ○ فرآیند صدورگواهی
۴۳۹ ■ ارزیابی کنترل‌های امنیتی
۴۴۲ ❖ استانداردها و رهنمودهای مربوطه
۴۴۲ ○ معیارهای ارزیابی سیستم‌های رایانه‌ای مورداعتماد
۴۴۳ ○ معیارهای مشترک (استاندارد ۱۵۴۰ سازمان بین‌المللی استاندارد)
۴۴۴ ○ فرآیند صدورگواهی و اعتباردهی در حوزه تضمین اطلاعات دفاعی
۴۴۷ ○ بخشنامه شماره A-130 دفتر مدیریت و بودجه
۴۴۸ ○ فرآیند ملی صدورگواهی و اعتباردهی در حوزه تضمین اطلاعات
۴۵۲ ○ قانون مدیریت امنیت اطلاعات فدرال
۴۵۳ ○ چارچوب ارزیابی امنیت فن‌آوری اطلاعات فدرال
۴۵۴ ○ استاندارد شماره ۱۹۹ پردازش اطلاعات فدرال
۴۵۵ ○ استاندارد شماره ۲۰۰ پردازش اطلاعات فدرال
۴۵۷ ○ سایر منابع و رهنمودها
۴۵۷ ❖ سازمان‌ها و نهادهای استانداردگذاری مرتبط
۴۵۸ ○ انجمن جریکو
۴۵۸ ○ کارگروه مدیریت توزیع شده
۴۵۹ ○ سازمان بین‌المللی استاندارد/ کمیسیون بین‌المللی برق
۴۶۳ ○ مؤسسه استانداردهای مخابراتی اروپا
۴۶۳ ○ انجمن صنعتی شبکه‌های ذخیره‌سازی
۴۶۴ ○ پروژه امنیت برنامه‌های‌کاربردی متن‌باز

۴۶۸ ○ سند ۳۰-۸۰۰ مؤسسه استانداردها و فن‌آوری ایالات متحده آمریکا
۴۷۱ ❖ آزمایشگاه‌های صدورگواهی
۴۷۱ ○ آزمایشگاه تضمین مرکز مهندسی نرم‌افزار
۴۷۲ ○ سایک (مؤسسه بین‌المللی کاربردهای علم)
۴۷۲ ○ آزمایشگاه‌های انجمن بین‌المللی امنیت رایانه
۴۷۳ ❖ مدل بلوغ ظرفیت مهندسی امنیت سیستم‌ها
۴۷۶ ❖ ارزش صدورگواهی
۴۷۷ ○ وقتی که صدورگواهی اهمیت دارد
۴۷۸ ○ وقتی که صدورگواهی اهمیتی ندارد
۴۷۸ ❖ انواع گواهی‌نامه
۴۷۸ ○ معیارهای مشترک
۴۷۹ ○ آزمون سازگاری و امنیت کارت هوشمند
۴۸۰ ○ پرداخت اروپایی، کارت هوشمند و ویزا
۴۸۰ ▪ کارت اعتباری/ بدهی هوشمند ویزا
۴۸۱ ▪ کارت هوشمند/ پردازنده
۴۸۱ ○ مدل ترکیبی پلت‌فرم جهانی
۴۸۲ ○ سایر معیارهای ارزیابی
۴۸۴ ○ آژانس امنیت ملی آمریکا
۴۸۵ ○ گواهی‌نامه شماره ۱۴۰

۴۸۸ **علائم اختصاری**

۵۰۷ **منابع**