باسمه تعالی

طرح درس جهت ارائه در نیمسال تحصیلی دوم ۱۴۰۳-۱۴۰۲

دانشکده	**مهندسی صنایع و سیستم‌ها**	**گروه**	**مهندسی فناوری اطلاعات**
گرایش	**سیستم‌های اطلاعاتی**	**مقطع**	**کارشناسی ارشد**
نام درس	**امنیت سیستم‌های اطلاعات**	**نوع درس**	**پایه** ☐ **نظری** ☑ **تخصصی** ☑ **عملی** ☐ **اختیاری** ☐ **نظری-عملی** ☐
تعداد واحد	**۳**	**نام اساتید**	**حسین همائی، صادق درّی نوگورانی و مهرداد کارگری**
دروس پیش‌نیاز	**ندارد**	**تلفن دفترکار**	**۳۹۰۵، ۵۰۹۸ و ۴۹۵۵**
دروس هم‌نیاز	**ندارد**	**پست الکترونیک**	homaei@modares.ac.ir dorri@modares.ac.ir m_kargari@modares.ac.ir

✓ **اهداف درس:**

۱. آشنایی با اصول اولیه امنیت
۲. آشنایی با مفاهیم کاربردی رمزنگاری
۳. آشنایی با ساز و کارهای پایه برقراری امنیت
۴. آشنایی با چالش‌های امنیتی سیستم‌ها و شبکه‌های رایانه‌ای
۵. آشنایی با روش‌های امن‌سازی سیستم‌ها و شبکه‌های رایانه‌ای
۶. آشنایی با نحوه تلفیق امنیت و چرخه حیات توسعه نرم‌افزار
۷. آشنایی با آسیب‌پذیری‌های نرم‌افزاری و چگونگی بهره‌مندی مهاجمان از آن‌ها
۸. آشنایی با مکانیزم‌های امنیتی شبکه
۹. آشنایی با استانداردهای مدیریت امنیت

✓ **رئوس مطالب و برنامه ارائه در کلاس:**

شماره هفته	موضوع جلسه درس	توضیحات
جلسات هفته اول	مقدمه	مبانی و تعاریف اولیه، نیازمندی‌های امنیتی، تهدیدات امنیتی، اقدامات امنیتی
جلسات هفته دوم	مسائل مدیریتی در امنیت	چارچوب امنیتی طرح‌های کلان فاوا، ساختار سازمانی امنیت، اصول مهم امنیت
جلسات هفته سوم	سازوکارهای پیشگیری	شناسایی و احراز اصالت، کنترل دسترسی، دیوار آتش، رمزنگاری و امضای دیجیتال، زیرساخت کلید عمومی (PKI)
جلسات هفته چهارم	سازوکارهای تشخیص	ضد بدافزارها، سامانه‌های تشخیص نفوذ، تله عسل‌ها
جلسات هفته پنجم	سازوکارهای ترمیم و پاک‌سازی	انواع روش‌های پشتیبان‌گیری، روش‌های امن پاک‌سازی رسانه
جلسات هفته ششم	مقدمه‌ای بر امنیت نرم‌افزار	اهمیت موضوع، اصول اولیه امنیت نرم‌افزار
جلسات هفته هفتم	تلفیق امنیت و چرخه حیات توسعه نرم‌افزار	اصول کلی، آشنایی با بازبینی کد و تست نفوذ

جلسات هفته هشتم	تلفیق امنیت و چرخه حیات توسعه نرم‌افزار	اصول تحلیل و مدیریت مخاطرات امنیتی نرم‌افزار، تحلیل مقاومت در برابر حمله، تحلیل ابهام، تحلیل ضعف
جلسات هفته نهم	تلفیق امنیت و چرخه حیات توسعه نرم‌افزار	آزمون امنیتی مبتنی بر ریسک، نیازمندی‌های امنیتی، ضد نیازمندی، موارد سوء استفاده، استقرار امن
جلسات هفته دهم	مدل‌سازی تهدید	اصول مدل‌سازی تهدید، STRIDE، درخت حمله، روش‌های مقابله با تهدیدات، اولویت‌بندی تهدیدات
جلسات هفته یازدهم	طراحی امن نرم‌افزار	روش‌های برآورده کردن محرمانگی، صحت، دسترس‌پذیری، تصدیق اصالت، مجازشناسی و ممیزی در طراحی نرم‌افزار
جلسات هفته دوازدهم	آشنایی با آسیب‌پذیری‌های نرم‌افزاری رایج	تزریق SQL، ربودن نشست، جعل درخواست بین‌سایتی، اسکریپت بین‌سایتی، سرریز بافر
جلسات هفته سیزدهم	آشنایی با اصول اولیه شبکه و امنیت آن	تجهیزات و پروتکل‌های شبکه، روش‌های حفاظت از شبکه، ابزارهای امنیتی شبکه، برخی پروتکل‌های امنیتی، امنیت شبکه‌های بی‌سیم
جلسات هفته چهاردهم	معماری امنیتی	MODAF
جلسات هفته پانزدهم	مدیریت مخاطرات	تحلیل و مدیریت مخاطرات امنیتی، پیشگیری از و پاسخ‌دهی به رخدادهای امنیتی
جلسات هفته شانزدهم	استانداردهای مدیریت امنیت اطلاعات	OCTAVE، ITIL، COBIT، ISMS

✓ **روش ارزشیابی:**

تمرین‌ها و پروژه‌ها (۴ نمره)، امتحانات (۱۶ نمره)

✓ **منابع :**

[1] W. Stallings, and L. Brown. *Computer security: principles and practice*. 4th edition, Pearson Education, 2017.
[2] W. Stallings, *Cryptography and Network Security*. 6th edition, Pearson, 2014
[3] M. Chapple, J. M. Stewart, and D. Gibson. *CISSP: Certified information systems security professional official study guide*. 8th edition, John Wiley & Sons, 2018.
[4] M. Bishop. *Introduction to Computer Security*. Addison-Wesley Professional, 2004.
[5] G. McGraw, *Software Security: Building Security In*, Addison-Wesley, 2006.
[6] M. Paul, *Official (ISC)² guide to the CSSLP CBK*. 2nd edition, CRC Press, 2014.
[7] A. Shostack, *Threat Modeling: Designing for Security*, Wiley, 2014.
[8] R. Anderson, *Security engineering*. Wiley, 2008.
[9] H. Carvey, *Windows Forensic Analysis DVD Toolkit*, 2nd Edition, Syngress, 2009.