حراست باید شکارچی
تهدید باشد، نه قربانی

برای اولین بار در ایران

دوره جامع ترکیبی

مدیریت امنیت سایبری

دانشگاه پیام نور - محفا شریف

دوره جامع ترکیبی
مدیریت امنیت سایبری

دوره جامع ترکیبی "مدیریت امنیت سایبری" دوره‌ای مشترک بین دانشگاه پیام نور تهران و مدرسه حاکمیت فن آوری اطلاعات شریف (محفا شریف) است که **طی ۱۱۲ ساعت** به صورت فشرده و اجرایی برگزار می شود.

این دوره در ۷ سرفصل درسی تعریف شده است که آخر هفته‌ها **توسط برخی از برجسته‌ترین متخصصین تجربی حوزه امنیت سایبری کشور** برگزار می‌شود. این دوره به صورت حضوری، آنلاین و آفلاین برگزار شده و مدرک معتبر پایان دوره توسط دانشگاه پیام نور اعطا می‌شود و هدف آن:

انتقال دانش تخصصی و جامع مدیریت امنیت سایبری به بدنه حراست کل کشور است.

آیا می‌دانید:

- اکثر مدیران حراست، هیچ دوره تخصصی سایبری ندیده‌اند؟
- طبق قوانین کشور،عالی‌ترین مقام اجرایی هر سازمان، مسئول تبعات حوزه امنیت سایبری آن سازمان محسوب می‌شود؟
- عدم آموزش کارکنان در حوزه امنیت سایبری یکی از اصلی‌ترین عوامل موفقیت حملات سایبری است؟
- ایران یکی از بزرگترین میدان‌های جنگ سایبری در دنیا است؟
- ایران همواره هدف قدرتمندترین و پیشرفته‌ترین حملات سایبری استکبار جهانی قرار داشته است؟
- ایران رتبه ۵۴ بین ۱۸۲ کشور از نظر شاخص جهانی امنیت سایبری(GCI) را دارد؟
- حملات سایبری به طور روزافزونی پیچیده‌تر و هدفمندتر از گذشته شده است؟
- ماهیت حملات سایبری به طور مستمر تغییر پیدا می‌کند؟
- پس از نیروهای زمینی، هوایی، دریایی و فضایی؛ نیروی سایبری نیز در ارتش‌های جهان شکل گرفته است؟
- حملات فیشینگ یکی از بالاترین نرخهای حملات سایبری در سال‌های اخیر در کشور را دارا بوده است؟
- اکثر نفوذهای سایبری از طریق کارکنان(به صورت ناآگاهانه) و نه تجهیزات فنی در سازمان‌ها رخ می‌دهد؟
- اگرچه آماری از ایران در دست نیست، اما طبق آمارهای جهانی بیش از ۸۶% سازمان‌ها در سال ۲۰۲۴ تجربه حمله یا چالش امنیت سایبری داشته‌اند؟

چرا این دوره برای همه ما مهم و حیاتی است؟

- ایران همواره زیر آتش سایبری قرار دارد و حراست سپر نهایی سازمان در دفاع می‌باشد.
- نیاز به حفاظت از زیرساخت‌های حیاتی کشور یک الزام و تکلیف است.
- منبع تهدیدات سایبری کشور عموماً امریکا و اسرائیل است که همواره ادامه دارد.
- حراست سایبری مترادف با امنیت ملی در کشور محسوب می‌شود.
- اقتدار دفاعی ایران در گرو اقتدار سایبری است.
- امنیت سایبری ستون فقرات تاب آوری ملی محسوب می‌شود.
- حوزه امنیت سایبری به موازات امنیت فیزیکی در بسیاری از حراست‌ها شکل نگرفته و یا کارآمد نیستند.
- ساختار سازمانی امنیت سایبری در حراست‌ها نیاز به تعریف و شکل گیری دارد.
- با توجه به عدم تخصص مدیران عامل و روسای سازمان‌ها، مدیران و کارشناسان مربوطه در حکم چشم مدیران سازمان در حوزه امنیت سایبری محسوب می‌شوند.

همواره پیشگیری بهتر از درمان است!

مخاطبین دوره:

- مدیران حراست
- مدیران حوزه امنیت اطلاعات
- کارشناسان امنیت و حراست
- کارشناسان فناوری اطلاعات
- کارشناسان مرتبط
- علاقمندان حوزه امنیت سایبری

محتواهای دوره:

دوره جامع ترکیبی **مدیریت امنیت سایبری**

مبانی شبکه و نرم‌افزار

۱۶ ساعت

- **مفاهیم پایه شبکه‌های کامپیوتری:** مدل‌های OSI و TCP/IP، توپولوژی‌ها و پروتکل‌های اصلی شبکه
- **تجهیزات و زیرساخت‌های شبکه:** سوئیچ‌ها، روترها، فایروال‌ها و نحوه عملکرد آنها
- **مبانی نرم‌افزار و سیستم‌عامل:** ساختار سیستم‌عامل‌های ویندوز و لینوکس، مدیریت فرآیندها و حافظه
- **پروتکل‌های ارتباطی و خدمات شبکه:** HTTP/HTTPS، DNS، DHCP و نقش آن‌ها در ارتباطات
- **مفاهیم مجازی‌سازی و رایانش ابری:** اصول مجازی‌سازی، مزایا و چالش‌های رایانش ابری

اصول و مبانی مدیریت امنیت اطلاعات

۱۶ ساعت

- **مفاهیم کلیدی امنیت اطلاعات:** محرمانگی، یکپارچگی، دسترس‌پذیری (CIA) و اهمیت آن‌ها
- **سیاست‌ها و رویه‌های امنیتی سازمانی:** تدوین، پیاده‌سازی و نظارت بر سیاست‌های امنیتی
- **مدیریت دارایی‌های اطلاعاتی:** شناسایی، طبقه‌بندی و حفاظت از دارایی‌های اطلاعاتی
- **آموزش و آگاهی‌بخشی امنیتی:** برنامه‌های آموزشی برای کارکنان و ارتقاء فرهنگ امنیتی
- **پایش و بهبود مستمر امنیت اطلاعات:** ارزیابی اثربخشی کنترل‌ها و اقدامات اصلاحی

امنیت شبکه، ارزیابی آسیب‌پذیری و تست نفوذ

۱۶ ساعت

- **تهدیدات و آسیب‌پذیری‌های شبکه‌ای:** انواع حملات مانند DoS، Man-in-the-Middle و بدافزارها
- **ابزارها و فنون ارزیابی آسیب‌پذیری:** اسکنرها، تحلیلگرهای ترافیک و روش‌های شناسایی نقاط ضعف
- **مبانی تست نفوذ (Penetration Testing):** مراحل برنامه‌ریزی، اجرا و گزارش‌نویسی تست نفوذ
- **سیستم‌های تشخیص و جلوگیری از نفوذ (IDS/IPS):** عملکرد، پیاده‌سازی و مدیریت این سیستم‌ها
- **امنیت در شبکه‌های بی‌سیم و موبایل:** تهدیدات خاص و راهکارهای مقابله با آن‌ها
- **مدیریت رخدادهای امنیتی:** شناسایی، پاسخ و بازیابی از حوادث امنیتی

محتواهای دوره:

دوره جامع ترکیبی **مدیریت امنیت سایبری**

ممیزی امنیت اطلاعات

۱۶ ساعت

- **مفاهیم و اصول ممیزی امنیت اطلاعات:** اهداف، انواع و فرآیندهای ممیزی
- **برنامه‌ریزی و اجرای ممیزی:** تعیین دامنه، زمان‌بندی و منابع مورد نیاز
- **تدوین چک‌لیست‌ها و ابزارهای ممیزی:** طراحی ابزارهای ارزیابی و جمع‌آوری شواهد
- **گزارش‌دهی و پیگیری نتایج ممیزی:** تهیه گزارش‌های جامع و پیشنهادات بهبود
- **نقش ممیزی در بهبود مستمر امنیت اطلاعات:** استفاده از نتایج ممیزی برای ارتقاء امنیت

مدیریت ریسک‌های امنیت اطلاعات

۱۶ ساعت

- **چارچوب‌های مدیریت ریسک:** استانداردها و به‌روش‌هایی مانند ISO 31000 و ISO/IEC 27005
- **شناسایی و تحلیل ریسک‌های امنیتی:** روش‌های شناسایی تهدیدات و آسیب‌پذیری‌ها
- **ارزیابی و اولویت‌بندی ریسک‌ها:** معیارهای احتمال و تاثیر، ماتریس ریسک
- **استراتژی‌های مقابله با ریسک:** پذیرش، انتقال، کاهش و اجتناب از ریسک
- **تدوین برنامه‌های مدیریت ریسک:** تعیین اقدامات کنترلی و منابع مورد نیاز
- **پایش و بازنگری ریسک‌ها:** نظارت مستمر و به‌روزرسانی برنامه‌های مدیریت ریسک
- **ادغام مدیریت ریسک با اهداف سازمانی:** همسویی استراتژی‌های امنیتی با اهداف کسب‌وکار

قوانین و مقررات امنیت سایبری

۱۶ ساعت

- **چارچوب‌ها و استانداردهای امنیتی:** NIST، ISO/IEC 27001 و COBIT
- **قوانین و مقررات ملی:** الزامات امنیتی مراکز بالادستی نظیر افتا، پدآفند غیرعامل و بانک مرکزی
- **مسئولیت‌های قانونی سازمان‌ها و مدیران:** تعهدات قانونی در قبال حفاظت از اطلاعات
- **پیامدهای حقوقی نقض امنیت:** بررسی موارد حقوقی و جریمه‌های مرتبط با نقض امنیت اطلاعات

محتواهای دوره:

دوره جامع ترکیبی **مدیریت امنیت سایبری**

مدیریت حراست: از اصول حفاظت و تا بهینه سازی ساختاری

۱۶ ساعت

- مفاهیم و اصول پایه حفاظت در مدیریت حراست
- مدیریت تهدیدات و ریسک‌های امنیتی
- سیاست‌ها و رویه‌های حفاظت سازمانی
- مدیریت حفاظت فیزیکی و زیرساختی و سایبری
- مدیریت حفاظت اطلاعات و اسناد دیجیتال و سایبری
- بهینه‌سازی و به روزسازی ساختارهای حراستی
- آموزش و آگاهی‌بخشی پرسنل در حوزه حراست
- مدیریت بحران و پاسخ به حوادث امنیت
- روشهای بهره گیری از هوش مصنوعی در حراست سازمانی

چرا این دوره با مشخصات جامع و ترکیبی تعریف شده است ؟

راهبردی‌ترین شیوه دفاع سایبری، پدافند غیرعامل مبتنی بر پیش بینی، پیشگیری و پیش دستی تعریف شده است که نیازمند دانش جامع حوزه مدیریت امنیت سایبری است.

- دیدگاه جامع مبتنی بر آموزش ابتدایی‌ترین مفاهیم امنیت سایبری تا ممیزی و ارزیابی الزامات امنیت سایبری و قوانین تخصصی مرتبط جهت تربیت و تقویت دانش کارشناسان و مدیران حراست
- در نظر گرفتن کاربردی‌ترین مطالب آموزشی لازم در قالب بسته‌های آموزشی ۱۶ ساعته به صورت جامع و حرفه‌ای
- تدبیراندیشی برای کارکنان تمام وقت با مشغله‌های فراوان از جمله ماموریتها،شیفت ها و بازدیدهای گاه و بیگاه سازمانی
- استفاده از ظرفیت‌های آموزش مجازی دانشگاه پیام نور برای **"آموزش برای همه، همه وقت و همه جا"**

چرا دانشگاه پیام نور؟

- **پلتفرم آموزش مجازی پیشرفته**
- **گواهینامه رسمی و معتبر وزارت علوم**
- **انعطاف زمانی مناسب(۷/۲۴) برای دسترسی به محتواهای ضبط شده**
- **رتبه اول آموزش مجازی دولتی کشور**
- **مکان در نظر گرفته شده در مرکز شهر با دسترسی های مختلف پیش بینی شده**

چرا مدرسه حاکمیت فناوری اطلاعات شریف (محفا شریف)؟

- هاب آموزش امنیت سایبری در کشور
- دارای برخی از برجسته‌ترین متخصصان حوزه امنیت سایبری کشور
- تجربه ارائه خدمات آموزشی، مشاوره‌ای، منتورینگ، پیاده سازی و ممیزی:
  - امنیت سایبری(Cyber Security)
  - مدیریت امنیت فن آوری اطلاعات(Information Security Management System)
  - مدیریت خدمات فناوری اطلاعات(Information Technology Service Management)
  - مدیریت ریسک(Risk Management)
  - مدیریت تاب آوری، پایداری و استمرار فعالیت سازمانی(Business Continuity Management &Disaster Recovery)
  - حاکمیت فناوری اطلاعات(Information Technology Governance)
  - باز مهندسی فرآیندهای سازمانی(Business Process Reengineering)

MAHFA SHARIF

School of Information Technology Governance

(Cyber Security and Resilience Department)

دستیافت های پایان دوره:

- دانش کامل حوزه مدیریت امنیت سایبری
- انتقال تجربیات حرفه ای و تخصصی بین المللی و داخلی
- توانایی تدوین استراتژی و برنامه‌های امنیت سایبری برای سازمان
- توانایی پیاده‌سازی و نظارت مؤثر بر کنترل‌های امنیتی و طرح‌های امنیت سایبری
- مهارت کافی در آموزش کارمندان و کاربران تحت تأثیر کنترل‌های امنیتی
- تدوین و پیاده‌سازی روش‌های مدیریت ریسک امنیت اطلاعات
- شیوه‌های ممیزی و نظارت بر اجرای برنامه‌های امنیت اطلاعات
- استفاده از بسترهای موجود برای انتقال دانش، شبکه سازی و یادگیری بیشتر
- بسته آموزشی و تحصیلی دوره
- امکان معرفی به سازمانها، شرکتهای معتبر دولتی و خصوصی برای کارآموزی و کار

دانشگاه پیام نور

سازمان مرکزی: تهران شهرک نفت خیابان نخل سازمان مرکزی پیام نور
ستاد مرکز: تهران، میدان فردوسی، خیابان سپهبد قرنی، خیابان شهید فلاحپور، پلاک ۲۷ **(محل برگزاری حضوری دوره)**

www.pnu.ac.ir

مدرسه محفا شریف

تهران بلوار شهید خرازی شهرک نمونه بلوک جی طبقه ۵ واحد ۳۶
اصفهان خیابان شریعتی، خیابان شهید حیدری، بن‌بست شادی، پلاک ۲۱

www.mahfah.ir

۰۲۱۱۸۴۲۳۴۱۳۱
۰۹۱۲۰۸۵۵۵۹۷

www.web.eitaa.com/
#@CyberSecurityManagement