

به نام صاحب امن و امان

کتاب مرجع آموزش عرضی و کوتاه مدت

مباحث مقدماتی پدافند سایبری

پدیدآورندگان:

دکتر محمود خالقی دخت

عضو هیأت علمی پژوهشگاه ارتباطات و فناوری اطلاعات

و جمعی از همکاران

۱۴۰۱

سرشناسه	خالقی دخت، محمود
عنوان و نام پدیدآور	مباحث مقدماتی پدافند سایبری /محمود خالقی دخت
مشخصات نشر	تهران: سپک نو، ۱۴۰۰
مشخصات ظاهری	۱۵۰ ص- ۱۷۵ در ۲۴۵-
شابک	۹۷۸-۶۲۲-۹۹۳۹۲-۴-۶
وضعیت فهرست نویسی	فیبا
رده بندی کنگره	۱۴۰۰ / م۵ / ۴۴ / ۵۹ BP
رده بندی دیویی	۱۴۱/۲۹۷
شماره کتابشناسی ملی	۵۵۲۳۶۳۰۲
اطلاعات رکورد کتابشناسی	فیبا



عنوان: مباحث مقدماتی پدافند سایبری
تألیف: محمود خالقی دخت
صفحه آرای: عباس چراغ چشم
ناشر: سپک نو

نوبت چاپ: چاپ اول، ۱۴۰۱
چاپ و صحافی: قدرولایت
تیراژ: چاپ اول ۵۰۰ نسخه
شابک: ۹۷۸-۶۲۲-۹۹۳۹۲-۴-۶
تعداد صفحات: ۱۵۰ صفحه
قیمت: ۸۰۰۰ تومان

کلیه حقوق، اعم از چاپ و تکثیر، نسخه برداری، ترجمه و اقتباس برای سازمان پدافند غیرعامل محفوظ است.

فهرست

صفحه	عنوان
۶	فصل اول:
۶	ارتباطات در سازمان
۶	۱-۱ شبکه خصوصی مجازی سازمانی
۷	۱-۱-۱ تاریخچه پیدایش VPN
۸	۱-۱-۲ اهمیت استفاده از VPN و کاربردهای آن
۱۰	۱-۱-۳ انواع VPN
۱۲	۱-۱-۴ انواع پروتکل‌های VPN
۱۶	۱-۱-۵ آسیب‌پذیری VPN‌ها
۱۶	۱-۱-۶ تهدیدات و مخاطرات استفاده از VPN‌ها
۲۱	۱-۱-۷ توصیه‌های دفاعی و مقابله با تهدیدات استفاده از شبکه‌های VPN
۲۴	۱-۲ وای فای سازمانی
۲۴	۱-۲-۱ اهمیت و نوع استفاده از وای فای

۲۷	۱-۲-۲ آسیب‌پذیری‌ها استفاده از وای فای
۲۸	۱-۲-۳ تهدیدها و مخاطرات وای فای
۲۹	۱-۲-۴ توصیه‌های پدافندی و مکانیزم‌های دفاعی در استقرار شبکه‌های وای فای سازمانی
۳۷	فصل دوم:
۳۷	حریم خصوصی و به‌آتش
۳۷	۲-۱-۱ حریم خصوصی با نگاه سازمانی
۴۰	۲-۱-۲ آسیب‌پذیری‌های حریم خصوصی سازمانی
۴۱	۲-۱-۳ تهدیدات و مخاطرات حریم خصوصی سازمان
۴۲	۲-۱-۴ توصیه‌های پدافندی و مکانیزم‌های دفاعی برای حفاظت از حریم خصوصی سازمانی
۴۵	۲-۲-۱ به همراه آوردن تجهیزات شخصی (به آتش)
۴۷	۲-۲-۲ آسیب‌پذیری‌های به‌آتش
۴۸	۲-۲-۳ تهدیدات و مخاطرات به‌آتش
۴۹	۲-۲-۴ توصیه‌های پدافندی و مکانیزم‌های دفاعی در مواجهه با "به آتش"
۵۹	فصل سوم:
۵۹	شبکه اجتماعی، مهندسی اجتماعی و سرقت هویت
۵۹	۳-۱ امنیت شبکه‌های اجتماعی در سازمان‌ها
۶۱	۳-۱-۱ مخاطرات شبکه‌های اجتماعی
۶۳	۳-۱-۲ توصیه‌های دفاعی و پدافندی برای مقابله با چالش‌های شبکه‌های اجتماعی
۶۷	۳-۲ مهندسی اجتماعی

۶۸	۳-۲-۱ چرخه حملات مهندسی اجتماعی
۶۹	۳-۲-۲ مکانیزمهای مهندسی اجتماعی
۷۳	۳-۳ سرقت هویت
۷۴	۳-۳-۱ روشهای سرقت هویت
۷۵	۳-۳-۲ مخاطرات سرقت هویت
۷۶	۳-۴ توصیههای پدافندی و دفاعی در برابر مهندسی اجتماعی و سرقت هویت
۸۱	فصل چهارم:
۸۱	مدیریت هویت، دفاع لایه ای، زنجیره تأمین و فناوریهای نوین
۸۱	۴-۱ مدیریت هویت رایانه ای (رایاهویت)
۸۳	۴-۱-۱ هویت دیجیتال، احراز هویت و صدور مجوز
۸۵	۴-۱-۲ ایجاد هویت دیجیتال
۸۵	۴-۱-۳ فسخ هویت دیجیتال
۸۵	۴-۱-۴ اعتبارنامه ها
۸۶	۴-۱-۵ مدیریت رایاهویت
۸۸	۴-۱-۶ اهمیت مدیریت رایاهویت
۹۱	۴-۱-۷ مؤلفه های یک سیستم مدیریت رایاهویت
۹۴	۴-۱-۸ برخی چالش ها و نیازمندی های مدیریت رایاهویت
۱۰۲	۴-۲ دفاع لایه ای
	۴-۲-۱ اهمیت، جایگاه و رابطه چارچوب تاب آوری سایبری و رویکرد دفاع چند لایه ای عمیق
۱۰۲	۴-۲-۲ دفاع چندلایه ای عمیق در زیرساخت های حیاتی
۱۰۸	۴-۲-۳ اهداف کلان، اهداف عینی و پیاده سازی تکنیک های تاب آوری

- ۴-۲-۴ جمع‌بندی و نتیجه‌گیری ۱۱۰
- ۴-۳ زنجیره تأمین خدمات ۱۱۱
- ۴-۳-۱ تاریخچه زنجیره تأمین خدمات ۱۱۲
- ۴-۳-۲ امنیت در زنجیره تأمین ۱۱۲
- ۴-۳-۳ وقفه داخلی ۱۱۳
- ۴-۳-۴ وقفه تأمین‌کننده ۱۱۳
- ۴-۳-۵ وقفه مشتری ۱۱۳
- ۴-۳-۶ وقفه خارجی ۱۱۴
- ۴-۳-۷ مشکلات (بسیار از وقفه) در زنجیره تأمین ۱۱۴
- ۴-۳-۷-۱ اثر شلاق چرمی ۱۱۵
- ۴-۳-۷-۲ علل وقوع اثر شلاق چرمی ۱۱۵
- ۴-۳-۷-۳ اقداماتی برای مقابله با شلاق چرمی ۱۱۵
- ۴-۳-۷-۴ ذخیره فریبنده ۱۱۶
- ۴-۳-۸ راه حل‌های مشکلات زنجیره تأمین ۱۱۶
- ۴-۴ فناوری‌های نوین ۱۱۸
- ۴-۴-۱ فناوری داده‌های کلان ۱۱۸
- ۴-۴-۱-۱ چالش‌های موجود در فناوری داده‌های کلان ۱۱۹
- ۴-۴-۱-۲ چالش‌های ده‌گانه امنیت و حریم خصوصی در داده‌های کلان ۱۲۱
- ۴-۴-۲ فناوری رایانش ابری ۱۲۲
- ۴-۴-۲-۱ چالش‌های امنیتی موجود در فناوری رایانش ابر ۱۲۴
- ۴-۴-۳ فناوری اینترنت‌اشیاء ۱۲۸

مقدمه

کلیات دوره آموزشی مقدماتی پدافند سایبری

در نظام آموزش پدافند سایبری کشور، دوره‌های آموزشی کوتاه‌مدت و عرضی در پنج سطح با عناوین دوره‌های عمومی، مقدماتی، تخصصی فنی، تخصصی پیشرفته و مدیریت راهبردی پدافند سایبری طراحی شده است. کتاب حاضر، به عنوان مرجع دوره آموزشی مقدماتی پدافند سایبری، توسط مرکز پدافند سایبری کشور، به عنوان عالی‌ترین مرجع برگزاری دوره‌های آموزش عرضی و کوتاه‌مدت پدافند سایبری در کشور، تهیه شده است. شکل (۱)، سطوح پنج‌گانه‌ی نظام آموزشی عرضی و کوتاه‌مدت پدافند سایبری و جایگاه دوره آموزشی عمومی پدافند سایبری در این نظام را نمایش می‌دهد.



شکل (۱): سطوح نظام آموزشی عرضی و کوتاه‌مدت پدافند سایبری و جایگاه دوره آموزشی مقدماتی

ویژگی‌های کلی دوره آموزشی مقدماتی پدافند سایبری، عبارتند از :

جایگاه : دوره آموزشی مقدماتی پدافند سایبری، مطابق شکل (۱)، به عنوان یکی از ۵ دوره‌ی پیش‌بینی شده در نظام آموزشی پدافند سایبری کشور و دومین سطح از دوره‌های آموزشی عرضی و کوتاه‌مدت پدافند سایبری است.

اهداف : این دوره آموزشی با هدف دستیابی به درک و فهم از موضوعات حوزه پدافند سایبری و واکنش مستقل نسبت به این موضوعات طراحی شده است. این دوره موجب ایجاد درک و فهم موضوعات در حیطه‌ی شناختی، توانایی انجام واکنش در حیطه‌ی عاطفی و توانایی اجرای مستقل اقدامات در حیطه‌ی روانی-حرکتی می‌شود. آموزش‌های پیش‌بینی شده در این دوره، موجب خواهند شد تا فراگیران، ضمن به‌دست آوردن درک و فهم نسبت به موضوعات مرتبط با پدافند سایبری، توانایی انجام واکنش مستقل را به‌دست آورده و رأساً به انجام اقداماتی که برای دفاع در مقابل هرگونه تجاوز سایبری باید انجام گیرد، مبادرت ورزند.

مدت : مدت زمان برگزاری این دوره آموزشی، ۳۰ ساعت پیش‌بینی شده است و فراگیر در صورت قبولی در آزمون انتهای این دوره، گواهی قبولی دریافت خواهد نمود. به‌منظور تصدی هر یک از مسئولیت‌های پیش‌بینی شده در نظام پدافند سایبری کشور، دریافت این گواهی، الزامی خواهد بود.

فراگیران (مخاطبین) : دوره آموزشی مقدماتی پدافند سایبری، یکی از دوره‌های آموزشی الزامی پیش‌بینی شده برای آن دسته از پرسنل دستگاه‌های دولتی و مجموعه‌های غیردولتی متولی زیرساخت‌های حیاتی کشور و عرضه‌کنندگان خدمات سایبری است که در بخش‌ها یا واحدهای فناوری اطلاعات، شبکه، مرکز داده، امنیت و پدافند فعالیت دارند.

ویژگی‌های فراگیر : فراگیران این دوره آموزشی، علاوه بر برخورداری از ویژگی‌های شغلی مندرج در بخش مخاطبین، باید از شرایط ذیل نیز به صورت توانمند برخوردار باشند :

- مدرک تحصیلی کارشناسی یا بالاتر
 - تخصص در حوزه‌های مرتبط با فضای سایبر، امنیت و پدافند سایبری
 - تجربه حداقلی در راه‌اندازی، تنظیم و مدیریت زیرساخت، خدمات و کاربردهای سایبری
- تشخیص برخورداری از ویژگی‌های فوق، بر عهده مرکز پدافند سایبری کشور است.

برگزارکننده : دوره آموزشی مقدماتی پدافند سایبری، قابلیت ارائه توسط کلیه مدرسین مورد تأیید معاونت آموزشی و پژوهشی مرکز پدافند سایبری کشور را دارد و به صورت دوره‌ای، توسط این مرکز نیز برگزار می‌شود.

پیش‌نیاز : فراگیران این دوره آموزشی، باید دوره‌ی آموزش عمومی پدافند سایبری را با موفقیت گذرانده و گواهی این دوره را اخذ نموده باشند.