پی‌جویی جرایم رایانه‌ای

مؤلف: رضا پرویزی

پرویزی، رضا، ۱۳۴۶ –
پی‌جویی جرایم رایانه‌ای / مؤلف رضا پرویزی؛ ویراستار علیرضا غلامی؛ [برای معاونت آموزش دانشگاه علوم انتظامی، اداره کل تدوین متون آموزشی]. – – تهران: جهان جام جم، ۱۳۸۴.
۲۲۰ ص. مصور، جدول، نمودار. – – (معاونت آموزش دانشگاه علوم انتظامی ناجا، اداره کل تدوین متون آموزشی؛ [برای] ۳۴)

ISBN: 964-8625-57-3

فهرستنویسی براساس اطلاعات فیپا.
۱. علوم نظامی – – ایران – – دستنامه‌های افسران. ۲.نیروی انتظامی جمهوری اسلامی ایران. ۳.جرایم رایانه‌ای – – پی‌جویی. ۴.جرایم رایانه‌ای. الف.دانشگاه علوم انتظامی ناجا، اداره کل تدوین متون آموزشی. ب.عنوان ج.فروست. ۳۴.
LGR ۹۹۶/د۲ ۳۷۸/۵۵
کتابخانه ملی ایران ۸۴-۲۵۸۷۱م

پی‌جویی جرایم رایانه‌ای
مؤلف: رضا پرویزی
ویراستار: علیرضا غلامی
مدیر اجرایی: محمدرضا نادرپور
صفحه‌آرا: نگین صارمی
طراح جلد: محمد خدایی
لیتوگرافی: بهنور پرداز
چاپ: نگرش
نوبت چاپ: اول
شمارگان: ۳۰۰۰ جلد
سال انتشار: ۱۳۸٤
قیمت: ۱۸۰۰۰ ریال
ناشر: مؤسسه انتشاراتی جهان جام جم
نشانی: تهران ـ خ جنت‌آباد شمالی ـ خ گلزار غربی ـ کوچه شهید محسنی بعد ـ پلاک ۱۳
تلفکس: ٤٤٨٢٩٢٣١

پیشگفتار

دانشگاه علوم انتظامی به عنوان مرکز تربیت افسران مؤمن، متعهد و متخصص، رسالت عظیمی در تأمین کارکنان مورد نیاز ناجا و ارتقاء علمی آنان در طول خدمت مقدس را برعهده دارد.

تولید و انتشار علوم پلیسی، مکتوب و مستند نمودن تجارب و یافته‌های علمی و تجربی نیز یکی دیگر از رسالت‌های این دانشگاه محسوب می‌شود.

در راستای مأموریتهای یاد شده، تألیف کتاب‌های علمی آموزشی توسط اساتید و صاحب‌نظران در برنامه‌های جاری معاونت آموزش دانشگاه گنجانده شده است تا در این رهگذر انتقال دانش به دانشجویان، فراگیران و سایر علاقه‌مندان روند مطلوب‌تری داشته باشند.

امیدواریم با تداوم روند موجود و انتشار متون جدید، بتوانیم ضمن انجام رسالت و مأموریتهای متصوره به ارتقاء سطح علمی و مهارتی کارکنان ناجا و در نهایت ارتقاء کمی و کیفی نیروی انتظامی جمهوری اسلامی ایران کمک نموده و رضایت خداوند متعال را کسب نماییم.

بدین‌وسیله از زحمات کلیه عزیزانی که در این خصوص ما را یاری نموده و یا می‌نمایند، به ویژه اساتید و مؤلفان گرامی، همکاران آموزشی و گروه‌های علمی تقدیر و تشکر می‌نمایم.

معاون آموزشی دانشگاه علوم انتظامی
سرهنگ پاسدار مهندس علی‌اصغر نیکنام

مقدمه

تولید منابع آموزشی غنی‌ترین بخش فرآیند برنامه‌ریزی آموزشی در دانشگاه‌ها و مؤسسه‌های علمی و آموزشی است و دانشگاه علوم انتظامی نیز به عنوان مرکز ثقل دانش، بینش و مهارت در علوم پلیسی، از این قائده مستثنی نیست. بنابراین، با توجه به توسعه و گسترش فناوری در علوم پلیسی و انتظامی، لزوم دگرگونی اساسی در نظام آموزشی دانشگاه علوم انتظامی بیش از پیش احساس گردید و به همین منظور تولید منابع و متون آموزشی به عنوان بخشی از نظام آموزشی دانشگاه علوم انتظامی در دستور کار قرار گرفت بطوری که در چند سال اخیر گام‌هایی در جهت تولید منابع و متون آموزشی در حوزه‌های تخصصی علوم پلیسی برداشته شده است که هنوز مراحل اولیه را طی می‌کند. در این مرحله دانش، بینش، مهارتها و ارزشهای علوم پلیسی تدوین، تنظیم و به رشته تحریر درآمده است تا به لحاظ تئوریک و نظری علوم پلیسی و انتظامی را پوشش دهد. در این راستا، اداره کل تدوین متون آموزشی معاونت آموزش، با تدوین، تألیف و ترجمه متون آموزشی، امکان تحقق اهداف ذیل را در نظام آموزشی دانشگاه فراهم می‌سازد:

الف) بالابردن توان شناختی و علمی دانشجویان دانشگاه علوم انتظامی

مهم‌ترین هدف تولید متون آموزشی بالابردن شناخت، بینش و مهارت دانشجویان دانشگاه علوم انتظامی است. این شناخت را می‌توان به چند دسته تقسیم کرد:

۱- آموختن و یادآوری دانش و اطلاعات تخصصی علوم پلیسی؛
۲- درک و فهم تخصصی علوم انتظامی؛
۳- به کار بردن اصول، قوانین و روشهای خاص علوم انتظامی؛
۴- تجزیه و تحلیل و نقد مسائل، عوامل و پدیده‌های انتظامی؛
۵- تولید، ارتقاء و اصلاح علوم پلیسی در کشور؛
۶- به‌کارگیری روشها و تکنیکهای علوم پلیسی گذشته و حال

ب) بالا بردن مشارکت فردی و جمعی دانشجویان

با تدوین منابع می‌توان ارزشها، علایق و نگرش‌های دانشجویان پلیس را بالا برد و با بالا بردن آن می‌توان:

۱- امکان خوب گوش دادن را برای دانشجویان فراهم آورد.
۲- امکان مشارکت فردی و جمعی را در حوزه‌های مسائل اجتماعی در دانشجویان مهیا نمود.
۳- دانش، بینش و مهارت را برای دانشجویان مهیا کرد تا بتوانند به اتکای آن از عملکرد و توان علمی و تخصصی خود در حوزه فعالیتهای انتظامی دفاع نمایند.
۴- امکان کنترل رفتار و گفتار را برای دانشجویان مهیا ساخته تا نظام آموزشی و منش انتظامی را پیوسته به صورت نظام ثابت ذهنی در خود به وجود آورند.

ج) بالا بردن تواناییهای مهارتی دانشجویان علوم انتظامی

تسلط بر مهارتهای علمی، تجربی، سنتی و عمومی پلیسی یکی از اهدافی است که با تولید و تدوین منابع آموزشی نهادینه خواهد شد. با ایجاد این منابع سازماندهی شده می‌توان:

۱- امکان مشاهده دقیق و هدفمند وقایع و پدیده‌های پلیسی را برای دانشجویان مهیا نمود.

۲- پیروی و تقلید از قوانین، روشها و ضوابط عمومی و علمی علوم پلیسی را برای دانشجویان فراهم کرد.

۳- دقت و سرعت عمل را در دانشجویان بالا برد.

۴- رعایت نظم و انضباط در انجام عملیات انتظامی را برای دانشجویان مهیا کرد.

۵- تسلط کامل بر وظایف اجرایی و شغلی برای دانشجویان را به وجود آورد.

د) شناخت ارزشهای مشترک جامعه و پلیس

با تولید منابع و متون آموزشی از دانشجویان پلیس توقع آن می‌رود که شناخت دقیقی از ارزشها، علایق، گرایشها، باورها و عقاید جامعه خود داشته و آنها را در انجام وظایف بکار گیرند، این شناخت می‌تواند شامل موارد ذیل باشد:

۱- شناخت ارزشهای مشترک عمومی جامعه و پلیس؛

۲- شناخت حقوق سازمانی و انسانی شهروندان از سوی پلیس؛

۳- ایجاد حس وفاداری به کشور، نظام و پلیس؛

۴- احساس احترام و تعلق خاطر نسبت به آرمانها، میراث، تاریخ، نهادهای اجتماعی، ارزشهای اسلامی و انسانی.

تغییر و ارتقای نظام تعلیم و تربیت در دانشگاه علوم انتظامی مسئله‌ای است که قابل شک و خدشه نیست و دانشگاه باید در این برهه از زمان با تولید، تدوین و تألیف منابع و متون آموزشی گام بردارد و در این راستا دانشگاه علوم انتظامی با ایجاد تشکیلات و مدیریت مستقل تصمیم به تولید منابع و محتوای آموزشی گرفته که متن حاضر حاصل زحمات یکی از تولید کنندگان عرصه تولید، و تدوین منابع و متون آموزشی است. امید است کارشناسان، محققان و مسئولان؛ منابع تولید شده را مورد نقد و اصلاح قرارداده و نقاط خلاء را به اطلاع نویسندگان گروه علمی مربوط و معاونت آموزش دانشگاه برسانند تا در جهت پرکردن خلا، موجود در علوم پلیسی و انتظامی اقدام لازم صورت پذیرد.

در پایان توفیق روز افزون نویسندگان، مترجمان و تلاشگران عرصه تولید متون آموزشی دانشگاه علوم انتظامی را از خداوند متعال خواستارم.

مسئول طرح تدوین متون آموزشی دانشگاه علوم انتظامی

محمدرضا نادرپور

فهرست مطالب

عنوان — صفحه

فهرست مطالب

عنوان — صفحه

فهرست مطالب

عنوان — صفحه

مقدمه مؤلف

دنیایی که امروزه در آن زندگی می‌کنیم، با پا گذاشتن به هزارهٔ سوم میلادی تحولات بسیار سریع و شگفت‌آوری را در تمام شئون خود تجربه می‌کند. بدون شک یکی از عوامل مهم و عمدهٔ این تحولات فناوری اطلاعات می‌باشد.

ویژگی برجسته فناوری اطلاعات، تأثیری است که بر تکامل فناوری ارتباطات راه دور گذاشته و خواهد گذاشت. ارتباطات کلاسیک هم چون انتقال صدای انسان، جای خود را به مبادله مقادیر وسیعی از داده‌ها، صوت، متن، موزیک، تصاویر ثابت و متحرک داده است. این تبادل و تکامل نه تنها بین انسانها بلکه ما بین انسانها و رایانه‌ها و همچنین بین خود رایانه‌ها نیز وجود دارد.

در نتیجه این تحولات، جامعه‌ای مجازی با آثار واقعی پدید آمده است. جامعه‌ای که تمامی فعالیتهای اجتماعی، اقتصادی، سیاسی و هنری را به طور شگفت‌انگیزی تحت تأثیر قرار داده و مبادلات تجاری، تعامل بین حاکمیت و شهروندان، توزیع اطلاعات علمی، هنری، آموزشی و خلاصه همه نهادهای جدید عصر صنعتی از آن متأثر گشته است. تحولات جدید موجب غیر مادی شدن واسط انتقال اطلاعات شده که در نتیجه باعث:

۱- حذف حضور فیزیکی افراد؛

۲-حذف واسطهای مادی انتقال اطلاعات مثل کاغذ، پلاستیک و ... ؛

۳-حذف تقریبی مدت انتقال اطلاعات و نهایتاً؛

٤-پیدایش محیط مجازی با ویژگیهای خاص خود می‌شود.

و ارزشهای جدید و آسیب‌پذیری مانند:

۱-**محرمانه ماندن اطلاعات:** حفظ اطلاعات در برابر افشای غیر مجاز آنها (*confidentiality*).[۱] ؛

۲-**تمامیت اطلاعات:** حفظ صحت اطلاعات در برابر تغییر یا آسیب به آنها *(integrity)*[۲] ؛

---

۱ -این عامل باعث می‌شود تا کسانی که هیچگونه مجوزی ندارند یا اجازهٔ آنها به اندازه‌ای نیست که بتوانند از آن اطلاعات استفاده کنند، از دسترسی به آن اطلاعات منع شوند. در حقیقت تعرض به این عامل، تجاوز به حقوق مشروع دیگران مبنی بر حفظ اطلاعات شخصی و خصوصی آنها می‌باشد. از آنجا که هتک سیستم دیگری و ورود به آن سر منشاء تمامی راههای کسب نامشروع اطلاعات می‌باشد، بسیاری بر این عقیده‌اند که تعرض به این عامل، اصلی‌ترین و مهمترین جرم در گروه جرایم رایانه‌ای محسوب می‌شود. تعرض به این عامل عموما زمانی به وقوع می‌پیوندد که یک متعرض (هکر) اطلاعات کاربر یا آنچه را که متعلق به او می‌باشد را بدون اجازه مشاهده یا کپی نماید.

۲ -این اطمینان را بوجود می‌آورد که هیچ کس بدون داشتن مجوز حق ندارد به اطلاعات دست یافته و تغییری در آنها بوجود آورد. بنابراین هرگونه مزاحمت و خسارت یا تغییر در اطلاعات ثبت شده در رایانه یا قسمتهای دیگر آن، بدون مجوز قانونی موجبات تعدی و تجاوز به این عامل مهم در تبادل اطلاعات الکترونیکی را فراهم می‌آورد. بسیاری از تعرضات عمدی که توسط هکرها صورت می‌گیرد مانند وارد کردن ویروسهای رایانه‌ای از قبیل *worms* و *trojan horses* در این رده جای می‌گیرند. این امر نه تنها از جانب کسانی که منافع اقتصادی را دنبال می‌کنند به وقوع می‌پیوندد، بلکه آنهایی که قصد مقابله به مثل (انتقام)، اغراض سیاسی، تروریسم یا صرفا قصد رقابت داشته باشند نیز مرتکب می‌شوند.

۳- **موجودیت اطلاعات و خدمات:** حفظ عملکرد مفید سیستم و در دسترس نگهداشتن اطلاعات (***availability***)[۳] را برای جامعه و افراد ایجاد می‌کند که نیازمند حمایت جدی می‌باشند.

فناوری اطلاعات با تمام قابلیتها و پیچیدگیهایش به شدت در مقابل تهدیدات آسیب‌پذیر است. بدین ترتیب که فناوری اطلاعات ارتکاب اعمال مجرمانه‌ای را که پیش از این به هیچ وجه امکانپذیر نبود فراهم نموده است. سیستمهای رایانه‌ای فرصتهایی تازه و بسیار پیشرفته برای قانون شکنی در اختیار مجرمین می‌گذارند و توان بالقوه ارتکاب گونه‌های مرسوم جرایم را به شیوه‌هایی غیر مرسوم به وجود می‌آورند. تهدیدات علیه جامعه اطلاعاتی را جرم رایانه‌ای یا جرایم مرتبط با رایانه می‌نامند.

آسیب‌پذیری امروزی جامعه اطلاعاتی از جانب جرم رایانه‌ای تا کنون به درستی و بطور کامل مورد تجزیه و تحلیل قرار نگرفته است. تجارت و بازرگانی، امور اداری و در مجموع جامعه ما بر کارآیی و امنیت بسیار بالای فناوری مدرن اطلاعات

---

۳ - بیانگر این مطلب است که تحصیل اطلاعات و برنامه‌های مرتبط با آن از طرف یک کاربر، آن هم زمانی که بدان احتیاج دارد، نشانگر مفید و کاربردی بودن آنها است. نقض این عامل زمانی بوقوع می‌پیوندد که کاربر دارای مجوز برای مدتی از ارتباط مستمر و قابل اتکاء و اطمینان خود با سیستم و مرکز مورد نظر خود باز می‌ماند و از آن منع می‌شود. نمونهٔ بارز و معمولی که در این رابطه به وقوع می‌پیوندد ***denial of service attack*** می‌باشد. عملی است که به موجب آن از فعالیت عضو انجمن سیستمهای اطلاعاتی ***(AIS)*** مطابق با اهدافی که برای آن پیش بینی شده، جلوگیری می‌کند. این عمل ممکن است شامل جلوگیری از ارائه سرویس یا فرآیندهای محدود شده‌ای به سیستم میزبان شود. با این حال این اصطلاح اغلب دلالت بر فعالیتهایی علیه یک میزبان یا یک گروه از آنها دارد که باعث غیرفعال شدن آنها در زمینهٔ ارائه خدمات به کاربران خصوصاً در ارتباط با شبکه می‌باشد.

استوار است. مثلاً در جامعه تجاری بسیاری از معاملات پولی بوسیله رایانه‌ها و در غالب سپرده گذاری انجام می‌شود. در تجارت الکترونیک برای انجام معاملات پولی در شبکه‌های رایانه‌ای به سیستمهای امن نیاز می‌باشد. کل تولید یک شرکت به عملکرد سیستم پردازش داده آن وابسته است. بسیاری از تجار، اطلاعات و اسرار تجاری با ارزش خودشان را بصورت الکترونیکی ذخیره می‌کنند. سیستمهای کنترل هوایی، دریایی و فضایی و همینطور پزشکی تا اندازه زیادی متکی بر سیستمهای رایانه‌ای هستند. رایانه‌ها و اینترنت نقش کلیدی در آموزش و تعلیم و تربیت خردسالان دارند. شبکه‌های رایانه‌ای بین‌المللی به منزله سلسله اعصاب اقتصاد، بخش عمومی و جامعه هستند. امنیت این سیستمهای رایانه‌ای و ارتباطی و مراقبت از آنها در مقابل جرایم رایانه‌ای از اهمیت ویژه‌ای برخوردار است.

در عوض جرم رایانه‌ای به تهدیدی مهم بر علیه جامعه اطلاعاتی امروز تبدیل شده است. رخنه فناوری اطلاعات به تمامی ابعاد زندگی و همچنین تعامل و ارتباط میان رایانه‌ها با شبکه‌های رایانه‌ای بین‌المللی پدیده جرم رایانه‌ای را متنوع‌تر و خطرناکتر ساخته و بعد بین‌المللی به آن بخشیده است. بررسی و تجزیه و تحلیل جنبه‌های مختلف جزایی جرم رایانه‌ای مشخص خواهد ساخت که رایانه‌های مدرن و شبکه‌های ارتباطی، دارای صفات و خصوصیاتی هستند که فرصتی بسیار مناسب برای مجرمین پدید می‌آورد و مشکلات زیادی را فراروی بزه‌دیدگان بالقوه و پلیس قرار می‌دهد (مثل مسائل پیچیده امنیتی، سیستمهای سخت‌افزاری و نرم‌افزاری متنوع، ناآگاهی کاربران، اختفاء، رمزنگاری و تحرک بین‌المللی) گروههای سازمان یافته جنایی فعال در سراسر جهان، جاسوسان صنعتی حرفه‌ای و سازمانهای اطلاعاتی این

امکانات و ابعاد جدید جرم رایانه‌ای را در یافته‌اند. با این وجود بسیاری از کشورها، تجار و کاربران عادی از حملات واقعه یا حملاتی که می‌تواند بر علیه آنها رخ دهد بی اطلاع‌اند. بنابراین، دولتمردان، تجار و کاربران باید بدانند که حمایت و حفاظت در مقابل جرم رایانه‌ای حائز اهمیت بسیاری است. آنان باید از ابعاد مختلف تهدیدات جرم رایانه‌ای و واکنشهایی که می‌توان داشت مطلع گردند.

رضا پرویزی