متن‌کاوی جرایم سایبری در فضای مجازی

مؤلف: بهزاد لک

(عضو هیأت علمی دانشگاه علوم انتظامی امین)

www.ketab.ir

۱۳۹۴

معاونت پژوهش دانشگاه علوم انتظامی امین

عنوان: متن‌کاوی جرایم سایبری در فضای مجازی

مؤلف: بهزاد لک

چاپ اول : ۱۳۹۴

شمارگان: ۵۰۰ جلد

آماده‌سازی و چاپ: کهن

نشانی: تهران، ابتدای بزرگراه شهید خرازی- خیابان شهید جدی اردبیلی- دانشگاه علوم انتظامی امین

تلفن: ۴۸۹۳۱۲۹۳

سرشناسه: لک، بهزاد، ۱۳۵۶ -

عنوان و نام پدیدآور: متن‌کاوی جرایم سایبری در فضای مجازی/مولف بهزاد لک.

مشخصات نشر: تهران : دانشگاه علوم انتظامی ناجا، معاونت پژوهش، ۱۳۹۲.

مشخصات ظاهری: ۳۰۶ ص.

شابک: 978-600-6647-85-2

وضعیت فهرست نویسی: فیپا

موضوع: جرایم کامپیوتری

موضوع: جرایم کامپیوتری -- پی‌جویی

شناسه افزوده: دانشگاه علوم انتظامی ناجا. معاونت پژوهش

رده بندی کنگره: HV۱۳۹۲۶۷۷۳ ۲م۸ل/

رده بندی دیویی: ۱۶۸/۳۶۴

شماره کتابشناسی ملی: ۳۳۷۵۸۷۲

www.ketab.ir

سخن ناشر

کسب علم و دانش و تلاش برای بهره‌گیری از علوم جدید و بومی‌سازی آن برای رفع نیازهای علمی، فرهنگی، اجتماعی و اقتصادی به منظور اعتلای اقتدار امت اسلامی از توصیه‌های مهم اسلام است. علوم پلیسی که همگام با پیشرفت بسیاری از علوم محض و تلفیق آنها با یکدیگر، روز به روز نو می‌شود و مرزهایی تازه از دانش می‌سازد، از جمله علومی است که درخت آن در کشورمان در حال رشد و نمو و ثمر دادن است.

تالیف آثار علمی برجسته و معتبر و اشاعه مفاهیم آنها از جمله رهیافت‌های کارآمد و اثربخش است که می‌توان در سایهٔ آن بستری مناسب برای بهره گیری از تجربه های ارزشمند و دانش بومی خبرگان و کارشناسان علوم پلیسی در کشورمان ساخت. بدیهی است اندیشمندان، خبرگان و کارشناسان امور پلیسی داخلی می توانند با تلفیق همگن تجربه‌های خود با علوم و تجربه‌های کارشناسان علوم پلیسی دیگر کشورها باعث پیشبرد دانش پلیسی در کشور شوند. امید است با نشر آثار تالیفی از این دست، گامی هرچند کوچک در این مسیر بلند برداریم و نویسندگان، محققان، کارشناسان و استادان را برانگیزانیم تا تجربه‌ها و توان علمی خود را متبلور کنند و اشاعه دهند.

معاونت پژوهش دانشگاه علوم انتظامی امین

www.ketab.ir

فهرست مطالب

www.ketab.ir

www.ketab.ir

www.ketab.ir

www.ketab.ir

www.ketab.ir

www.ketab.ir

پیش‌گفتار

پیشگیری از جرم همواره یکی از موضوعات اساسی و مهم در زندگی بشری بوده که در طول تاریخ به شیوه‌های مختلف اعمال شده است. با توجه به گسترش فناوری‌های اطلاعات و ارتباطات و به تبع آن توسعهٔ سیستم‌های اطلاعاتی در سازمان‌ها، روش‌ها و الگوریتم‌های داده‌کاوی نقش مؤثری در فرمولیزه داده‌ها و شناسایی الگوهای جرم ایفا می‌کند، تا بدین طریق پلیس بتواند، قبل از وقوع جرایم، از آنها پیشگیری نماید.

امروزه بیشتر از ۸۰ درصد از دانش افراد به‌صورت متن، مستندات و دیگر صور رسانه‌ای نظیر تصویر و صدا نگهداری می‌شود. اگر از منظر علوم رایانه‌ای به این مستندات نگاه شود، همه آنها به طبیعتی غیر ساخت‌یافته وابسته‌اند. یک فرد برای دریافت دانش از اطلاعات موجود در یک متن، ابتدا باید آن را درک و سپس آن را پردازش کند تا بفهمد چه معنی و مفاهیمی در آن نهفته است، چه ارتباطی میان مفاهیم وجود دارد و از میان این مفاهیم کدام جدید است و کدام قدیمی. یکی از کاربردهای مهم متن کاوی، استفاده از الگوریتم‌های متن‌کاوی است، از آنجا که این فناوری جوان و در حال رشد است؛ به کمک آن می‌توان دانش موجود در متون غیر ساخت‌یافته بهره برد.

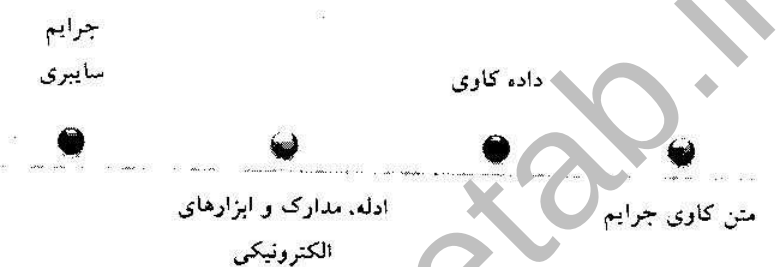
از جمله دغدغه‌های پلیس در عصر حاضر شناسایی، پیشگیری و مقابله با جرایم در فضای سایبر است که استفاده از روش‌های سنتی برای این منظور کاربرد چندانی نخواهد داشت. با توجه به اینکه کاربردهای متن‌کاوی بسیار زیاد بوده و تاکنون کتابی در زمینه کاربرد این‌گونه روش‌ها با رویکرد تشخیص جرایم فضای مجازی تدوین نشده است، اهمیت و ضرورت تالیف کتاب حاضر بیشتر احساس می‌شود.

این تألیف بر اساس تجارب چند ساله تحقیق و پژوهش مؤلف در حوزه فناوری اطلاعات تدوین شده است، تا دانشجویان و کارشناسان با روش‌های نوین استخراج اطلاعات از متون و ادلهٔ دیجیتال فضای سایبر آشنا شوند. به‌طور قطع نظرات اصلاحی اساتید ارجمند و متخصصان گرامی می‌تواند در تکمیل و پربارشدن این کتاب تأثیرگذار باشد.

www.ketab.ir

مقدمه مؤلف

با پیدایش رایانه و رشد سریع فناوری اطلاعات، جرایم نیز وارد پاردایم جدیدی شده است؛ تا جایی که امروزه تعدد جرایم در فضای مجازی قابل مقایسه با جرایم سنتی نیست. یکی از دغدغه‌هایی که پلیس با آن مواجه است، عدم دسترسی به شرایط مکانی و زمانی مجرمان در این فضا است؛ زیرا روش‌های شناسایی، پیشگیری و مقابله با جرایم سایبری نیازمند استفاده از روش‌های نوین است. از این‌رو نقشه راه در نظر گرفته شده برای این کتاب مطابق شکل زیر می‌باشد:



همان‌طور که مشخص است، به‌منظور بهره‌مندی مخاطب از محتوای کتاب و نیز برقراری ارتباط منطقی بین مفاهیم مرتبط با روش‌های نوین شناسایی و کشف جرایم در فضای مجازی، چهار فصل برای این کتاب در نظر گرفته شده است:

فصل اول، ضمن معرفی فضای مجازی، مفاهیمی از جمله انواع جرایم سایبری، تروریسم سایبر، پلیس سایبر، امنیت در فضای سایبر، آسیب‌ها و تهدیدات فضای سایبر، .... مطرح می‌گردد تا مخاطب دید عمیق‌تری نسبت به این فضا و مخاطرات آن پیدا کند.

در فصل دوم، از آنجا که در این فضا، اطلاعات به شکل الکترونیکی ثبت می‌شوند؛ لذا لازم است ابعاد مختلف ادله، مدارک و ابزارهای الکترونیکی تشریح شود تا مخاطب بتواند به‌طور منطقی تفاوت‌های اسناد سنتی و الکترونیکی را درک کند؛ از این‌رو در این فصل پس از بررسی خصوصیات و ویژگی‌های ادله و ابزار الکترونیکی؛ همچنین اهمیت استفاده از آنها در این فضا، نقش‌های اجراشده توسط ابزارهای دیجیتال مطرح می‌گردد تا از آن طریق بتوان روش‌های جمع‌آوری و تجزیه‌وتحلیل شواهد الکترونیکی در فضای مجازی را بیان کرد. در پایان این فصل به دلیل اهمیت موضوع و اینکه زیربنای

www.ketab.ir

روش‌های نوین تحلیل جرایم در فضای مجازی ادله‌های الکترونیکی است؛ لذا مزایا و چالش‌های آینده در جمع‌آوری ادله الکترونیکی؛ همچنین مثال‌هایی از نقش ابزار الکترونیکی در تشکیل پرونده جنایی مطرح می‌گردد.

فصل سوم، به معرفی مفهوم داده‌کاوی و الگوریتم‌ها و روش‌های مختلف آن می‌پردازد. با توجه به اینکه در دو فصل قبل ادبیات لازم و ضروری داده‌کاوی مورد بحث و بررسی قرار گرفته است، در این فصل مخاطب می‌تواند اهمیت و ضرورت استفاده از روش‌های داده‌کاوی را در شناسایی و تحلیل جرایم درک کند؛ از این‌رو سعی شده تا کلیه مطالب مرتبط با حوزهٔ داده‌کاوی، بر اساس ساختار منظم و به شکل پیوسته بر اساس آخرین نظرها تدوین شود.

فصل چهارم، مربوط به یکی از روش‌ها و کاربردهای داده‌کاوی به نام متن‌کاوی است. با توجه به اینکه بیشتر ۸۰ درصد اطلاعات به‌صورت متن و غیر ساختاریافته است و با عنایت به اینکه ادله الکترونیکی به اشتراک گذاشته‌شده در فضای سایبر، حجم انبوهی از اطلاعات سازمان‌ها را تشکیل می‌دهد، استفاده از روش‌های استخراج اطلاعات در این فضا به‌منظور شناسایی جرایم احتمالی امری ضروری است که چنانچه سازمان پلیس برای بومی‌سازی این‌گونه روش‌ها در سامانه‌های جاری خود تصمیم مناسبی اتخاذ نکند، در آینده‌ای نه چندان دور حجم و اشکال مختلف جرایم به شکل غیر قابل باوری افزایش خواهد یافت که جبران آن، خسارات زیادی در پی خواهد داشت؛ لذا سعی شده است فرایند متن‌کاوی و شیوه‌های تشخیص و شناسایی جرایم به شکلی کاملاً کاربردی مطرح شود تا مخاطب با مطالعه این فصل یک دید علمی و تجربی نسبت به روش‌های متن‌کاوی جرایم در فضای مجازی پیدا کند.

بهزاد لک

سال ۱۳۹۴

www.ketab.ir