



متن کاوی جرایم سائیری در فضای مجازی

مؤلف: بهزاد نک

(عضو هیأت علمی دانشگاه علوم انتظامی)

۱۳۹۴



معاونت پژوهش دانشگاه علوم انتظامی امین

عنوان: متن کاوی 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: متن کاوی جرایم سایبری در فضای مجازی/مؤلف 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 -- پی جویی

شناسه افزوده: دانشگاه علوم انتظامی ناجا. معاونت پژوهش

رده بندی کنگره: HV ۱۳۹۲۶۷۷۳ م۲/۸

رده بندی دیویی: ۱۶۸/۳۶۴

شماره کتابشناسی ملی: ۳۳۷۵۸۷۲

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 علمی 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 می‌تواند سایه آن بستری مناسب برای بهره‌گیری از تجربه‌های ارزشمند و دانش بومی خبیران و کارشناسان علوم پلیسی در کشورمان ساخت. بدیهی است اندیشمندان، خبرگان و کارشناسان امور پلیسی داخلی می‌توانند با تلفیق همگن تجربه‌های خود با علوم و تجربه‌های کارشناسان علوم پلیسی دیگر کشورها باعث پیشبرد دانش پلیسی در کشور شوند. امید است با نشاندن حلقه‌ای از زنجیره‌ای از 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

فهرست مطالب

عنوان	پیش گفتار	مقدمه مؤلف	صفحه
فصل اول - جرایم سایبری			
۱. مقدمه	۲		
۲. عصر اطلاعات و عصر مجازی	۳		
۳. جرم و مجرمان سایبری	۵		
الف) پیشینه	۵		
ب) از قربانی تا آگاهی و اطلاعاتی	۵		
ج) انقلاب صنعتی و انقلاب داده ها	۷		
د) فضای سایبر	۸		
هـ) جرم سایبری	۱۰		
۴. انواع جرایم سایبری	۱۳		
۵. تروریسم سایبر	۲۲		
۶. پلیس سایبر	۲۸		
الف) ویژگی های پلیس سایبر	۲۹		
ب) تجربه سایر کشورها	۳۰		
ج) ملزومات پلیس سایبری	۳۱		
د) خدمات پلیس سایبری	۳۱		
۷. امنیت در فضای سایبر	۳۲		
الف) فناوری های امنیت اطلاعات	۳۴		
ب) راهکارها و اقدامات مؤثر بر امنیت فضای مجازی و اینترنت	۳۸		
۸. آسیب ها و تهدیدهای فضای سایبر	۴۱		
نتیجه گیری	۴۳		

فصل دوم- ادله، مدارک و ابزارهای الکترونیکی در تحقیقات جنایی ۴۵

۱. مقدمه ۴۶
۲. خصوصیات و ویژگی ادله الکترونیکی ۴۸
۳. پیشرفت‌های اساسی در مورد ادله و ابزارهای الکترونیکی ۴۹
۴. اهمیت و مزایای جمع‌آوری مدارک الکترونیکی و استفاده از شواهد الکترونیکی ۵۵
۵. ادله و ابزارهای الکترونیکی در جامعه ۵۷
۶. ادله و ابزار الکترونیکی ۵۹
- الف) روش یافتن ادله الکترونیکی ۶۰
- ب) ابزارهای الکترونیکی در سیستم‌های باز و بسته ۶۳
- ج) سیستم‌های بسته ۶۴
- د) سیستم‌های باز ۶۴
- هـ) شناسایی محل جرم ۶۶
۷. نقش‌های اجرا شده توسط ابزارهای دیجیتال ۶۷
- الف) شاهد، (مدارک) ۶۹
- ب) ابزار ۶۹
- ج) هم‌دست ۶۹
- د) قربانی ۷۰
- هـ) محافظ ۷۰
- و) نقش‌های تعیین‌کننده ۷۰
۸. روش‌های جمع‌آوری و تجزیه و تحلیل شواهد الکترونیکی ۷۱
۹. مزایا و چالش‌های آینده در جمع‌آوری ادله الکترونیکی ۷۳
۱۰. بیان مثال‌هایی از نقش ابزار الکترونیکی در تشکیل پرونده جنایی ۷۴
- الف) پرونده‌ها و مجرمان سایبری ۷۴
- ب) پرونده‌سازی برای نفوذی‌ها (داخلی‌ها) ۷۷
- ج) بکارگیری ادله و شواهد الکترونیکی در اثبات جرایم رایانه‌ای ۷۹

۸۱	 (د) کپی برداری غیر قانونی از DVD
۸۳	 (هـ) قتل
۸۴	 نتیجه گیری
۸۹	 فصل سوم- داده کاوی
۹۰	 ۱. مقدمه
۹۲	 ۲. سابقه داده کاوی
۹۹	 ۳. از داده ها تا تصمیم گیری ها
۹۹	 (الف) تکامل تأثیر گذاری داده ها
۱۰۲	 (ب) از داده ها تا تصمیم گیری ها
۱۰۴	 ج. مفهوم ذرات داده ها
۱۰۸	 ۴. فرایند داده کاوی
۱۱۱	 ۵. مدل داده کاوی کرسپ، CRISP-DM
۱۲۱	 ۶. کارکردها و وظایف داده کاوی
۱۲۱	 (الف) دسته بندی (طبقه بندی)
۱۲۶	 (ب) پیش بینی
۱۲۶	 (ج) تحلیل سری های زمانی
۱۲۶	 (د) رگرسیون
۱۲۷	 (هـ) کشف توالی
۱۲۷	 (و) قوانین با هم آیی
۱۳۰	 (ز) خلاصه سازی
۱۳۱	 (ح) خوشه بندی (گروه بندی)
۱۳۲	 ۷. نرم افزارهای داده کاوی
۱۳۹	 ۸. داده کاوی جرم
۱۴۱	 (الف) کاربرد داده کاوی در حوزه های کاربردی پلیس
۱۴۴	 (ب) تحلیل و کشف جرم با استفاده از روش های داده کاوی

۱۴۸	ج) روش‌های داده‌کاوی جرم
۱۵۰	۱) استخراج موجودیت (اطلاعات فردی)
۱۵۰	۲) شبکه‌های عصبی
۱۵۳	۳) خوشه‌بندی
۱۵۷	۴) قوانین با هم آبی یا کاوش قوانین پیوندی
۱۵۷	۵) کاوش الگوی ترتیبی
۱۵۷	۶) اساین انحراف
۱۵۸	۷) طایفه‌بندی
۱۵۸	۸) مقایسه گررسته‌ها
۱۵۸	۹) تحلیل شبکه اجتماعی
۱۵۹	د) چارچوب کاربردی داده‌کاوی در مدل‌سازی جرایم
۱۶۳	ه) ابزارهای موجود داده‌کاری جرم
۱۶۸	و) مطالعه موردی کوپلینگ
۱۷۵	۹. مثال‌های داده‌کاوی در حوزه تشخیص ردپای جرایم
۱۷۵	الف) داده‌کاوی و بررسی صحنه جرم
۱۷۷	ب) داده‌کاوی و جرایم خشونت‌آمیز
۱۷۷	ج) داده‌کاوی و تحلیل حوادث ویژه
۱۷۸	د) داده‌کاوی و حوادث تیراندازی
۱۷۹	ه) داده‌کاوی و دوباره قربانی شدن
۱۸۰	و) داده‌کاوی و سرقت از منازل
۱۸۱	ز) داده‌کاوی و حملات تروریستی
۱۸۲	ح) داده‌کاوی و جرایم مجازی
۱۸۳	ط) داده‌کاوی و سرقت‌های مسلحانه
۱۸۳	نتیجه‌گیری
۱۸۷	فصل چهارم- متن کاوی جرایم

۱۸۸	۱. مقدمه
۱۹۱	۲. وب کاوی
۱۹۶	۳. متن کاوی
۲۰۱	۴. متن کاوی در مقایسه با داده کاوی
۲۰۳	۵. کاربردهای متن کاوی
۲۰۸	۶. ساختاردهی به متون
۲۰۸	الف) کشکول کلمه
۲۰۸	ب) پردازش زبان طبیعی
۲۰۹	ج) چالش‌های پیاده‌سازی پردازش زبان طبیعی (NLP)
۲۱۲	۷. فرایند متن کاوی
۲۱۴	الف) مرحله اول: آماده‌سازی متن
۲۱۵	ب) مرحله دوم: پردازش متن
۲۱۷	ج) مرحله سوم: تحلیل متن
۲۱۸	۸. معماری عمومی سامانه‌های متن کاوی
۲۱۹	الف) وظایف پردازشی
۲۲۰	ب) عملیات‌های هسته کاوی
۲۲۰	ج) اجزاهای لایه ارائه و قابلیت‌های مرور
۲۲۰	د) روش‌های پالایش
۲۲۵	۹. زبان‌های پرس و جوی متن کاوی
۲۲۹	۱۰. ابزارهای متن کاوی
۲۳۱	۱۱. متن کاوی و شیوه‌های تشخیص و جلوگیری از جرم
۲۳۶	الف) استخراج اطلاعات جنایی
۲۳۷	ب) دسته‌بندی اطلاعات جنایی
۲۳۸	ج) کاربرد جنایی از شبکه‌های عصبی
۲۳۸	د) استخراج قانون انجمن در اطلاعات جنایی

۲۳۹	 (ه) شیوه متن کاوی جرایم
۲۴۴	 (و) نظارت کردن با استفاده از چارچوب سامانه هوشمند مبتنی بر عامل
۲۴۷	 (ز) سناریوی ساختگی
۲۴۸	 (ح) روش شناسی
۲۵۰	 (ط) کاربرد شبکه‌های بیز چند موجودیتی (MEBN)
۲۵۱	 (ی) محدودیت‌ها و تحقیقات دیگر در این حوزه
۲۵۳	 ۱۲. استفاده از متن کاوی برای کشف فعالیت‌های تروریستی در فضای مجازی
۲۵۵	 (الف) کاربرد روش‌های خوشه‌بندی
۲۵۵	 (ب) کشف مجرمان، نام‌های فعالیت‌های تروریستی
۲۵۶	 (ج) شناسایی رفتار، نوع تروریست‌ها
۲۵۷	 (د) فراگیری رفتار بومی تروریست‌ها
۲۵۸	 (ه) مطالعه موردی چارچوب فوق
۲۶۰	 ۱۳. متن کاوی خودکار موجودیت‌های مهم از متن گزارشات پلیس
۲۶۲	 (الف) خوشه‌بندی داده‌های جرم
۲۶۷	 (ب) تطابق جرم
۲۷۱	 ۱۴. نتیجه‌گیری
۲۷۵	 منابع مأخذ

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 توسعه 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.

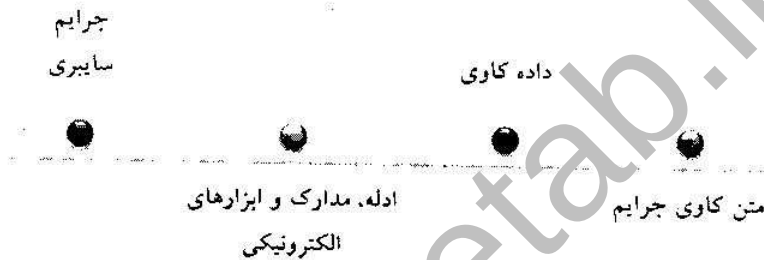
امروزه بیشتر از ۸۰ درصد از دانش افراد به صورت متن، مستندات و دیگر صور رسانه‌ای نظیر تصویر و صدا نگهداری می‌شود. اگر از منظر علوم رایانه‌ای به این مستندات نگاه شود، همه آنها به طبعی غیر ساخت یافته وابسته‌اند. یک فرد برای دریافت دانش از اطلاعات موجود در یک متن، ابتدا باید آن را درک و سپس آن را پردازش کند 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 متن کاوی است، از آنجا که این فناوری جوان و در حال رشد است؛ به کمک آن می‌توان دانش موجود در متون غیر ساخت یافته 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 متن کاوی بسیار زیاد بوده و تاکنون کتابی در زمینه کاربرد این گونه روش‌ها با رویکرد تشخیص جرایم در فضای مجازی تدوین نشده است، اهمیت و ضرورت تألیف 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 ادله دیجیتال فضای سایبر آشنا شوند. به طور قطع نصرات اصلاحی اساتید ارجمند و متخصصان گرامی می‌تواند در تکمیل و پربار شدن این کتاب تأثیرگذار باشد.

مقدمه مؤلف

با پیدایش رایانه و رشد سریع فناوری اطلاعات، جرایم نیز وارد پارادایم 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 از سید 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 - رایم 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 اجرا شده توسط ابزارهای دیجیتال مطرح می‌گردد تا از آن طریق بتوان روش‌های جمع‌آوری و تجزیه و تحلیل شواهد الکترونیکی در فضای مجازی را بیان کرد. در پایان این فصل به دلیل اهمیت موضوع و اینکه زیربنای

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

فصل چهارم، مروری بر یکی از روش‌ها و کاربردهای داده کاوی به نام متن کاوی است. با توجه به اینکه بیش از ۸۰ درصد اطلاعات به صورت متن و غیر ساختاریافته است و با عنایت به اینکه ادله الکترونیکی، به اشتراک گذاشته شده در فضای سایبر، حجم انبوهی از اطلاعات سازمان‌ها را تشکیل می‌دهد، استفاده از روش‌های استخراج اطلاعات در این فضا به منظور شناسایی جرایم اخته الی امری ضروری است که چنانچه سازمان پلیس برای بومی سازی این گونه روش‌ها در سامانه های جاری خود تصمیم مناسبی اتخاذ نکند، در آینده ای 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 متن کاوی و شیوه‌های تشخیص و سنجایی جرایم به شکلی کاملاً کاربردی مطرح شود تا مخاطب با مطالعه این فصل یک دید علمی و تجربی نسبت به روش‌های متن کاوی جرایم در فضای مجازی پیدا کند.

بهزاد لک

سال ۱۳۹۴