تعیین درجه اهمیت جرایم رایانه‌ای از دیدگاه صاحب نظران انتظامی استان بوشهر

حمید شاهبندرزاده[۱]
شهلا یوسفی ده‌بیدی[۲]

تاریخ وصول: ۹۱/۵/۳۰ تاریخ پذیرش: ۹۱/۸/۱۴

چکیده

جرم رایانه‌ای[۳] به استفاده غیرمجاز از فناوری‌های رایانه‌ای برای به دست گرفتن اطلاعات شخصی حساس و همین‌طور اطلاعات محرمانه سازمان‌ها اطلاق می‌شود. در این مقاله سعی شده است در ارتباط با انواع جرایم رایانه‌ای بحث شود که با بررسی متون و ادبیات گذشته پنج نوع جرم اصلی مرتبط با رایانه شناسایی شدند و مشخص گردید که از این پنج جرم اصلی (علیه عفت و اخلاق عمومی، علیه مقدسات اسلامی، علیه امنیت و آسایش عمومی، علیه مقامات و نهادهای دولتی و عمومی و سایر جرایم رایانه‌ای) محتوای علیه امنیت و آسایش عمومی از درجه اهمیت و امتیاز بیشتری از نظر متخصصان و خبرگان برخوردار است. سپس به اهمیت نسبی تمامی زیر شاخص‌های مربوط به هر کدام از محتوای اصلی اقدام شد و مهم‌ترین زیر شاخص‌ها نیز شناسایی شدند. پژوهش حاضر از نظر نوع تحقیق، کاربردی است. در این پژوهش‌ها شاخص‌های شناسایی شده با استفاده از دیدگان متخصصان و خبرگان انتظامی از طریق روش فرایند سلسله مراتب گروهی انجام شده است.

بنابراین، پس از استفاده از روش تحلیل سلسله مراتبی گروهی که به مقایسه زوجی شاخص‌های اصلی و فرعی بر حسب طیف ساعتی[۴] صورت گرفت، تصویر استراتژیک اهمیت هر یک از زیر شاخص‌ها به هر یک از شاخص‌های اصلی که محتوای جرم را مشخص کند معلوم شد.

۱- استادیار گروه مدیریت صنعتی دانشگاه خلیج فارس
۲- دانشجوی کارشناسی ارشد رشته مدیریت صنعتی دانشگاه خلیج فارس (نویسنده مسئول) yousafi-shala@yahoo.com

3. Computer crime
4. Saaty

نتایج این تحقیق نشان می‌دهد که مهم‌ترین نوع جرایم رایانه‌ای «محتوای علیه امنیت و آسایش عمومی بیشترین وزن و زیرشاخص» تشکیل جمعیت، دسته و گروه در فضای مجازی با هدف بر هم زدن امنیت کشور تقریباً ۳۰ درصد از وزن مورد را به خود اختصاص داده است.

کلید واژه‌ها: *جرایم رایانه‌ای، نظم اجتماعی، امنیت عمومی، روش تحلیل سلسله مراتبی*[1].

مقدمه و بیان مسئله

با شیوع استفاده از رایانه در زندگی شخصی و روابط اداری، بزهکاری و تخلف در استفاده از رایانه نیز، واقعه‌ای اجتناب ناپذیر است. آنچه امروز تحت عنوان جرایم رایانه‌ای نام برده می‌شود، مجموعه‌ای از همین تخلفات و بزهکاری‌هاست که از طریق رایانه یا مؤثر بر رایانه اتفاق می‌افتد و مصادیق متعددی از آن نیز در ذهن ما نقش بسته است.چه بسا ساده‌ترین مصادیقی که به جهت کثرت اتفاق در ذهن داریم، مواردی مانند هک پایگاه‌های اینترنتی یا انتشار داده‌های محرمانه از طریق وب سایت‌هاست که اغلب با تصور تخلف در خلأ قانون و عدم امکان تعقیب اتفاق افتاده است. این خلأ قانونی یا عدم شناخت قوانین مرتبط در حدی است که قربانیان این تخلفات همواره در یافتن پناهی برای تظلم خواهی، عاجز می‌مانند.

از زمان ابداع اینترنت تا زمانی که استفاده از اینترنت شکل عمومی پیدا کرد، تصور از پیش تعیین شده‌ای درباره این امکان ارتباطاتی و اتفاقاتی که در آن می‌افتد، وجود نداشت. اتفاقات بسیاری در این زمینه روی داد و سپس کسانی به دنبال تبیین و در مواردی برخورد یا جلوگیری از آن برآمدند.

رایانه و فناوری‌های مرتبط با آن ابزاری ضروری است که جنبه‌های مختلف قابل توجهی از زندگی اجتماعی و شخصی از قبیل آموزش، کسب و کار، فرهنگ و فعالیت‌های اوقات فراغت را تحت تأثیر قرار می‌دهد. استفاده گسترده از رایانه‌های شخصی و اینترنت با سرعت بالا انحرافات مرتبط با رایانه و رفتارهای جنایی از قبیل هک کردن[2]،

1.Group Analytical Hierarchy Process
2. Hacking

بارگذاری موسیقی به صورت غیر قانونی، برنامه‌های نرم افزاری، سرقت رمز عبور دیگران و... به صورت قابل توجهی افزایش داده است (روبرت[1] و اولسون[2]، ۲۰۱۰).

مجرمان رایانه‌ای معمولاً به از بین بردن، خراب کردن و دزدی اطلاعات تمایل دارند.کارهایی از قبیل کلاهبرداری‌های الکترونیکی، سوء استفاده از تجهیزات، جازدن خود به جای کس دیگر و همین‌طور اخلال در سیستم‌ها از جمله جرایم رایانه‌ای معمول است که بسیار اتفاق می‌افتد. یک عمل مجرمانه رایانه‌ای لزوماً وارد کردن خسارت فیزیکی به یک تجهیزات یا یک سیستم نیست. بلکه گاه فقط دسترسی به بعضی اطلاعات حساس یا محرمانه[3] می‌تواند جرم باشد. این اطلاعات می‌تواند اطلاعات خصوصی یا فردی باشد. این روزها این گونه اعمال خلاف روبه افزایش است و تنوع آنها هم روز به روز بیشتر می‌شود و ما هم ناگزیریم از سیستم‌های امنیتی جدیدتر استفاده کنیم و در این میان آگاهی ما می‌تواند از قربانی شدن ما جلوگیری کند (پست نت، ۲۰۰۶). بنابراین مسئله اصلی این مطالعه این است که انواع جرایم رایانه‌ای کدامند؟ و هر کدام از این جرایم از نظر خبرگان و متخصصان انتظامی از چه درجه و اهمیتی برخوردارند و چه نقشی در امنیت و آسایش عمومی دارند؟ هدف اصلی این پژوهش شناسایی و تبیین انواع جرایم رایانه‌ای که در امنیت و آسایش عمومی نقش دارند و هدف دیگر آن تعیین میزان اهمیت و نقش هرکدام از جرایم از دیدگاه انتظامی در تأمین نظم و امنیت انتظامی است.

مبانی نظری تحقیق

تعریف جرایم رایانه‌ای

در مورد تعریف جرم رایانه‌ای، خرم آبادی (۱۳۸۳) جرایم رایانه‌ای را جزء جرایم مرتبط با فناوری اطلاعات می‌دانند و این‌گونه بیان می‌کنند که «اصطلاحات جرم رایانه‌ای و جرم مرتبط با رایانه، اولین و قدیمی‌ترین اصطلاحاتی هستند که برای نسل اول جرایم فناوری اطلاعات مورد استفاده قرار گرفته‌اند (ص ۷۶) و «علت انتخاب عناوین جرم رایانه‌ای و

1. Robert
2.Olson
3.Confidential

جرم مرتبط با رایانه برای این‌گونه جرایم این بوده که رایانه به عنوان هدف یا وسیله ارتکاب جرم در این گونه جرایم محوریت داشته است».

تعریف جرایم از منظر سازمان‌های مختلف

سازمان OECD

سوء استفاده از رایانه شامل هر رفتار غیرقانونی، غیراخلاقی یا غیر مجاز مربوط به پردازش خودکار در انتقال داده است.

سازمان ملل متحد: جرم رایانه‌ای می‌تواند شامل فعالیت‌های مجرمانه‌ای باشد که ماهیتی سنتی دارند اما از طریق ابزار مدرنی مثل رایانه و اینترنت صورت می‌گیرد.

کمیته اروپایی مسائل جنایی در شورای اروپا: هر فعل مثبت غیرقانونی که رایانه در آن ابزار یا موضوع جرم باشد. به عبارت دیگر هر جرمی که ابزار و هدف تأثیرگذاری آن رایانه باشد.

پلیس فدرال آلمان: جرایم متضمن اعمال توأم با بی مبالاتی یا حوادثی که موجب تخریب عملکرد سیستم رایانه یا استفاده از آن باشد، جرم رایانه‌ای است.

یک مضمون مشترک در میان تعاریف از جرم و جنایات رایانه‌ای، استفاده غیر قانونی از رایانه و دستگاه‌های مرتبط با رایانه به وسیله افراد، گروه‌ها یا سازمان‌های خاص با دانش رایانه است.

تعداد چشمگیری از مکالمات بر انواع متعددی از جرم و جنایت تمرکز کرده‌اند، که شامل کپی غیر قانونی و تجاری از نرم افزارهای شرکت‌های تجاری، دسترسی غیر قانونی به سیستم‌های رایانهٔ اشخاص و ایجاد انتشار برنامه‌های ویروس رایانه‌ای با استفاده از نمونه‌های غیرتصادفی از دانشجویان دانشگاه است (هیگینس، ۲۰۰۷).

تاریخچه پیدایش جرم رایانه‌ای

تاریخچه مشخصی از پیدایش جرم اینترنتی و رایانه‌ای وجود ندارد ولی به هرحال این دسته از جرایم را باید نتیجه فناوری ارتباطی و اطلاعاتی دانست.کارشناسان رایانه بر این باور هستند که منشأ پیدایش جرم رایانه و اینترنتی به قضیه رویس[1] باز می‌گردد؛ این شخص که بعد از بی‌مهری مسئولان یک شرکت فروش عمده میوه و سبزی، به عنوان حسابدار آنها انتخاب شد از طریق رایانه اقدام به حسابرسی می‌کرد و با تغییر قیمت‌ها و تنظیم درآمد جنس، مبلغی از مرجع آن را کاهش می‌داد و به حساب دیگری واریز می‌کرد. رویس با ظرافت خاصی قیمت‌ها را تغییر می‌داد، بعد از آن با نام هفده شرکت محل و طرف قرارداد، چک‌های جعلی صادر و از آن حساب برداشت می‌کرد به طوری که در کمتر از شش سال به بیش از یک میلیون دلار رسید اما به علت نداشتن مکانیزمی برای توقف این روند، رویس خودش را به محاکم قضایی معرفی کرد و به ده سال زندان محکوم شد. به این ترتیب، کارشناسان رایانه می‌گویند بر اساس مطالعات صورت گرفته زمینه پیدایش جرم رایانه‌ای این گونه به وجود آمده است (پست نت، ۲۰۰۶).

براساس اطلاعات موجود اولین جرم اینترنتی درایران در تاریخ ۲۶ خرداد ۱۳۷۸ به وقوع پیوست. یک کارگر چاپ خانه و یک دانشجوی رایانه اقدام به جعل چک‌های تضمینی مسافرتی کردند و بعد از این بود که گروه‌های هکر جرم‌های دیگری را مرتکب شدند، مواردی چون جعل اسکناس، اسناد و بلیت‌های شرکت‌های اتوبوس‌رانی، جعل اسناد دولتی از قبیل گواهی نامه، کارت پایان خدمت، مدرک تحصیلی و جعل چک‌های مسافرتی و عادی بخشی از این جرایم رایانه‌ای است.

مون[2] و مک کلوسکی[3] (۲۰۱۰) بیان می‌کنند که جرایم رایانه‌ای به یک مسئله جهانی تبدیل شده است و همچنان به سرعت در حال رشد است. با این حال مطالعات کمی در مورد کاربرد نظریه عمومی جرم و جنایت صورت گرفته است. با استفاده از یک مطالعه که از ۲۷۵۱ جوان کره‌ای صورت گرفت، بررسی کردند که آیا خود کنترلی می‌تواند به عنوان

1.Theorem Roiis
2. Moon
3. McCluskey

یک چارچوب نظری برای کاهش جنایات رایانه‌ای مؤثر واقع شود یا نه. نتایج مطالعات نشان داد که دانلود غیرقانونی نرم‌افزارها و استفاده غیرقانونی از هویت شخصی دیگران تا حدودی به خود کنترلی مربوط می‌باشد. مطابق با پیش‌بینی این نظریه‌ها متغیرهای فرصتی همچون ساعات استفاده از رایانه به این پیش‌بینی کمک کرده است.

هیگینس[1] و فل[2] (۲۰۰۵) با استفاده از یک نمونه مورد مطالعه از ۳۱۶ دانشجوی کالج نشان دادند که بین خودکنترلی کم و دزدی نرم افزار یک رابطه مثبت وجود دارد.

بر اساس گفته آدل[3] و رومان[4] (۲۰۰۸)، رایانه و فناوری‌های مرتبط با آن ابزاری ضروری است که جنبه‌های مختلف قابل توجهی از زندگی اجتماعی و شخصی از قبیل آموزش، کسب و کار، فرهنگ و فعالیت‌های اوقات فراغت را تحت تأثیر قرار می‌دهد. با استفاده گسترده از رایانه‌های شخصی و اینترنت با سرعت بالا انحرافات مرتبط با رایانه و رفتارهای جنایی از قبیل هک کردن، بارگذاری موسیقی به صورت غیر قانونی، برنامه‌های نرم افزاری، سرقت رمز عبور دیگران و... به صورت قابل توجهی افزایش پیدا کرده است (هیگینس و ریکرت[5]، ۲۰۰۹).

با توجه به اهمیت موضوع تعداد فزاینده‌ای از مطالعات در سال‌های اخیر به بررسی جنایات رایانه‌ای پرداخته‌اند. یار[6] (۲۰۰۵)، هیگنس (۲۰۰۷) و فوستر[7] (۲۰۰۴) با تمرکز بر علت انحرافات رایانه‌ای و نظریه‌های جرم شناسی سنتی از قبیل (خود کنترلی، نظریه یادگیری اجتماعی- عقلایی و نظریه انتخاب توانستند انحرافات رایانه‌ای را مورد بررسی قرار دهند.

به طور کلی یافته‌های تجربی شواهدی را در ارتباط با توانایی نظریه‌های جرم شناسی سنتی در توضیح انواع مختلفی از جرایم مربوط به رایانه فراهم می‌کند.

1. Higgins
2. Fell
3. Audal
4. Roman
5. Ricketts
6.Yar
7. Foster

مک کواد[1] (۲۰۰۸) بیان می‌کند که اگر چه مطالعات تجربی به بهبود درک درستی از جرایم رایانه‌ای کمک می‌کند اما محدودیت‌هایی نیز دارند. از جمله اینکه تعداد محدودی از مطالعات تجربی نظریه عمومی جرم را در مورد گسترش انحرافات رایانه‌ای مورد بررسی قرار داده‌اند. با وجود ادعای این نظریات عدم خود کنترلی علت اصلی بسیاری از رفتارهای مجرمانه است.

یک نظرسنجی که ویلسون[2] و پاترسون[3] (۲۰۰۶) از ۲۰۶۶ سازمان کسب و کار در ایالات متحده انجام دادند متوجه که ۶۴ درصد از کسب وکارهای منتشر شده حداقل از یک حادثه امنیتی رایانه زیان مالی دیده‌اند. با توجه به اهمیت موضوع تعداد فزاینده‌ای از مطالعات انجام شده در سال‌های اخیر به بررسی انحرافات رایانه‌ای با تمرکز بر علت این انحرافات پرداخته است.

انواع جرایم رایانه‌ای

با توجه به مطالب ذکر شده در بالا انواع و اقسام جرایم رایانه‌ای موجود در ایران را می‌توان به پنج دسته تقسیم کرده که در زیر مجموعهٔ هر یک از آنها در جدول ۱ ذکر شده است.

جدول ۱: انواع و اقسام جرایم رایانه‌ای

شاخص‌های اصلی	زیر شاخص‌ها (متغیرها)	
محتوای علیه عفت و اخلاق عمومی	A_1	تحریک، تشویق، ترغیب، تهدید یا دعوت به فساد و فحشا و ارتکاب جرایم منافی عفت یا انحرافات جنسی
	A_2	اشاعه فحشا و منکرات
	A_3	انتشار، توزیع و معامله محتوای خلاف عفت عمومی(مبتذل و مستحجن)
	A_4	تحریک، تشویق، ترغیب، تهدید یا تطمیع افراد به دستیابی به محتویات مستحجن و مبتذل
	A_5	استفاده ابزاری از افراد در تصاویر و محتوا، تحقیر و توهین به جنس زن، تبلیغ تشریفات و تجملات(نامشروع و غیر قانونی)

1. McQuade
2.Wilson
3. Patterson

محتوای علیه مقدسات اسلامی	B_1	محتوای الحادی و مخالف موازین اسلامی
	B_2	اهانت به دین مبین اسلام و مقدسات آن
	B_3	اهانت به هر یک از انبیا عظام یا ائمه طاهرین
	B_4	تبلیغ به نفع حزب، گروه یا فرقه منحرف و مخالف اسلام
	B_5	تبلیغ مطالب از نشریات و رسانه‌ها و گروه‌های داخلی و خارجی منحرف و مخالف اسلام به نحوی که تبلیغ از آنها باشد.
	B_6	اهانت به امام خمینی و تحریف آثار ایشان
	B_7	اهانت به مقام معظم رهبری و سایر مراجع مسلم تقلید
محتوای علیه امنیت و آسایش عمومی	C_1	تشکیل جمعیت، دسته و گروه در فضای مجازی(سایبر) با هدف برهم زدن امنیت کشور
	C_2	محتوایی که به اساس جمهوری اسلامی ایران لطمه وارد می‌کند
	C_3	فاش کردن و انتشار غیر مجاز اسرار نیروهای مسلح
	C_4	اخلال در وحدت ملی و ایجاد اختلاف مابین اقشار جامعه به ویژه از طریق طرح مسائل نژادی و قومی
	C_5	انتشار بدون مجوز مذاکرات محاکم غیر علنی دادگستری و تحقیقات مراجع قضایی
	C_6	تبلیغ علیه نظام جمهوری اسلامی ایران
	C_7	تبلیغ به نفع گروه‌ها و سازمان‌های مخالف نظام جمهوری اسلامی ایران
	C_8	فاش کردن و انتشار غیر مجاز اسناد محرمانه و سری دولتی و عمومی
	C_9	انتشار محتوی علیه اصول قانون اساسی
محتوای علیه مقامات و نهادهای دولتی	D_1	اهانت نسبت به مقامات، نهادها و سازمان‌های حکومتی و عمومی
	D_2	افترا به مقامات، نهادها و سازمان‌های حکومتی و عمومی
	D_3	نشر اکاذیب و تشویق اذهان عمومی علیه مقامات، نهادها و سازمان‌های حکومت
سایر جرایم رایانه ای	E_1	انتشار یا توزیع و در دسترس قراردادن یا معامله داده‌ها یا نرم‌افزارهایی که صرفاً برای ارتکاب جرایم رایانه‌ای به کار می‌رود
	E_2	فروش، انتشار یا در دسترس قرار دادن غیر مجاز گذرواژه‌ها و داده‌هایی که امکان دسترسی غیر مجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی دولتی و عمومی را فراهم می‌کند
	E_3	انتشار یا در دسترس قرار دادن محتویات آموزش دسترسی غیر مجاز، شنود غیر مجاز، جاسوسی رایانه‌ای، تحریف و اخلال در داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی
	E_4	انجام هرگونه فعالیت تجاری و اقتصادی رایانه ای مجرمانه مانند شرکت‌های هرمی
	E_5	تبلیغ و ترویج مصرف مواد مخدر، مواد روان گردان و سیگار
	E_6	انتشار محتوایی که از سوی شورای عالی امنیت ملی منع شده باشد
	E_7	عرضه تجاری آثار سمعی و بصری بدون مجوز وزارت فرهنگ و ارشاد اسلامی

E_8	تشویق، تحریک و تسهیل ارتکاب جرایمی که دارای جنبه عمومی هستند از قبیل اخلال در نظم، تخریب اموال عمومی، اختلاس، کلاهبرداری، قاچاق مواد مخدر و مشروبات الکلی

منبع: دبیرخانه کارگروه تعیین مصادیق جرایم رایانه‌ای (۱۳۹۱)

روش‌شناسی تحقیق

روش تحقیق این پژوهش از نوع کاربردی است. در این پژوهش، با استفاده از مطالعات پیشین و قوانینی که در کشور مطرح شده‌اند همچنین با توجه به اینکه سعی شده است از مقالات جدید استفاده گردد، شاخص‌های مربوطه از ادبیات موضوعی استخراج و اقدام به شناسایی و رتبه‌بندی انواع جرایم رایانه‌ای شده و مدل مفروض از طرف نویسندگان طرح شده است. همچنین در این پژوهش شاخص‌های شناسایی شده با استفاده از دیدگاه اندیشمندان و متخصصان از طریق روش فرایند تحلیل سلسله مراتبی گروهی رتبه‌بندی می‌شود. در این شیوه به نرخ ناسازگاری نظر متخصصان به صورت انفرادی و سپس جمع‌بندی گروهی اقدام گردیده است. در واقع با توجه به کمیته کردن نرخ ناسازگاری سعی شده به تلفیق نظر متخصصان اقدام شود.

در اینجا فرض شده است که این شاخص‌ها از هم مستقل بوده و با تأیید یکی، در ارزیابی گزینه‌ها بی‌نیاز از دیگری نبوده یا به عبارتی روش ارزیابی از نوع غیر جبرانی خواهد بود.

در مدل سلسله مراتبی مربوط به این پژوهش سعی شده است که همچنان از سطوح گزینه‌ها به سطح شاخص‌های فرعی و شاخص‌های اصلی بالا برویم. شاخص اثرگذار پایین را بر حسب وزن و اهمیت اثرگذاریشان بر تعیین جرم رایانه‌ای چنان مشخص کنیم که بتواند برای مسئولان و تصمیم‌گیرندگان مشخص کند که با کمترین هزینه‌ها در شاخص‌های فرعی یا زیرشاخص‌ها چگونه می‌توان بیشترین اثربخشی را دنبال کرد. چنین حرکتی در مسیر مدل سلسله مراتبی توسط نویسندگان مسیر راهبردی نام‌گذاری شده است.

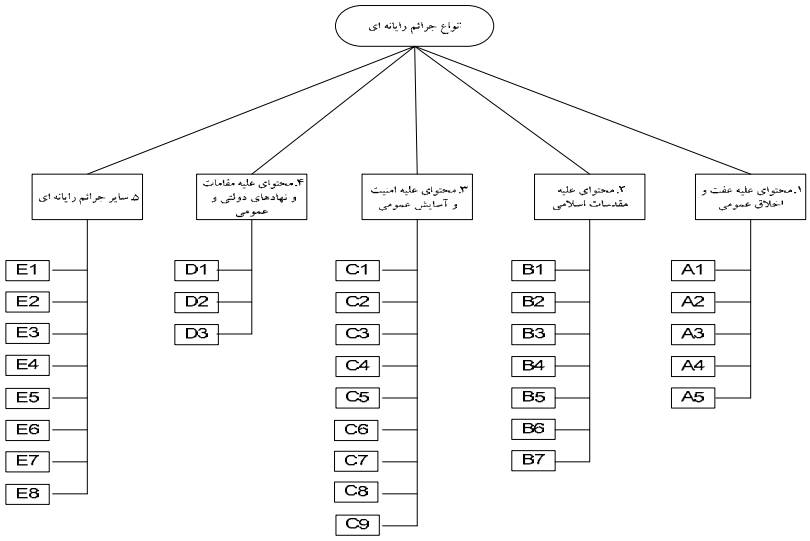
فرایند تحلیل سلسله مراتبی (G AHP)

فرایند تحلیل سلسله‌مراتبی یکی از معروف‌ترین فنون تصمیم‌گیری چند معیاره است که اولین بار توسط توماس. ال. ساعتی عراقی‌الاصل در دهه ۱۹۷۰ ابداع شد و در موارد مختلف تصمیم‌گیری، مورد مطالعه و استفاده قرار گرفته است. این روش هنگامی که عمل تصمیم‌گیری با چند گزینهٔ رقیب و معیار تصمیم‌گیری روبه رو است می‌تواند استفاده شود. معیارهای مطرح شده می‌توانند کمی یا کیفی باشند. اساس این روش تصمیم‌گیری بر مقایسه‌های زوجی نهفته است. تصمیم‌گیرنده با درخت سلسله‌مراتب تصمیم آغاز می‌کند. درخت سلسله‌مراتب تصمیم عوامل مورد ارزیابی در تصمیم را نشان می‌دهد. سپس یک سری مقایسه‌های زوجی انجام می‌پذیرد. این مقایسه‌های وزن هر یک از فاکتورها را در راستای گزینه‌های رقیب مشخص می‌سازد. در نهایت منطق AHP به گونه‌ای ماتریس‌های حاصل از مقایسه‌های زوجی را با همدیگر تلفیق می‌سازد که تصمیم بهینه حاصل آید. در AHP برای مقایسهٔ گزینه‌های رقیب از مقایسه‌های زوجی استفاده می‌شود که از ترجیح یکسان تا بی‌اندازه مرجح طراحی شده است (هوپن، ۲۰۰۸). تجربه نشان داده است که استفاده از طیف ۱/۹ تا ۹ تصمیم‌گیرنده را قادر می‌سازد تا مقایسه‌ها را به گونه‌ای مطلوب انجام دهد. به همین علت استفاده از جدول شمارهٔ دو به صورت یک مقیاس استاندارد در آمده‌است (آذر و معماریانی، ۷۳.

جدول ۲: مقیاس مقایسهٔ دو به دو درAHP

مقدار عددی	درجهٔ اهمیت در مقایسه‌ی ۲ به ۲
۱	ترجیح یکسان
۲	یکسان تا نسبتاً مرجح
۳	نسبتاً مرجح
۴	نسبتاً تا قویاً مرجح
۵	قویاً مرجح
۶	قویاً تا بسیار قوی مرجح
۷	ترجیح بسیار قوی
۸	بسیار تا بی‌اندازه مرجح
۹	بی‌اندازه مرجح

در مدل‌سازی سلسله مراتبی، تهیه درخت سلسله مراتبی از مسئله، شاخص‌های تصمیم‌گیری و گزینه‌های تصمیم از اهمیت فراوانی برخوردار است. همان‌گونه که در نمودار ۱ دیده می‌شود درخت سلسله مراتبی تصمیم در این مقاله دارای سه سطح است. سطح اول، مربوط به سطح هدف است، که در اینجا سطح هدف انواع جرایم رایانه‌ای می‌باشد و قرار است که پی برده شود که مهم‌ترین جرم رایانه‌ای چیست. سطح دوم، سطح معیارهاست و نشان‌دهنده عواملی است که ملاک مقایسه گزینه‌ها هستند و مهم‌ترین محتوای جرایم رایانه‌ای را شناسایی کرده که در این راستا با توجه به مطالعه ادبیات موضوعی در داخل و خارج از کشور و استفاده از نظر کارشناسان در استان بوشهر پنج محتوای اصلی برای جرایم رایانه‌ای شناسایی شد، همچنین در سطح سوم که مربوط به زیرمعیارهاست مشخص شد که هر کدام از این شاخص‌های کلی خود می‌تواند به شاخص‌های فرعی که حداقل در این زیرمجموعه‌ها ۳ و حداکثر ۹ مورد بوده است تفکیک شود. این سطح بیان کننده گزینه‌هایی است که با همدیگر مقایسه می‌شوند و برای انتخاب در رقابت با همدیگر هستند. همچنین در این فرایند سلسله مراتبی سعی شده است مشخص کنیم که کدام محتوای جرم از اهمیت بالاتری برخوردار است و در درون آن کدام یک از جرایم مرتبط با آن از نظر کارشناسان این بخش دارای اهمیت بیشتری است. در نتیجه با توجه به این مسیرهای راهبردی می‌توان به منظور کنترل بیشتر بر این جرایم ضابطه‌های مدیریتی را رشد داده و حتی به آموزش نیروهای پلیس در این جهت و تخصیص بودجه لازم برای نظارت و کنترل مؤثر بر این نوع جرایم اقدام اساسی کرد.



نمودار ۱. درخت سلسله مراتبی تصمیم

در اینجا ماتریس‌های نهایی مقایسه‌های دوتایی فازی که حاصل ترکیب پنج ماتریس مربوط به پنج خبره است نمایش داده شده و سپس وزن‌های نهایی آنها ارائه شده است.

لازم به ذکر است که در زیر یکی از این ماتریس‌ها به عنوان نمونه آورده شده است. بدیهی است به دلیل کاهش تعداد جداول در متن بقیه جداول به ضمائم انتقال یافته است.

جدول ۳. ماتریس مقایسه معیارهای شاخص محتوای علیه عفت و اخلاق عمومی

	A_1	A_2	A_3	A_4	A_5
A_1	۱	۲	۲/۰	۳	۴
A_2	۵/۰	۱	۳۳۳۳۳۳/۰	۲	۳
A_3	۵	۳	۱	۲	۳
A_4	۳۳۳۳۳۳/۰	۵/۰	۵/۰	۱	۲
A_5	۲۵/۰	۳۳۳۳۳۳/۰	۳۳۳۳۳۳/۰	۵/۰	۱

CI = ۰/۰۷۲۳۴

جدول ۳ ماتریس نهایی مقایسه پنج خبره است که به صورت گروهی از جمع‌بندی ماتریس‌های انفرادی به دست آمده است.

جدول ۴. ماتریس مقایسه شاخص‌های اصلی

	K_1	K_2	K_3	K_4	K_5
K_1	۱	۲	۱	۳	۲
K_2	۰/۵	۱	۰/۵	۲	۱
K_3	۱	۲	۱	۲	۳
K_4	۰/۳۳۳۳۳۳.	۰/۵	۰/۵	۱	۰/۳۳۳۳۳۳.
K_5	۰/۵	۱	۰/۳۳۳۳۳۳.	۳	۱

CI=0/033132

جدول ۴، ماتریس مقایسه‌ای پنج شاخص اصلی است که هر کدام از این شاخص‌های اصلی با یکدیگر مقایسه شده که این جدول نیز از ترکیب ماتریس نظرات پنج نفر نتیجه‌گیری برای اوزان و اهمیت هر یک از شاخص‌ها آمده است. پس از تولید ماتریس‌های مقایسه‌های زوجی، با استفاده از اطلاعات به دست آمده از این ماتریس‌ها، وزن (اولویت) هر یک از عناصر تصمیم تعیین می‌شود. این اوزان در نگاره‌های ۵ تا ۱۴ آورده شده است، هر یک از این عناصر بر اساس وزن‌ها به ترتیب از بزرگ به کوچک مرتب شده‌اند که تحلیل مختصری در مورد هریک از این نگاره‌ها در زیر جداول ارائه شده است.

جدول ۵: وزن معیارهای شاخص محتوای علیه عفت و اخلاق عمومی

ردیف	زیرشاخص	گزینه	وزن
۱	A_5	استفاده ابزاری از افراد در تصاویر و محتوا، تحقیر و توهین به جنس زن، تبلیغ تشریفات و تجملات(نامشروع و غیر قانونی)	۰/۴۰۶۷
۲	A_1	تحریک، تشویق، ترغیب، تهدید یا دعوت به فساد و فحشا و ارتکاب جرایم منافی عفت یا انحرافات جنسی	۰/۲۳۵۷
۳	A_4	تحریک، تشویق، ترغیب، تهدید یا تطمیع افراد به دستیابی به محتویات مستحجن و مبتذل	۰/۱۶۴۷
۴	A_3	انتشار، توزیع و معامله محتوای خلاف عفت عمومی(مبتذل و مستحجن)	۰/۱۲۰۵
۵	A_2	اشاعه فحشا و منکرات	۰/۰۷۲۱

جدول ۵ وزن‌های مربوط به شاخص محتوای علیه عفت و اخلاق عمومی را نشان می‌دهد. همان‌طور که مشاهده می‌کنید بیشترین وزن از نظر گروه خبرگان نظر سنجی شده

به استفاده ابزاری از افراد در تصاویر و محتوا، تحقیر و توهین به جنس زن، تبلیغ تشریفات و تجملات (نامشروع و غیر قانونی)، به شاخص(A_5) اختصاص دارد و کمترین وزن مربوط به اشاعه فحشا و منکرات یا شاخص (A_2) است.

جدول ۶: وزن معیارهای شاخص محتوای علیه مقدسات اسلامی

ردیف	زیرشاخص	گزینه	وزن
۱	B_3	اهانت به هر یک از انبیا عظام یا ائمه طاهرین	۰/۳۸۹۱
۲	B_2	اهانت به دین مبین اسلام و مقدسات آن	۰/۲۰۰۳
۳	B_1	محتوای الحادی و مخالف موازین اسلامی	۰/۱۲۸۹
۴	B_6	اهانت به امام خمینی و تحریف آثار ایشان	۰/۰۹۸۶
۵	B_7	اهانت به مقام معظم رهبری و سایر مراجع مسلم تقلید	۰/۰۸۶۹
۶	B_4	تبلیغ به نفع حزب، گروه یا فرقه منحرف و مخالف اسلام	۰/۰۶۱۸
۷	B_5	تبلیغ مطالب از نشریات و رسانه‌ها و گروه‌های داخلی و خارجی منحرف و مخالف اسلام به نحوی که تبلیغ از آن‌ها باشد	۰/۰۳۳۹

جدول ۶ وزن‌های مربوط به شاخص محتوای علیه مقدسات اسلامی را نشان می‌دهد. همان‌طور که این ماتریس نشان می‌دهد بیشترین وزن از نظر گروه خبرگان مربوط به اهانت به هر یک از انبیاء عظام یا ائمه طاهرین، شاخص (B3) می‌باشد، و کمترین وزن مربوط به تبلیغ مطالب از نشریات، رسانه‌ها و گروه‌های داخلی و خارجی منحرف و مخالف اسلام به نحوی که تبلیغ از آنها باشد، (B5) است.

جدول ۷. وزن معیارهای شاخص محتوای علیه امنیت و آسایش عمومی

ردیف	زیرشاخص	گزینه	وزن
۱	C_1	تشکیل جمعیت، دسته و گروه در فضای مجازی(سایبر) با هدف برهم زدن امنیت کشور	۰/۲۹۱۱
۲	C4	اخلال در وحدت ملی و ایجاد اختلاف مابین اقشار جامعه از طریق طرح مسائل نژادی و قومی	۰/۲۲۱۴
۳	C_5	انتشار بدون مجوز مذاکرات محاکم غیرعلنی دادگستری و تحقیقات مراجع قضایی	۰/۱۱۲۶

۴	C_6	تبلیغ علیه نظام جمهوری اسلامی ایران	۰/۱۱۰۲
۵	C_2	محتوایی که به اساس جمهوری اسلامی ایران لطمه وارد می کند	۰/۰۸۰۲
۶	C_8	فاش نمودن، انتشار غیر مجاز اسناد، دستور و مسائل محرمانه، سری دولتی و عمومی	۰/۰۶۸۱
۷	C_9	انتشار محتوی علیه اصول قانون اساسی	۰/۰۵۳۸
۸	C_7	تبلیغ به نفع گروهها و سازمان‌های مخالف نظام جمهوری اسلامی ایران	۰/۳۶۸
۹	C_3	فاش نمودن و انتشار غیر مجاز اسرار نیروهای مسلح	۰/۰۲۵۴

جدول ۷ وزن‌های مربوط به شاخص محتوای علیه امنیت و آسایش عمومی را نشان می‌دهد، که بیشترین وزن مورد نظر به شاخص C_1 (۰/۲۹۱۱) داده شده است و کمترین وزن به شاخص C_3 (۰/۰۲۵۴) تعلق دارد.

جدول ۸: وزن معیارهای شاخص محتوای علیه مقامات و نهادهای دولتی و عمومی

ردیف	زیرشاخص	گزینه	وزن
۱	D2	افترا به مقامات، نهادها و سازمان‌های حکومتی و عمومی	۰/۵۷۳۶
۲	D_1	اهانت نسبت به مقامات، نهادها و سازمان‌های حکومتی و عمومی	۰/۲۸۶۴
۳	D_3	نشر اکاذیب و تشویق اذهان عمومی علیه مقامات، نهادها و سازمان‌های حکومتی	۰/۱۳۹۹

جدول ۸ وزن‌های مربوط به شاخص محتوای علیه مقامات و نهادهای دولتی و عمومی است که بیشترین وزن داده شده از نظر خبرگان مربوط به شاخص D_2 است و کمترین وزن مربوطه متعلق به شاخص D_3 می‌باشد.

جدول ۹: وزن معیارهای شاخص سایر جرایم رایانه‌ای

ردیف	زیرشاخص	گزینه	وزن
۱	E_1	انتشار یا توزیع و در دسترس قرار ددادن یا معامله داده‌ها یا نرم‌افزارهایی که صرفاً برای ارتکاب جرایم رایانه‌ای به کار می‌رود	۰/۲۵۸۷
۲	E_4	انجام هرگونه فعالیت تجاری و اقتصادی رایانه ای مجرمانه مانند شرکت‌های هرمی	۰/۱۷۳۷
۳	E_6	انتشار محتوایی که از سوی شورای عالی امنیت ملی منع شده باشد	۰/۱۶۹۹

۴	E_5	تبلیغ و ترویج مصرف مواد مخدر، مواد روان گردان و سیگار	۰/۱۴۶۹
۵	E_3	انتشار, دسترس قرار دادن محتویات آموزش دسترسی غیر مجاز، شنود غیر مجاز، جاسوسی رایانه‌ای، تحریف و اخلال در داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی	۰/۰۷۹۱
۶	E_2	فروش، انتشار یا در دسترس قرار دادن غیر مجاز گذرواژه‌ها و داده‌هایی که امکان دسترسی غیر مجاز به داده‌ها با سامانه‌های رایانه‌ای یا مخابراتی دولتی و عمومی را فراهم می‌کند	۰/۰۶۴۵
۷	E_7	عرضه تجاری آثار سمعی و بصری بدون مجوز وزارت فرهنگ و ارشاد اسلامی	۰/۰۵۵۷
۸	E_9	تشویق، تحریک و تسهیل ارتکاب جرایمی که دارای جنبه عمومی هستند از قبیل اخلال در نظم، تخریب اموال عمومی، اختلاس، کلاهبرداری، قاچاق مواد مخدر و مشروبات الکلی	۰/۰۵۱۰

جدول ۹ وزن‌های مربوط به شاخص سایر جرایم رایانه‌ای است که بیشترین وزن داده شده مربوط به شاخص E_1 و کمترین وزن داده شده از نظر گروه خبرگان مربوط به شاخص E_9 است.

جدول ۱۰: وزن معیارهای کلی

ردیف	شاخص	گزینه	وزن
۱	K_4	محتوای علیه امنیت و آسایش عمومی	۰/۲۹۹۷
۲	K_3	محتوای علیه مقدسات اسلامی	۰/۲۹۰۶
۳	K_2	محتوای علیه مقامات و نهادهای دولتی و عمومی	۰/۱۶۲۵
۴	K_1	محتوای علیه عفت و اخلاق عمومی	۰/۱۵۴۴
۵	K_5	سایر جرایم رایانه‌ای	۰/۰۹۲۶

جدول ۱۰ مربوط به پنج شاخص اصلی جرایم رایانه‌ای است که هر کدام از این شاخص‌ها با هم مقایسه شده‌اند و وزن‌های مربوط به آنها به دست آمده است. همان‌طور که مشاهده می‌کنید بیشترین وزن از نظر خبرگان مربوط به شاخص محتوای علیه امنیت و

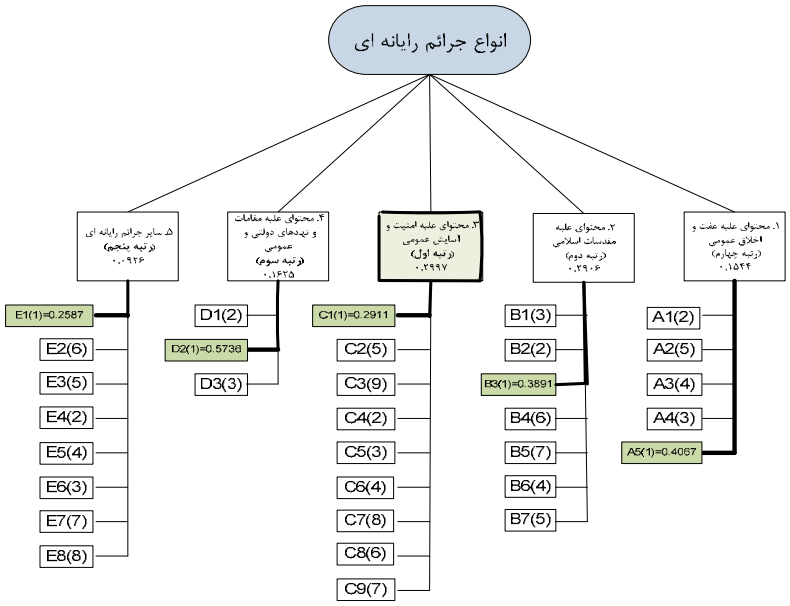
آسایش عمومی (K_4) است و کمترین وزن آن به شاخص سایر جرایم رایانه‌ای مربوط می‌شود.

نتیجه‌گیری

همان‌گونه که قبلاً در روش‌شناسی پژوهشی نیز بحث شد و همچنان‌که در شکل دو ملاحظه می‌شود مسیر راهبردی[1] هر یک از جرایم رایانه‌ای مشخص شده است. بعد از ارزیابی و اولویت‌بندی جرم‌ها، وزن هر یک از جرم‌های اصلی و زیر معیارهای آن به دست آمد و مسیر راهبردی آنها مشخص شد، که با استفاده از آن می‌توان به راحتی اهمیت هر یک از جرایم رایانه‌ای را مورد بررسی قرار داد.

همان‌طور که مشاهده می‌شود مهم‌ترین نوع جرایم رایانه‌ای «محتوای علیه امنیت و آسایش عمومی» است که بیشترین وزن ممکن را به خود اختصاص داده است و مهم‌ترین زیر معیار آن مربوط به شاخص c_1 (تشکیل جمعیت، دسته و گروه در فضای مجازی با هدف برهم زدن امنیت کشور) است که تقریباً ۳۰ درصد از وزن مورد نظر را به خود اختصاص داده است. بنابراین بیشترین توجه مسئولان باید متوجه این زیر شاخص باشد و سپس زیرمعیارهای دیگر به ترتیب اهمیت وزن رتبه‌بندی شده‌اند. برای این پنج معیار اصلی مهم‌ترین زیرشاخص‌ها مشخص شده‌اند و وزن‌های هر کدام از آنها به دست آمد، که همان‌طور که در شکل مشاهده می شود رتبه‌های هر کدام از زیر معیارها نوشته شده است. برای مثال در شاخص محتوای علیه مقامات و نهادهای دولتی مهم‌ترین زیرشاخص، اهانت نسبت به مقامات، نهادها و سازمان‌های حکومتی و عمومی (D_2) است که ۵۷ درصد وزن مربوطه را به خود اختصاص داده است.

۱- نویسندگان به دلیل اینکه زیر شاخص‌های مؤثر بر شاخص‌های بالاتر را بر اساس وزن‌های به دست آمده و نرخ ناسازگاری متناسب یافته‌اند مسیر مذکور را مسیر راهبردی نام نهاده‌اند.



نمودار ۲. مدل مسیر راهبردی جرایم رایانه‌ای

پیشنهادها

پژوهشگران بر این عقیده‌اند که باید براساس اطلاعات به دست آمده از این پژوهش که همان مسیر راهبردی اثرگذاری شاخص‌ها و زیرشاخص‌های شناخته شده در جرایم رایانه-ای است، دست‌اندکاران امنیت کشور و کارکنان نیروی انتظامی بودجه و آموزش‌های لازم را برای کنترل جرایم رایانه‌ای تخصیص دهند تا هم در صرف بودجه موردنظر مدیریت و اداره لازم صورت پذیرد و هم اینکه برای جلوگیری از جرایم رایانه‌ای از مهم‌ترین آنها شروع کرده و اقدامات لازم را مبذول دارند. واضح است بر حسب یافته‌های پژوهشی این مقاله هزینه‌های مرتبط با کاهش جرایم رایانه‌ای می‌بایست با بذل توجه به زیرشاخص C_1 از شاخص اصلی k_4 صورت پذیرد. همچنین درگام‌های بعدی زیرشاخص‌های k_3 ،k_2 ،k_1 و k_5 قرار می‌گیرد. همچنین بدیهی است به این طریق می توان به بررسی، طبقه‌بندی و شناسایی انواع جرایم رایانه‌ای از نظر متخصصان و خبرگان نیروی انتظامی اقدام کرد.

منابع

آذر، ع؛ معماریانی ,ع. (۱۳۷۳). تکنیکی نوین برای تصمیم‌گیری گروهی. *دانش مدیریت* - دوره۲۷ و ۲۸، شماره ٤.

خرم آبادی، عبدالصمد. (۱۳۸۳). جرایم فناوری اطلاعات. (رساله دکتری) دانشکده حقوق و علوم سیاسی دانشگاه تهران.

دبیرخانه کارگروه تعیین مصادیق محتوای مجرمانه (۱۳۹۱). مصادیق محتوای مجرمانه، قابل دسترسی در آدرس http://peyvandha.ir/gozaresh/

Audal, J., & Roman, P. (2008). Computer crime. American Criminal Law Review 45. 233−274.

Foster, D. (2004). Can the general theory of crime account for computer offenders:Testing low self-control as a predictor of computer crime offending. Unpublished master thesis, University of Maryland, College Park.

Higgins, D. (2007). Digital piracy: An examination of low self-control and motivation using short-term longitudinal data. *cyberpsychology & Behavior 10* , 523-529.

Higgins, G. E., & Fell, B. (2005). An application of deterrence theory to software piracy. *Journal of Criminal Justice and Popular Culture* , 166−184.

Higgins, G. E., & Ricketts, M. L. (2009). Digital piracy: A latent class analysis. *Social Science Computer Review* , 24−40.

Hoppean, w. (2008). Eurointegrated analytic hierarchy process and its applications - A literature review. *journal of operational research 186* , 211-228.

McQuade, S. (2008). Understanding and managing cybercrime. Boston, MA: Pearson National Internet Development Agency of Korea. *Survey on the computer and Internet usage. Seoul, South Korea: Ministry of Information and Communication* .

Moon, B., McCluskey, J., & McCluskey, C. (2010). A general theory of crime and computer crime: An empirical test. *Journal of Criminal Justice 38* , 767–772.

postnote. (2006).

Robert, M., & Olson, l. a. (2010). The chicago Alternative Policing Strategy, A reassessment of the CAPS program. *An International Journal of Police Strategies & Management Vol. 33 No. 4* , 586-606.

Wall, D. (2001). cybercrime and the internet. in D.S.wall(Ed). *crime and thelinternet london: Routledge* .

Wilson, D., Patterson, A., & Hembury, R. (2006). Fraud and technology crimes:Findings from the 2003/04 British Crime Survey, the 2004 offending, crime, and justice survey and administrative sources. Home Office Online Report 09/06. Retrieved from . *http://rds.homeoffice.gov.uk/rds/pdfs06/rdsolr0906.pdf*