مقاله علمی - پژوهشی

تجزیه‌وتحلیل عوامل مرتبط بر ایجاد جرائم فضای مجازی با استفاده از رویکرد فازی

حسین صیادی تورانلو،[1] سید حبیب‌الله میرغفوری،[2] محمدرضا مهدوی،[3] سپیده ثقفی[4]

پژوهش‌نامه نظم و امنیت انتظامی، سال سیزدهم، شماره سوم (پیاپی پنجاه‌ویکم)، پاییز 1399

از صفحه 27 تا 54

تاریخ دریافت: 98/12/19
تاریخ پذیرش: 99/05/14

چکیده

مقدمه: فضای مجازی فرصت بسیار مناسبی را برای ارتکاب و اختفای جرائم سایبری که تهدیدهای آن به‌مراتب در مقایسه با محیط واقعی بیشتر است، به مرتکب اعطا می‌کند. اهمیت موضوع در اینجا است که نتایج حاصل از عدم رعایت مسائل اقتصادی، اجتماعی، روانی و فنی در این حوزه، بسیاری از اصول و قواعد زندگی ما را تهدید می‌کند؛ بنابراین، لازم است که عوامل مرتبط بر ایجاد جرائم فضای مجازی در راستای ممانعت از ارتکاب جرم در فضای مجازی شناسایی و مورد تجزیه‌وتحلیل قرار گیرند.

روش: پژوهش حاضر ازنظر هدف، کاربردی و ازنظر نوع روش، توصیفی- تحلیلی است. جامعه و نمونه آماری پژوهش حاضر کلیه مدیران و کارشناسان خبره درزمینه جرائم فضای مجازی هستند. نمونه تحقیق شامل 10 نفر از خبرگان پلیس فتای یزد و دانشگاه علم و هنر است و جامعه آماری تمام شمار بوده است. در ادامه، به‌منظور جمع‌آوری داده‌ها، سه نوع پرسشنامه بین خبرگان توزیع شد. هدف از توزیع این پرسشنامه‌ها شناسایی عوامل و تبیین روابط علی بین آن‌ها بود.

یافته‌ها: عوامل سطح پایین آگاهی مردم و کاربران در مورد نحوه استفاده از فضای مجازی، نبود احساس گناه در مجرمان، نبود شغل‌های درآمدزا ازجمله عوامل تأثیرگذار هستند.

نتیجه‌گیری: تعیین عوامل تأثیرگذار بر ایجاد جرائم فضای مجازی می‌تواند در طراحی و انتخاب بهترین اقدامات و سیاست‌ها برای مدیران و تصمیم‌گیران این حوزه، مخصوصاً ناجا، مفید و اثربخش باشد.

کلیدواژه‌ها: فناوری اطلاعات، فضای مجازی، جرائم فضای مجازی، رویکرد فازی.

1- دانشیار گروه مدیریت، دانشکده علوم انسانی، دانشگاه میبد، یزد، ایران (نویسنده مسئول): h.sayyadi@meybod.ac.ir
2- دانشیار گروه مدیریت، دانشگده اقتصاد، مدیریت و حسابداری دانشگاه یزد، ایران
3- کارشناسی ارشد فناوری اطلاعات، دانشگاه علم و هنر یزد، ایران.
4- کارشناسی ارشد مدیریت دولتی، دانشگاه ولی‌عصر (عج) رفسنجان، ایران.

مقدمه

امروزه، فراگیری اینترنت و فناوری‌های جدید ارتباطی و اطلاعاتی و انقلاب ارتباطات، نوع جدیدی از ارتباطات مجازی را که خالی از روح حاکم بر روابط واقعی اجتماعی است به‌وجود آورده است. این امر موجب ظهور و شکل‌گیری فضای مجازی به‌موازات جهان واقعی شده و معادلات و الگوهای ارتباطات سنتی، تولید، انتقال و مصرف اطلاعات را به هم زده و موجب جنبش جهانی در حوزه ارتباطات و انتقال محتوا و پیام‌های ارتباطی در سریع‌ترین زمان ممکن شده است (دی کیمپ[1] و همکاران، 2020: 2؛ هالت[2] و بوسلر،[3] 2015: 68؛ پوپیللو،[4] 2018: 2؛ اومانامیو[5] و همکاران، 2019: 1224). چنین فضایی که به‌عنوان واقعیت مجازی یکپارچه، در نظر گرفته می‌شود، برخی از مهم‌ترین محدودیت‌های دست‌وپاگیر موجود در دنیای فیزیکی را از میان برده و محیط جذابی برای کاربران خود به‌وجود آورده که باعث فریب کاربران و ایجاد اعواج در نگرش‌های آنان شده است (دی کیمپ و همکاران، 2020: 3-2؛ پوپیللو، 2018: 2؛ نوریس[6] و همکاران، 2005: 4-1). از خلال بزرگ‌نمایی توانمندی‌ها یا به‌بیان‌دیگر، غرق شدن در جاذبه‌های واقعیت‌های مجازی است که زمینه بروز ناهنجاری‌های سایبری و بسیاری از جرائم در اشکال پیچیده و جدید شکل می‌گیرد و در نتیجه، شاهد پیدایش نوعی تعارض میان رفتارهای کاربران در فضای مجازی با دنیای واقعی هستیم. به‌طوری‌که در یک‌چشم بر هم زدن جرائم هولناکی در فضای مجازی رخ می‌دهد که گاهی قربانیان را تا پای مرگ می‌کشاند (فرهادی آلاشتی و جوان جعفری بجنوردی، 1396: 78-70؛ جاه‌بین و همکاران، 1397: 11-10؛ حسین‌پور و ترکمان، 1395). سرعت، کثرت، سهولت ارتکاب، ارزان بودن، بی‌مرز بودن، ناشناختگی، خودکار بودن و ... در جرائم دیجیتال‌سازی موجب ظهور گونه‌ای متمایز از جرائم شده است (دی کیمپ و همکاران، 2020: 5؛ جوان‌جعفری، 1389: 137؛ برایانز،[7] 2014: 98-93؛ شچربک،[8] 2014: 46؛

1- De Kimpe
2- Holt
3- Bossler
4- Pupillo
5- Umanailo
6- Norris
7- Bryans
8- Shcherbak

وگبرگ[1] و همکاران، 2018: 420). همچنین، گمنامی هر کاربر اینترنتی کشف و شناسایی مرتکب را بسیار دشوار ساخته است، به‌نحوی‌که این انحرافات، یکی از چالش‌های اصلی تمامی جوامع بشری شده است؛ زیرا می‌توان به تعداد فرصت‌های آن، تهدیدهای اجتماعی، اخلاقی، حقوقی و سیاسی برشمرد (دی کیمپ و همکاران، 2020: 5؛ برایانز، 2014: 98-93؛ شچربک، 2014: 46؛ کابای،[2] 2009: 3؛ کیزا،[3] 2009: 106؛ وال،[4] 2001: 3-4). جرائم فضای مجازی در ایران نیز به‌موازات سایر کشورها در حال شکل‌گیری، رشد و گسترش بوده و روزبه‌روز بر کثرت و پیچیدگی آنها افزوده می‌شود. بر اساس آخرین اعلام آمارها توسط مرکز آمار انفورماتیک قوه قضائیه طی 6 ماه اول سال 1396 تعداد پرونده‌های جرائم سایبری در کل کشور 10609 بود که بیشترین تعداد پرونده‌ها 3050 پرونده مربوط به استان تهران و 1109 پرونده مربوط به استان خراسان رضوی در رتبه دوم جرائم سایبری قرار گرفته‌اند (جاه‌بین و همکاران، 1397: 11). گستره کلان خسارات ناشی از جرائم سایبری سبب شده است تا کنگره‌های اخیر پیشگیری از جرم و عدالت کیفری سازمان ملل متحد نیز به همکاری بین‌المللی برای پیشگیری از این جرائم تأکید فراوانی کند (فرهادی آلاشتی و جوان جعفری بجنوردی، 1396: 73-70). اهمیت موضوع در اینجا است که نتایج حاصل از عدم رعایت مسائل اقتصادی، اجتماعی، روانی و فنی در این حوزه، بسیاری از اصول و قواعد اقتصادی و اجتماعی ما را تهدید می‌کند؛ بنابراین، لازم است که عوامل مرتبط بر ایجاد جرائم فضای مجازی در راستای ممانعت از ارتکاب جرم در فضای مجازی شناسایی و مورد تجزیه‌وتحلیل قرار گیرند. در این راستا، هدف پژوهش حاضر این است تا با استفاده از رویکرد فازی به بررسی و تجزیه‌وتحلیل عوامل مرتبط بر ایجاد جرائم فضای مجازی بپردازد. در این راستا، این سؤال مطرح می‌شود که روابط علت و معلولی بین عوامل مرتبط بر ایجاد جرائم فضای مجازی چگونه است؟

1- Wegberg
2- Kabay
3- Kizza
4- Wall

پیشینه و مبانی نظری پژوهش

پیشینه پژوهش

چنگ[1] و همکاران (2020)، به ارزیابی تفاوت‌های فردی در بزهکاری سایبری و پیامدهای روانی آن پرداختند. یافته‌ها نشان داد که تشدید خطرات مربوط به بزهکاری سایبری است؛ زیرا میزان استفاده از فناوری اطلاعات و مهارت IT کاربران در حال افزایش است و برنامه‌های مبتنی بر شواهد برای افزایش آگاهی کاربران از شیوع جرائم سایبری و ایجاد مقاومت در برابر حملات سایبری مورد نیاز است.

اومانامیو و همکاران (2019)، به بررسی جرائم اینترنتی به‌عنوان تأثیر توسعه فناوری‌های ارتباطی بر نگرانی جامعه پرداختند. آنان اذعان داشتند که جرائم سایبری بدون قواعد و هنجارها به یک فضای آنارشیستی تبدیل می‌شود. بارتومومی[2] (2018)، جرائم سایبری و رایانش ابری را مورد بررسی قرار داد. در این تحقیق چندین سناریو با سطوح مختلف امنیت داده‌ها و پیگرد عمومی هکر مورد تجزیه‌وتحلیل قرار گرفت.

چانگ[3] و همکاران (2018)، پژوهشی با موضوع خودیاری، هوشیاری و جرائم سایبری انجام دادند. نتایج تحقیق آنها نشان داد که با توجه به منابع و توانایی‌های محدود ایالات برای حفظ امنیت سایبری، اقدامات مختلف همزمانی توسط افراد یا جمعی با درجه‌های مختلف سازمان‌دهی و هماهنگی انجام‌شده است.

محمدی برزگر و همکاران (1398)، در پژوهشی به شناسایی ابعاد و مؤلفه‌های پیشگیری از جرائم علیه عفت و اخلاق عمومی در فضای مجازی پرداختند. نتایج تحقیق نشان داد که پیشگیری از جرائم علیه عفت و اخلاق عمومی در فضای مجازی نیازمند فرایندی بهم پیوسته از ایجاد و مؤلفه‌ها است.

داودی دهاقانی (1398)، در مطالعه‌ای به بررسی موانع اساسی تحقق پیشگیری از جرائم سایبر پرداختند. نتایج پژوهش حاکی از آن بود که برای پیشگیری از جرائم فضای سایبر، در دو سطح می‌توان نسبت به حذف موانع اقدام کرد: نخست، با تدابیر

1- Cheng
2- Bartholomae
3- Chang

راهبردی و بلندمدت و دوم، به‌صورت مستقیم از طریق اقدامات ایجابی یا سلبی.

جاه‌بین و همکاران (1397)، در پژوهشی عوامل مؤثر بر ارتکاب جرم در فضای مجازی از دیدگاه قضات دادسرا جرائم رایانه‌ای تهران را مورد واکاوی قرار دادند. از دیدگاه قضات، عوامل گمنامی و سهل‌الوصول بودن، فراگیر بودن، جذابیت‌های فضای مجازی، مهم‌ترین دلایل ارتکاب جرائم سایبری بودند.

فتاحی (1397)، به بررسی عناصر تشکیل‌دهنده مادی و معنوی مصادیق جرائم رایانه‌ای اقدام و جرائم رایانه‌ای را تبیین کردند. کرمی (1397)، سیاست کیفری افتراقی در قلمرو ارکان متشکله جرائم سایبری را بررسی کردند. نتایج نشان داد که منطق حاکم بر حقوق کیفری ماهوی جرائم سایبری در بسیاری از موارد متفاوت از جرائم سنتی است.

جاه‌بین و همکاران (1397)، به مطالعه کیفی عوامل ارتکاب جرائم در فضای مجازی پرداختند. آن‌ها عوامل را در 5 دسته اصلی عوامل فردی و شخصیتی بزه‌کار، عوامل فردی و شخصیتی بزه‌دیده، عوامل اقتصادی، عوامل اجتماعی، عوامل مذهبی و اعتقادی طبقه‌بندی کردند.

کردعلیوند و همکاران (1397)، پژوهشی با عنوان «گونه‌شناسی جرائم سایبری با نگاهی به قانون جرائم رایانه‌ای و آمار پلیس فتا» انجام دادند. آنها ابتدا به تبیین دو گونه‌شناسی از جرائم سایبری پرداخته و سپس، وضعیت بزه‌کاری سایبری در کشور ایران را بررسی کردند. صابرنژاد و حسین‌پور (1396)، تحلیل حقوقی گونه‌شناسی نقض حریم خصوصی در فضای سایبر را بررسی کردند.

بررسی پژوهش‌های پیشین نشان می‌دهد که تاکنون به‌صورت مستقیم تمام ابعاد عوامل مرتبط بر ایجاد جرائم فضای مجازی در محیط فازی مورد بررسی قرار نگرفته است. ضمن اینکه، پژوهش‌ها و مطالعات موجود هر کدام به بخشی از جرائم سایبری پرداخته‌اند و نگاه کلان و راهبردی در این تحقیقات نیز کمرنگ است؛ پژوهش حاضر تلاش کرده است تا خلأ پژوهشی موجود را پرکند.

مبانی نظری پژوهش

جرائم سایبری در اصطلاح، به جرائمی گفته می‌شود که در محیطی غیرفیزیکی علیه فناوری اطلاعات با حالات شبیه‌سازی و مجازی‌سازی ارتکاب می‌یابند (صابرنژاد و حسین‌پور، 1396: 4-3؛ وطنی و اسدی، 1395: 101؛ آن[1] و کیم،[2] 2018: 26636؛ بارتومومی، 2018: 297؛ چانگ و همکاران، 2018: 102). امروزه، بسیاری از جرائم سنتی، همزمان با پیشرفت فناوری اطلاعات و ارتباطات به‌شدت متحول شده و به جرائم سایبری تبدیل‌شده‌اند. جرائم سایبری نیز به جهت گسترش خود، رفته‌رفته جانشین عباراتی چون جرم‌های رایانه‌ای و جرم‌های اینترنتی می‌شوند (اومانامیو و همکاران، 2019: 1224؛ برایانز، 2014: 95؛ وگبرگ و همکاران، 2018: 420؛ صابرنژاد و حسین‌پور، 1396: 4-3؛ وطنی و اسدی، 1395: 102-101؛ آن و کیم، 2018: 26636). عطف توجه به تعاریفی که ارائه شده است می‌توان مسئله‌ای همچون غیرفیزیکی بودن این محیط را خصیصه بارز آن نامید. با این حال، می‌توان ویژگی‌های دیگری نظیر دست‌یابی کاربران به هرگونه خدمات اطلاعات الکترونیکی، ارتباط کاربر با کاربران دیگر و انجام دادن معاملات تجاری در سطح بین‌المللی بدون خالت فرد برای آن برشمرد (اومانامیو و همکاران، 2019: 1225؛ برایانز، 2014: 96؛ شچربک، 2014: 46؛ وگبرگ و همکاران، 2018: 420؛ رضوی، 1386: 125؛ صابرنژاد و حسین‌پور، 1396: 4-3). امروزه، این فضا از اهمیت شایانی برخوردار است؛ کلیه بخش‌های اقتصادی تمامی کشورها، ازجمله امکانات دولتی و خصوصی، بانکداری و امور مالی، حمل‌ونقل، تولید، پزشکی، آموزش‌وپرورش، دولت، همگی برای انجام عملیات روزانه وابسته به رایانه هستند (اومانامیو و همکاران، 2019: 1225؛ وگبرگ و همکاران، 2018: 420؛ چنگ و همکاران، 2020: 1؛ رضوی، 1386: 121؛ صابرنژاد و حسین‌پور، 1396: 6-3). برخی معتقدند اگرچه فضای سایبری چالش‌های جدیدی را پدید آورده است، اما مکانیسم‌های زیرین ارتکاب جرم در فضای مجازی همانند جهان واقعی است. این دسته از محققان جرائم نوظهور سایبری را با استفاده از نظریه‌های سنتی تبیین کرده‌اند و در این میان، نظریه خودکنترلی، نظریه یادگیری اجتماعی و نظریه سبک زندگی-

1- An
2- Kim

فعالیت‌های روتین- بیشترین سهم را داشته‌اند (جاه‌بین و همکاران، 1397: 13؛ نالا،[1] 2014: 4)؛ اما برخی دیگر نیز به تدوین نظریه‌های جدید یا بازنویسی نظریه‌های قدیمی اعتقاددارند؛ چراکه تصور می‌کنند جرائم سایبری نوع جدیدی از جرائم هستند (جاه‌بین و همکاران، 1397؛ نالا، 2014؛ کردعلیوند و میرزایی، 1397). این دو دیدگاه منجر به تعاریف مختلفی از جرائم سایبری نیز شده است. از میان تعاریف متعدد ارائه‌شده از جرائم سایبری، به نظر می‌رسد که تعریف به‌کاررفته توسط مک گوئیر و داولینگ، تعریفی کامل و جامع باشد. آنها جرائم سایبری را به‌عنوان مفهومی چتری تعریف می‌کنند که دو نوع فعالیت مجرمانه کاملاً متمایز ولی مربوط به هم را پوشش می‌دهد؛ جرائم وابسته به فضای سایبری و جرائم ممکن شده توسط فضای سایبری (جاه‌بین و همکاران، 1397: 13؛ مک‌گور[2] و دولینگ،[3] 2013: 3).

الف) جرائم وابسته به فضای سایبری: این نوع از جرائم تنها با استفاده از رایانه، شبکه‌ها رایانه‌ای یا اشکال دیگری از فناوری اطلاعات و ارتباطات انجام می‌گیرند. فعالیت‌هایی نظیر ویروس‌ها و سایر بدافزارها، هک کردن، حملات پخش DDOS مصادیقی از این نوع جرائم هستند (اومانامیو و همکاران، 2019: 1225؛ جاه‌بین و همکاران، 1397: 13-11؛ برایانز، 2014: 93-98؛ سوخای،[4] 2004: 2؛ وال، 2008: 45).

ب) جرائم ممکن شده توسط فضای سایبری: برخلاف جرائم وابسته به فضای سایبری، این نوع از جرائم هنوز هم بدون استفاده از فناوری اطلاعات و ارتباطات قابل ارتکاب هستند. جرائمی نظیر کلاه‌برداری‌های مالی اینترنتی، فیشینگ، فارمینگ و... ازاین‌دست جرائم هستند (اومانامیو و همکاران، 2019: 1225؛ جاه‌بین و همکاران، 1397: 13-11؛ برایانز، 2014: 98-93؛ سوخای، 2004: 2؛ وال، 2008: 45). طبق آمار منتشرشده در اینترنت در سال 2009، ایالات‌متحده آمریکا با 23 درصد، بیشترین جرائم رایانه‌ای را داشته است. چین با 9 درصد در رده دوم، آلمان با 6 درصد در رده سوم و بریتانیا با 5 درصد در رده چهارم قرار دارند. به‌هرحال، وسعت رخداد جرائم رایانه‌ای در زمان کنونی به حدی است که همه باید مراقب امنیت رایانه‌ای خود باشند.

1- Nalla
2- McGuire
3- Dowling
4- Sukhai

بیشترین میزان شکایت‌های رایانه‌ای و اینترنتی از سال 2000 تا 2010 در امریکا به تجارت الکترونیکی مربوط می‌شود که شامل حراج آنلاین و کارت‌های اعتباری است. همچنین، شکایت مربوط به دزدی هویت از سال 2009 به بعد افزایش داشته است. البته برخی ادعا می‌کنند که آمار گزارش درباره جرائم رایانه‌ای، واقعی و قابل‌اعتماد نیست، چون تعدادی از جرم‌ها به دلیل مشکلات مربوط به اثبات جرم گزارش نمی‌شوند. مهم‌ترین جرم اینترنتی که هم‌اکنون برای کاربران به بحران تبدیل‌شده سرقت هویت است که آنها را مجبور به تغییر هویت به سمت هویت دیجیتالی کرده است (اومانامیو و همکاران، 2019: 1225؛ وگبرگ همکاران، 2018: 420؛ چنگ و همکاران، 2020: 2؛ آن و کیم، 2018: 26636).

با توجه به بررسی ادبیات نظری و پژوهش‌های پیشین حول جرائم سایبری عوامل مرتبط بر ایجاد جرائم فضای مجازی به شرح جدول شماره(1) هستند:

جدول 1: عوامل مرتبط بر جرائم فضای مجازی

عوامل	شاخص‌ها	منابع
فرهنگی اجتماعی	سطح پایین آگاهی مردم و کاربران در مورد نحوه استفاده از فضای مجازی	مسعودیان، 1391
	افزایش روزافزون تعداد کاربران و به‌تبع آن، افزایش تعداد مجرمان و قربانیان	بیات‌پور، 1396
	فقر فرهنگی و عدم پایبندی به ارزش‌های جامعه و باورهای دینی	سپهری و همکاران، 1394
	هم‌نشینی با دوستان ناباب	برودهرست و همکاران، 2014
	نحوه گذراندن اوقات فراقت (بیکاری جوانان)	آریف و همکاران، 2015
اقتصادی	کمبود درآمد	لاگازیو و همکاران، 2014
	افزایش روزافزون هزینه‌ها	مسعودیان، 1391
	نبود شغل‌های درآمدزا	بیات‌پور، 1396؛ آریف و همکاران، 2015
روحی روانی	مشکلات روحی و روانی بزهکاران فضای مجازی همچون حسادت و انتقام‌جویی	سپهری و همکاران، 1394؛ لاگازیو و همکاران، 2014
	اعتیاد به اینترنت	برودهرست و همکاران، 2014
	نبود احساس گناه در مجرمان	مسعودیان، 1391؛ سپهری و همکاران، 1394؛ آریف و همکاران، 2015
فنی	اشکالات ساختار فنی فضای مجازی	بیات‌پور، 1396؛ لاگازیو و همکاران، 2014
	سهولت ارتکاب جرم مجازی و پنهان ماندن	سپهری و همکاران، 1394؛ برودهرست و همکاران، 2014

روش‌شناسی

این تحقیق که عوامل مرتبط بر ایجاد جرائم فضای مجازی را با استفاده از منابع علمی و اطلاعات حاصل از دیدگاه نمونه تحقیق و از طریق روش‌های تصمیم‌گیری چندمعیاره (AHP و DEMATEL) در محیط فازی را مورد تجزیه‌وتحلیل قرار می‌دهد، ازنظر هدف، کاربردی و ازنظر نوع روش، توصیفی- تحلیلی است. جامعه و نمونه آماری پژوهش حاضر، کلیه مدیران و کارشناسان خبره در زمینه جرائم فضای مجازی می‌باشند. با توجه به تخصصی بودن موضوع و با عنایت به اینکه جامعه آماری خبره در این حوزه محدود است، لذا نمونه تحقیق در این بخش، تعداد 10 نفر از خبرگان پلیس فتای یزد و دانشگاه علم و هنر است و جامعه آماری تمام شمار بوده است. در این تحقیق ابتدا تمامی عوامل مرتبط بر ایجاد جرائم فضای مجازی از ادبیات مربوطه استخراج و سپس، بر اساس نظرسنجی از خبرگان و اساتید دانشگاهی این معیارها مورد بررسی، اصلاح و بعضاً حذف یا تعدیل شد. به‌عبارت‌دیگر، روایی محتوای مورد تأیید قرار گرفت. در ادامه، به‌منظور جمع‌آوری داده‌ها، سه نوع پرسشنامه بین خبرگان توزیع شد. هدف از توزیع پرسشنامه اول، شناسایی و رسیدن به اتفاق‌نظر درباره عوامل مرتبط بر ایجاد جرائم فضای مجازی بوده است. پرسشنامه نوع دوم، برای تعیین اهمیت عوامل شناسایی‌شده و پرسشنامه نوع سوم، برای بررسی روابط میان عوامل بوده است. فرایند تحقیق شامل سه فاز به شرح زیر است.

فاز اول: شناسایی عوامل بر اساس ادبیات تحقیق و مطالعات مشابه و نظرسنجی از خبرگان: در این مرحله، ابتدا با بررسی ادبیات نظری و پژوهش‌های پیشین حول جرائم سایبری و نظرسنجی از خبرگان، عوامل نهایی تعیین شد.

فاز دوم: وزن‌دهی عوامل با استفاده از تکنیک AHP فازی: در تحقیق حاضر، از روش AHP فازی بوکلی[1] (1985) جهت تعیین وزن عوامل استفاده شده است. با این روش، ماتریس مقایسات زوجی با استفاده از اعداد فازی مثلثی (l, m, u) تشکیل می‌شود. مراحل تکنیک AHP فازی بوکلی (1985) به شرح زیر هستند:

1- Buckley

گام اول. رسم نمودار سلسله‌مراتبی: بر اساس عوامل مرتبط بر پیاده‌سازی جرائم فضای مجازی نمودار سلسله‌مراتبی ترسیم می‌شود.

گام دوم. تشکیل ماتریس مقایسات زوجی با استفاده از اعداد فازی: در این مرحله، از خبرگان درخواست می‌شود تا نظرات خود را در مورد مقایسه زوجی عوامل مذکور، با استفاده از عبارات کلامی جدول شماره (2) بیان کنند.

جدول 2: مقیاس اولویت‌بندی اعداد فازی مثلثی (بزبورا[1] و همکاران، 2007: 1105)

کد	عبارات کلامی	عدد فازی
1	ترجیح کاملاً برابر	(1,1,1)
2	ترجیح تقریبا برابر	(0.5,1,1.5)
3	ترجیح کم	(1,1.5,2)
4	ترجیح زیاد	(1.5,2,2.5)
5	ترجیح خیلی زیاد	(2,2.5,3)
6	ترجیح کاملاً زیاد	(2.5,3,3.5)

پس از گردآوری نظرات خبرگان و تبدیل داده‌های کلامی به اعداد فازی، ماتریس مقایسات زوجی با استفاده از رابطه (1) تشکیل می‌شود.

$$\tilde{A}=\begin{bmatrix}1 & \tilde{a}_{12} & \cdots & \tilde{a}_{1n}\\ \tilde{a}_{12} & 1 & \cdots & \tilde{a}_{2n}\\ \vdots & \vdots & \ddots & \vdots\\ \tilde{a}_{n2} & \tilde{a}_{n2} & \cdots & 1\end{bmatrix}=\begin{bmatrix}1 & \tilde{a}_{12} & \cdots & \tilde{a}_{1n}\\ 1/\tilde{a}_{12} & 1 & \cdots & \tilde{a}_{2n}\\ \vdots & \vdots & \ddots & \vdots\\ 1/\tilde{a}_{1n} & 1/\tilde{a}_{2n} & \cdots & 1\end{bmatrix} \quad (1)$$

گام سوم. محاسبه میانگین هندسی مقایسات زوجی خبرگان: میانگین هندسی مقایسات زوجی خبرگان با استفاده از رابطه (2) به دست می‌آید:

$$\tilde{a}_{ij}=(\tilde{a}_{ij}^{1}\otimes\tilde{a}_{ij}^{2}\otimes\ldots\otimes\tilde{a}_{ij}^{n})^{\frac{1}{n}} \quad (2)$$

گام چهارم. محاسبه وزن‌های فازی: وزن فازی هر شاخص از رابطه (3) به دست می‌آید.

1- Bozbura

$$\tilde{w}_j = \tilde{a}_j \otimes (\tilde{a}_1 \oplus \tilde{a}_2 \oplus ... \oplus \tilde{a}_n)^{-1} \quad j = 1,2,...,n \qquad (3)$$

j تعداد شاخص‌ها است.

گام پنجم. دی‌فازی و نرمالایز کردن وزن‌های به‌دست‌آمده: برای نرمالایز کردن وزن‌های فازی مثلثی از رابطه (4) استفاده می‌شود (وانگ،[1] 2009: 229).

$$W_j = \frac{a+b+c}{3} \qquad (4)$$

فاز سوم: تبیین ارتباط میان عوامل با تکنیک DEMATEL **فازی**

روش دیمتل اولین بار توسط دو پژوهشگر به نام‌های فونتلا و گابوس[2] در سال 1976 ارائه شد. این تکنیک از انواع روش‌های تصمیم‌گیری بر اساس مقایسه‌های زوجی است. این تکنیک علاوه بر تبدیل روابط علت و معلولی به یک مدل ساختاری- بصری، قادر است وابستگی‌های درونی بین عوامل را نیز شناسایی و آنها را قابل‌فهم کند (وو،[3] 2008: 830). بااین‌حال، به‌طورکلی، برآورد نظر خبرگان با مقادیر عددی دقیق، مخصوصاً در شرایط عدم قطعیت، بسیار دشوار است، چراکه نتایج تصمیم‌گیری به‌شدت به داوری‌های ذهنی غیردقیق و مبهم وابسته است. این عامل باعث نیاز به منطق فازی در دیمتل شده است (عبدلله و زولکیفلی،[4] 2015: 4398). مراحل این تکنیک به شرح زیر است.

گام ششم. ایجاد ماتریس اولیه روابط مستقیم (A): پرسشنامه مربوط به سطح نفوذ هر شاخص به دیگر شاخص‌ها تهیه و بین خبرگان توزیع می‌شود و پس از جمع‌آوری نظرات خبرگان و با استفاده از جدول شماره (3)، داده‌های کلامی به اعداد فازی تبدیل شده و با استفاده از رابطه (5) ماتریس اولیه روابط مستقیم تعیین می‌شود.

1- Wang
2- Fontela & Gabus
3- Wu
4- Abdullah & Zulkifli

جدول 3: الگوی مقیاس کلامی فازی تأثیر هر متغیر در متغیر دیگر (بایکسوگلو[1] و همکاران، 2013: 902)

عبارت کلامی	مقدار فازی
بدون تأثیر	(1,000, 1,000, 1,000)
تأثیر خیلی کم	(2,000, 3,000, 4,000)
تأثیر کم	(4,000, 5,000, 6,000)
تأثیر زیاد	(6,000, 7,000, 8,000)
تأثیر خیلی زیاد	(8,000, 9,000, 9,000)

$$A_{ij} = \frac{1}{H}\sum_{k=1}^{H} x_{ij}^{k} \qquad (5)$$

گام هفتم. نرمالایز کردن ماتریس اولیه روابط مستقیم (D): ماتریس اولیه روابط مستقیم با استفاده از روابط (6) و (7) به دست می‌آید.

$$D = \frac{A}{S} \qquad (6)$$

$$S = \max\left(\max_{1\le i\le n}\sum_{j=1}^{n} A_{ij} , \max_{1\le i\le n}\sum_{i=1}^{n} A_{ij} \right) \qquad (7)$$

گام هشتم. ساختن ماتریس $Z = [Z_x]$: با استفاده از رابطه (8) ماتریس Z_x ساخته می‌شود.

$$Z_x = \begin{bmatrix} 0 & x_{12} & \cdots & x_{1n} \\ x_{21} & 0 & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \cdots & 0 \end{bmatrix} \qquad (8)$$

بر اساس $x = (a,b,c)$ از ماتریس فوق، سه ماتریس $n \times n$ به دست می‌آید. علت نوشتن ماتریس D به‌صورت سه ماتریس، سهولت در انجام محاسبات در گام بعدی است.

1- Baykasog˘lu

گام نهم. تبیین ماتریس روابط کل (T_x): ماتریس روابط کل شاخص‌ها با استفاده از رابطه (9) به دست می‌آید که در آن I ماتریس همانی است.

$$T_x = Z_x (I - Z_x)^{-1} \quad (9)$$

گام دهم. تحلیل روابط علی: مجموع مقادیر سطرها و ستون‌ها را برای تحلیل روابط علی به دست آورده و برای تعیین مقادیر $D+R$ و $D-R$ فازی از روابط (10-12) استفاده می‌شود.

$$T_X = \lfloor t_{ij} \rfloor_{m\times n} \qquad i, j = 1,2,\ldots,n \quad (10)$$

$$D = r_X = \left[\sum_{j=1}^{n} t_{ij}\right]_{n\times 1=[t_i]n\times 1} \quad (11)$$

$$R = c_X = \left[\sum_{j=1}^{n} t_{ij}\right]_{1\times n=[t_i]1\times n} \quad (12)$$

گام یازدهم. محاسبه مقادیر قطعی روابط علی $E(\varpi)$: برای مقادیر $\tilde{D}+\tilde{R}$ و $\tilde{D}-\tilde{R}$ فازی به‌دست‌آمده در گام قبلی، مقادیر قطعی با استفاده از روش مرکز ناحیه مطابق رابطه (13) به دست می‌آید.

$$E(\varpi) = \frac{a+b+c}{3} \quad \varpi = \tilde{D}-\tilde{R} \;\; or \;\; \varpi = \tilde{D}+\tilde{R} \quad (13)$$

که در آن a,b,c درایه‌های مربوطه به مقادیر فازی $D+R$ و $D-R$ می‌باشند.

گام دوازدهم. ترکیب کردن وزن‌های فازی و $E(\varpi)$: وزن‌های فازی به‌دست‌آمده از گام چهارم از فاز اول (وزن‌های به‌دست‌آمده از روش AHP در فاز قبلی) را در مقادیر $E(\varpi)$ مربوط به هر شاخص ضرب می‌شود تا مقادیر جدید به دست آید برای این کار از رابطه (14) استفاده می‌شود.

$$E(\varpi)_{new} = w_j \otimes E(\varpi) \quad (14)$$

گام سیزدهم. طراحی نمودار علی: نمودار علی مربوط به‌تمامی شاخص‌ها ترسیم می‌شود.

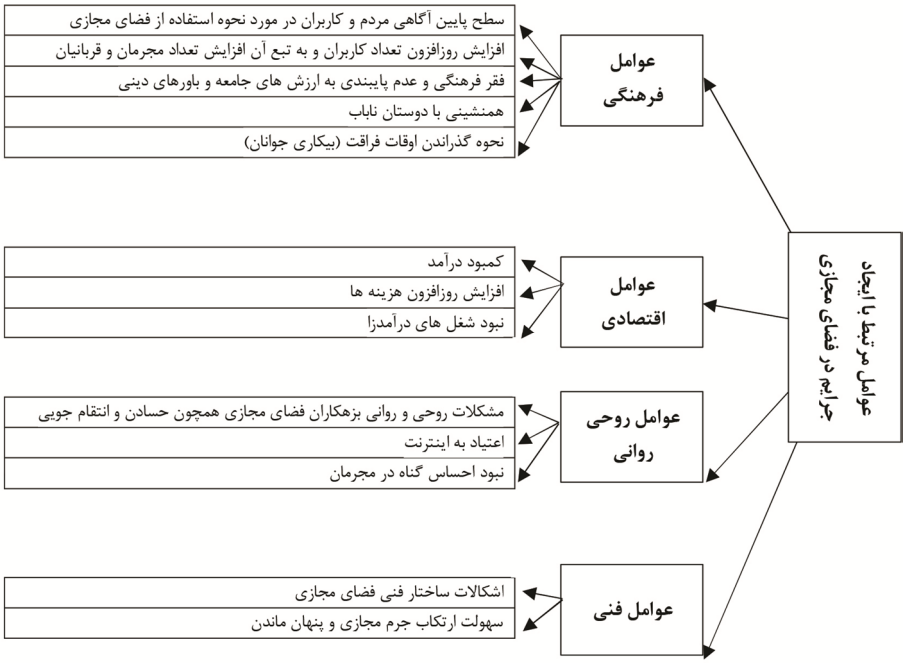
یافته‌های پژوهش

در این بخش بر اساس فرایند تحقیق، یافته‌های پژوهش ارائه شده است.

فاز اول. شناسایی عوامل بر اساس ادبیات تحقیق و مطالعات مشابه و نظرسنجی از خبرگان: با بررسی ادبیات تحقیق و نظرسنجی از خبرگان درمجموع 13 شاخص در چهار حوزه تعیین شد (شکل 1).

فاز دوم. تعیین اوزان معیارها با استفاده از تکنیک AHP فازی

گام اول. ترسیم درخت سلسله‌مراتبی: درخت سلسله‌مراتبی تحقیق دارای سه سطح به شرح شکل (1) است.



شکل 1: درخت سلسله‌مراتبی عوامل مؤثر بر ایجاد جرائم در فضای مجازی

گام دوم. تشکیل ماتریس مقایسات زوجی: برای نمونه ماتریس مقایسات زوجی عوامل اصلی نسبت به هدف در جدول (4) نشان داده شده است. برای محاسبه سازگاری

ماتریس مقایسات زوجی از روش گوگوس و بوچر[1] (1998) استفاده شد. نتایج حاکی از سازگار بودن جداول مقایسات زوجی بود.

جدول 4: میانگین مقایسات زوجی عوامل اصلی بر اساس هدف

	فرهنگی اجتماعی	اقتصادی	روحی روانی	فنی	میانگین هندسی
فرهنگی اجتماعی	(1,1,1)	(0.794,1.31,1.817)	(0.874,1,1.26)	(0.794,1.31,1.817)	(0.861,1.145,1.428)
اقتصادی	(0.55,0.763,1.26)	(1,1,1)	(0.667,1,2)	(0.794,1.145,1.442)	(0.735,0.967,1.381)
روحی روانی	(0.794,1,1.145)	(0.5,1,1.5)	(1,1,1)	(1.145,1.651,2.154)	(0.821,1.134,1.387)
فنی	(0.55,0.763,1.26)	(0.693,0.874,1.26)	(0.464,0.606,0.874)	(1,1,1)	(0.649,0.797,1.085)
مجموع					(3.066,4.042,5.281)

CR^m=0.007 CR^E=0.037

سازگار

گام سوم. محاسبه میانگین هندسی مقایسات زوجی خبرگان: بر اساس رابطه (2)، میانگین هندسی مقایسات زوجی خبرگان در هر یک از پنج ماتریس مقایسات زوجی تعیین می‌شود. میانگین هندسی عوامل اصلی مرتبط با ایجاد جرائم در فضای مجازی در ستون آخر جدول (4) نشان داده‌شده است.

گام چهارم. محاسبه وزن‌های فازی: در این مرحله مقادیر به‌دست‌آمده از گام سوم بر اساس رابطه (3) نرمالیزه می‌شود. جدول (5)، وزن‌های فازی عوامل و شاخص‌های را نشان می‌دهد.

1- Gogus and Boucher

جدول 5: محاسبه وزن‌های فازی و قطعی عوامل و شاخص‌های مرتبط با ایجاد جرائم در فضای مجازی

عوامل	وزن‌های فازی/ قطعی	شاخص	وزن‌های نهایی فازی	وزن قطعی مؤلفه‌ها
فرهنگی اجتماعی	(0.163,0.283,0.466) (0,299)	سطح پایین آگاهی مردم و کاربران	(0.02,0.06,0.174)	0.079
		افزایش روزافزون تعداد کاربران	(0.024,0.068,0.181)	0.085
		فقر فرهنگی	(0.019,0.056,0.156)	0.072
		هم‌نشینی با دوستان ناباب	(0.017,0.048,0.137)	0.062
		نحوه گذراندن اوقات فراقت	(0.018,0.051,0.136)	0.064
اقتصادی	(0.139,0.239,0.45) (0,267)	کمبود درآمد	(0.036,0.083,0.222)	0.106
		افزایش روزافزون هزینه‌ها	(0.031,0.082,0.226)	0.105
		نبود شغل‌های درآمدزا	(0.033,0.074,0.179)	0.09
روحی روانی	(0.155,0.28,0.452) (0,292)	مشکلات روحی و روانی بزهکاران	(0.037,0.11,0.287)	0.136
		اعتیاد به اینترنت	(0.029,0.082,0.212)	0.101
		نبود احساس گناه در مجرمان	(0.03,0.089,0.232)	0.11
فنی	(0.123,0.197,0.354) (0,218)	اشکالات ساختار فنی	(0.039,0.083,0.198)	0.1
		سهولت ارتکاب جرم مجازی	(0.054,0.115,0.273)	0.139

گام پنجم. دیفازی کردن: در این مرحله اوزان فازی به‌دست‌آمده، طبق رابطه (4) دیفازی می‌شوند. با انجام این محاسبات، اوزان نهایی عوامل و شاخص‌ها تعیین می‌شود. نتایج در جدول (5)، نشان داده شده است.

فاز دوم: تعیین ارتباط میان معیارها با استفاده از تکنیک دیمتل فازی:

گام ششم. ایجاد ماتریس اولیه روابط مستقیم (A): پس از جمع‌آوری نظرات خبرگان و با استفاده از جدول (3)، با استفاده از رابطه (5) ماتریس تجمیعی نظرات خبرگان به شرح جدول (6) تعیین شد.

جدول 6: ماتریس تجمیعی نظرات خبرگان

	C_1	C_2	...	C_{12}	C_{13}
C_1	(0.000,0.000,0.000)	(4.000,5.000,6.000)		(6.667,7.667,8.333)	(6.000,7.000,8.000)
C_2	(2.000,3.000,4.000)	(0.000,0.000,0.000)		(6.000,7.000,8.000)	(2.667,3.667,4.667)
⋮	⋮	⋮		⋮	⋮
C_{12}	(5.333,6.333,7.333)	(6.000,7.000,7.333)		(0.000,0.000,0.000)	(8.000,9.000,9.000)
C_{13}	(4.000,5.000,6.000)	(6.000,7.000,8.000)		(5.333,6.333,7.000)	(0.000,0.000,0.000)

گام هفتم: نرمالایز کردن ماتریس اولیه روابط مستقیم (D): ماتریس اولیه روابط مستقیم با استفاده از روابط (7-6) به شرح جدول (7) به دست آمد.

جدول 7: ماتریس نرمالایز شده روابط درونی شاخص‌های مرتبط با ایجاد جرائم مجازی

	C_1	C_2	...	C_{12}	C_{13}
C_1	(0.000,0.000,0.000)	(0.047,0.059,0.071)		(0.078,0.090,0.098)	(0.071,0.082,0.094)
C_2	(0.024,0.035,0.047)	(0.000,0.000,0.000)		(0.071,0.082,0.094)	(0.031,0.043,0.055)
⋮	⋮	⋮		⋮	⋮
C_{12}	(0.063,0.075,0.086)	(0.071,0.082,0.086)		(0.000,0.000,0.000)	(0.094,0.106,0.106)
C_{13}	(0.047,0.059,0.071)	(0.071,0.082,0.094)		(0.063,0.075,0.082)	(0.000,0.000,0.000)

گام هشتم: ساختن ماتریس $Z = [Z_x]$ **:** با استفاده از رابطه 8 ماتریس Z_x ساخته می‌شود.

گام نهم: تبیین ماتریس روابط کل (T_x): ماتریس روابط کل شاخص‌ها با استفاده از رابطه (9) به شرح جدول (8) تعیین شد.

جدول 8: ماتریس T شاخص‌های مرتبط با ایجاد جرائم مجازی

	C_1	C_2	...	C_{12}	C_{13}
C_1	(0.081,0.203,0.613)	(0.136,0.279,0.729)	...	(0.176,0.327,0.801)	(0.182,0.346,0.847)
C_2	(0.092,0.214,0.601)	(0.078,0.197,0.602)	...	(0.153,0.291,0.731)	(0.130,0.280,0.742)
⋮	⋮	⋮		⋮	⋮
C_{12}	(0.131,0.254,0.647)	(0.148,0.280,0.693)	...	(0.092,0.222,0.659)	(0.189,0.341,0.800)
C_{13}	(0.122,0.249,0.650)	(0.153,0.289,0.719)	...	(0.154,0.299,0.753)	(0.107,0.255,0.724)

گام دهم: تحلیل روابط علی: با استفاده از روابط (12-9) مقادیر $\tilde{D}+\tilde{R}$ و $\tilde{D}-\tilde{R}$ فازی به شرح جدول (9) تعیین شد.

جدول 9: مقادیر فازی و قطعی D+R **و** D-R

شاخص‌ها	$\tilde{D}_i+\tilde{R}_i$	$\tilde{D}_i-\tilde{R}_i$	$(\tilde{D}_i+\tilde{R}_i)^{def}$	$(\tilde{D}_i-\tilde{R}_i)^{def}$
C_1	(3.434,7.007,18.255)	(-6.232,0.886,8.589)	8.925	1.032
C_2	(3.351,6.871,18.007)	(-7.172,0.143,7.483)	8.775	0.149
C_3	(3.851,7.690,19.688)	(-8.748,-0.658,7.089)	9.730	-0.744
C_4	(3.589,7.260,18.892)	(-7.696,-0.086,7.607)	9.250	-0.066
C_5	(3.850,7.689,19.457)	(-7.232,0.484,8.375)	9.671	0.528
C_6	(3.176,6.583,17.333)	(-7.957,-0.745,6.200)	8.419	-0.811
C_7	(3.667,7.387,19.025)	(-8.272,-0.372,7.087)	9.366	-0.482
C_8	(3.690,7.426,19.219)	(-7.206,0.376,8.323)	9.440	0.467
C_9	(3.411,6.969,18.352)	(-7.807,-0.275,7.135)	8.925	-0.305
C_{10}	(3.546,7.189,18.573)	(-7.475,0.007,7.552)	9.124	0.023
C_{11}	(3.936,7.829,19.704)	(-7.175,0.587,8.593)	9.825	0.648
C_{12}	(3.582,7.248,18.817)	(-7.745,-0.048,7.490)	9.224	-0.088
C_{13}	(3.919,7.801,19.753)	(-8.320,-0.300,7.514)	9.818	-0.351

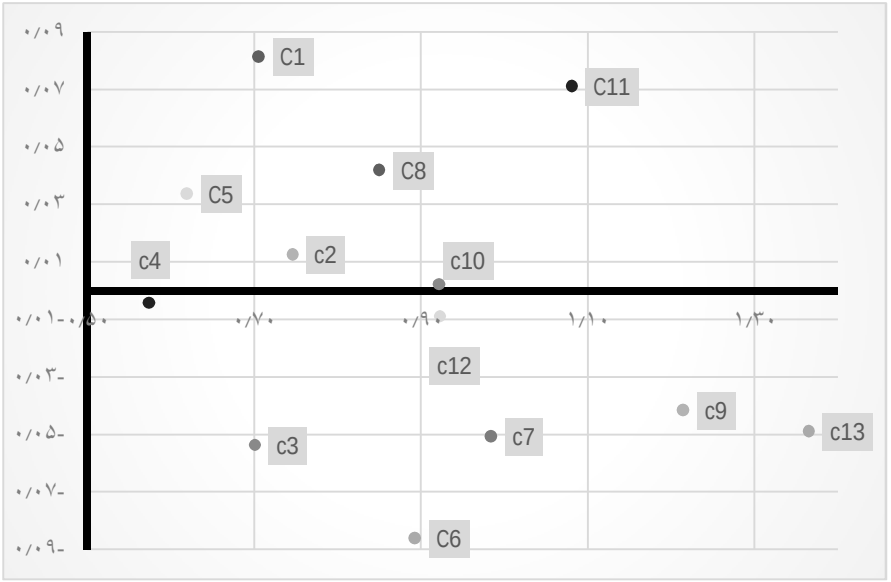
گام یازدهم: محاسبه مقادیر قطعی $E(\varpi)$: با استفاده از رابطه (13)، مقادیر قطعی $D+R$ و $D-R$ تعیین شد (جدول 9).

گام دوازدهم. ترکیب کردن وزن‌های فازی و $E(\varpi)$: با ضرب نمودن وزن‌های شاخص‌ها (جدول 4) در مقادیر قطعی $D+R$ و $D-R$ یعنی $E(\varpi)$(جدول 8)، مقادیر جدید $E(\varpi)_{new}$ مربوط به هر شاخص مطابق رابطه (14)، به شرح جدول (10)، تعیین می‌شود.

جدول 10: مقادیر $E(\varpi)_{new}$ شاخص‌های مرتبط با ایجاد جرائم در فضای مجازی

	شاخص	$(D+R)_{new}$	$(D-R)_{new}$
C1	سطح پایین آگاهی مردم و کاربران در مورد نحوه استفاده از فضای مجازی	0.705	0.082
C2	افزایش روزافزون تعداد کاربران و به‌تبع آن افزایش تعداد مجرمان و قربانیان	0.746	0.013
C3	فقر فرهنگی و عدم پایبندی به ارزش‌های جامعه و باورهای دینی	0.701	-0.054
C4	هم‌نشینی با دوستان ناباب	0.574	-0.004
C5	نحوه گذراندن اوقات فراقت (بیکاری جوانان)	0.619	0.034
C6	کمبود درآمد	0.892	-0.086
C7	افزایش روزافزون هزینه‌ها	0.983	-0.051
C8	نبود شغل‌های درآمدزا	0.850	0.042
C9	مشکلات روحی و روانی بزهکاران فضای مجازی همچون حسادت و انتقام‌جویی	1.214	-0.041
C10	اعتیاد به اینترنت	0.922	0.002
C11	نبود احساس گناه در مجرمان	1.081	0.071
C12	اشکالات ساختار فنی فضای مجازی	0.922	-0.009
C13	سهولت ارتکاب جرم مجازی و پنهان ماندن	1.365	-0.049

گام سیزدهم: طراحی نمودار علی: بر اساس مقادیر $E(\varpi)_{new}$: نمودار علی مربوط به‌تمامی شاخص‌ها به شرح نمودار (1) ترسیم می‌شود.



نمودار 1: نمودار علی مرتبط با ایجاد بر جرائم فضای در فضای مجازی

با توجه به نمودار شماره (1)، عوامل سطح پایین آگاهی مردم و کاربران در مورد نحوه استفاده از فضای مجازی، نبود احساس گناه در مجرمان، نبود شغل‌های درآمدزا، نحوه گذراندن اوقات فراقت (بیکاری جوانان)، افزایش روزافزون تعداد کاربران و به‌تبع آن، افزایش تعداد مجرمان و قربانیان و اعتیاد به اینترنت دارای $(D-R)_{new}$مثبت هستند و علت محسوب می‌شوند. همچنین، عوامل کمبود درآمد، فقر فرهنگی و عدم پایبندی به ارزش‌های جامعه و باورهای دینی، افزایش روزافزون هزینه‌ها، سهولت ارتکاب جرم مجازی و پنهان ماندن، مشکلات روحی و روانی بزهکاران فضای مجازی همچون حسادت و انتقام‌جویی، اشکالات ساختار فنی فضای مجازی و هم‌نشینی با دوستان ناباب دارای $(D-R)_{new}$ منفی هستند و معلول محسوب می‌شوند. این عوامل همانند مؤلفه‌های روبنایی هستند که نشأت‌گرفته از عوامل زیربنایی هستند.

نتیجه‌گیری

پژوهش حاضر درصدد بود تا در ابتدا مؤلفه‌های مرتبط بر ایجاد جرائم فضای مجازی را شناسایی کند و در ادامه، با استفاده از تکنیک‌های AHP و DEMATEL فازی به

بررسی و تجزیه‌وتحلیل آنها بپردازد. نتایج حاصل از تجزیه‌وتحلیل داده‌های تحقیق در جدول شماره (6) و نمودار شماره (1) حاکی از آن است که عامل سهولت ارتکاب جرم مجازی و پنهان ماندن با $(D_i + R_i)_{NEW}$ =1/365 به‌عنوان بااهمیت‌ترین بعد شناخته شده است. همان‌طور که محققانی همچون برایانز (2014)، شچربک (2014)، کابای (2009)، کیزا (2009)، وال (2001)، دی کیمپ و همکاران (2020) اذعان دارند ناشناختگی از اصول حاکم بر جرائم جهان مجازی است. از یک‌سو، اصولاً شناسایی کاربران ماشین متصل به شبکه امری پیچیده و پرهزینه است. از سوی دیگر، استفاده از شیوه‌های سرقت مشخصات دیگر ماشین‌ها، استتار آنلاین و سایر مخفی‌کاری‌های موجود، امر شناسایی مرتکبین را به‌صورت معمول سخت و بعضاً غیرممکن ساخته است. لازم است ناجا برای مقابله با سهولت ارتکاب جرم مجازی و پنهان ماندن باوجود پرهزینه بودن این امر مجرمین در فضای مجازی را شناسایی و برخورد شدید شود تا حدی این جرائم کاهش یابد. پس‌ازآن به ترتیب، مشکلات روحی و روانی بزهکاران فضای مجازی همچون حسادت و انتقام‌جویی، نبود احساس گناه در مجرمان و افزایش روزافزون هزینه‌ها دارای اهمیت هستند. مشکلات روحی و روانی نظیر افسردگی، عصبانیت، حسادت، انتقام‌جوئی، حس تنفر، تفریح و سرگرمی، خودکم‌بینی و حقارت، حس رقابت و ... جز عواملی هستند که در شکل‌گیری جرائم سایبری مؤثرند که آریف و همکاران (2015) در پژوهش خود به این موضوع توجه دارند. بخش عمده‌ای از جرائم رایانه‌ای ارتکاب یافته در کشور برخواسته از مشکلات روحی و روانی بزهکاران فضای مجازی است. فردی صرفاً به جهت اختلاف و با قصد انتقام‌گیری از دیگری اقدام به انتشار عکس‌ها و فیلم‌های خصوصی وی در سایت‌های اینترنتی کرد. در پرونده دیگری، فردی از روی حسادت اقدام به نصب نرم‌افزار شنود بر سیستم رایانه‌ای شخص دیگری کرده و سپس متن چت‌های خصوصی وی را دریافت و برای سایرین ارسال می‌کرد. لازم است ناجا برخورد سخت و سنگین در این خصوص داشته باشد. همچنین، قوانین سخت‌گیرانه در خصوص جرائم فضای مجازی همچون انتشار عکس و فیلم‌های خصوص و هتاکی اعمال کند تا افراد به دلیل انتقام و حسادت و موارد مشابه دست به چنین اقدامی نزنند و عملاً محدودتر شوند. سه بعد هم‌نشینی با دوستان ناباب، نحوه گذراندن اوقات فراقت (بیکاری جوانان)، فقر فرهنگی و عدم پایبندی به ارزش‌های

جامعه و باورهای دینی و سطح پایین آگاهی مردم و کاربران در مورد نحوه استفاده از فضای مجازی در رتبه بعدی اهمیت قرار دارند؛ اما بااین‌حال به‌عنوان ابعاد اثرگذار بر جرائم فضای مجازی هستند.

همچنین، می‌توان اذعان داشت که از بین عوامل مرتبط بر ایجاد جرائم فضای مجازی، سطح پایین آگاهی مردم و کاربران در مورد نحوه استفاده از فضای مجازی با$(D_i - R_i)_{NEW}$ =0/705به‌عنوان اثرگذارترین عامل شناخته می‌شود. فضای مجازی واقعیتی است که توانسته در جامعه نفوذ و در دسترس بسیاری از افراد جامعه قرار گیرد. محققانی ازجمله مسعودیان (1391)، بیات‌پور (1396)، سپهری و همکاران (1394) و برادروست و همکاران (2014)، یکی از راهکارهای کارآمد مقابله با چالش‌های فضای مجازی را بصیرت بخشی و آگاهی دادن به کاربران می‌دانند. بسیار واضح و روشن است که بسیاری از فعالیت‌های تخریب‌گرایانه که در فضای مجازی صورت می‌پذیرد، جهت سوءاستفاده است. حال اگر کاربری که قصد استفاده از فضای مجازی را دارد، این مسئله را به‌خوبی بداند، در مقابل آن جبهه گرفته و هرگز تحت‌تأثیر این‌گونه آسیب‌ها قرار نخواهد گرفت. علاوه بر این، تکنولوژی‌های جدید موجب فراهم آمدن افزایش آگاهی‌های جامعه شده است. به‌این‌ترتیب، خود شبکه‌های اجتماعی موجب افزایش مهارت‌های IT و ارتقا درک کاربران از تکنولوژی خواهند شد. در واقع، شبکه‌های اجتماعی هزینه آگاه‌تر شدن شهروندان را کاهش می‌دهند. به‌این‌ترتیب، می‌توان موجبات افزایش آگاهی‌های اجتماعی را فراهم کرد. لذا باید به این مهم اهتمام ورزید که سطح آگاهی کاربران ازنظر فنی و فرهنگی همزمان با پیشرفت تکنولوژی تکامل و پیشرفت داشته باشد. لازم است ناجا به‌منظور افزایش سطح آگاهی مردم و کاربران در فضای مجازی با صداوسیما همکاری مداوم و مستمر داشته باشد و به تولید محتوا در این زمینه بپردازند. همچنین، راه‌اندازی شبکه ملی اطلاعات، دریافت مشاوره از متخصصان مجرب و دلسوز، آموزش و اطلاع‌رسانی به جوانان در زمینه آسیب‌ها، برگزاری کارگاه‌های آموزشی همگانی باهدف آگاه‌سازی عمومی در خصوص فضای مجازی، افزایش آگاهی خانواده‌ها، برخورد جدی با متخلفان در فضای مجازی و برگزاری میزگردهای علمی از مهم‌ترین راهکارها برای مقابله با عدم آگاهی با فضای مجازی است. عامل بعدی اثرگذار، نبود احساس گناه در مجرمان است. احساس گناه و شرم،

احساس‌های خود تنبیهی دردناکی هستند که به ترتیب، بر رفتارها یا عیوب شخصیتی تمرکز دارند. در واقع، انجام یک عمل اشتباه ممکن است به افکار، احساسات و رفتارهای خود تخریبی منجر شود که محققینی همچون آریف و همکاران (2015) و سپهری (1394) در مطالعات خود به این موضوع اشاره دارند. زندگی در میان این احساسات اغلب باعث می‌شود خطاکار کمتر به خود ارزش و احترام بگذارد و به جهت رهایی از این عواطف منفی روان‌شناختی، خطاکاران مکرراً درگیر خود بخشایشگری می‌شوند. به‌این‌ترتیب، احساس گناه، احساسی فطری است که صرف‌نظر از نوع دین و اخلاقیات افراد، با انجام بعضی امور به‌وجود می‌آید. نتایج مطالعات مسعودیان (1391)، آریف و همکاران (2015) و سپهری و همکاران (1394) نشان می‌دهد هرچه احساس گناه در کاربران کمتر باشد احتمال وقوع جرم توسط آن‌ها بیشتر خواهد بود؛ بنابراین لازم است که ناجا برای مجرمین آموزش‌ها و جلسات توجیهی به‌منظور تقویت عقاید دینی برگزار کند و در این امر فرهنگ‌سازی صورت گیرد. عامل اثرگذار دیگر، نبود شغل‌های درآمدزا است. عدم دسترسی یا دسترسی محدود به فرصت‌ها و منابع کسب درآمد و اشتغال کامل که در جامعه به‌صورت کم‌کاری عینیت می‌یابد از عوامل موجد فقر و نابرابری اقتصادی است. مطالعاتی همچون مسعودیان (1391)، آریف و همکاران (2015) و بیات‌پور (1396) نشان می‌دهند که این عوامل باعث بروز جنایات، انحرافات، تنش‌ها و بی‌نظمی‌های اجتماعی و خشونت می‌شوند. به‌این‌ترتیب، عدم شغل درآمدزا برای فرد، به فقر شخص و از سوی دیگر، سبب ایجاد بیماری‌های روانی، افسردگی، ضعف اعتمادبه‌نفس و از بین رفتن امیدواری می‌شود. فرد به دلیل نداشتن درآمد آبرومند به مشاغل اینترنتی روی می‌آورد و برای خود شغل کاذب ایجاد می‌کند. لذا پیشنهاد می‌شود شغل‌های درآمدزا و مفید ایجاد شود که مشکل اصلی پیش‌روی جوانان است. کمبود درآمد با کمترین مقدار $(D_i - R_i)_{NEW}$ به‌عنوان تأثیرپذیرترین بعد شناسایی شده است. مسعودیان (1391)، آریف و همکاران (2015) و بیات‌پور (1396) در پژوهش‌های خود اذعان دارند که محیط اقتصادی جوامع به‌نوبه خود در تأثیرگذاری بر جرم و ناهنجاری در سطح کلان تأثیر به‌سزایی دارد. بدون تردید، فقر، نابرابری‌های اقتصادی و بیکاری در زمره مهم‌ترین معضلات جامعه بشری است که از جایگاه ویژه‌ای بین سایر مسائل اقتصادی برخوردار است. پس از کمبود درآمد، عامل دیگر تأثیرپذیر،

فقر فرهنگی و عدم پایبندی به ارزش‌های جامعه و باورهای دینی است. فقر فرهنگی و عدم پایبندی به ارزش‌های جامعه و باورهای دینی، یکی از عوامل مهم ارتکاب برخی جرائم اخلاقی در فضای مجازی است. با ظهور و گسترش دنیای مجازی، موانع بسیاری از بین رفته و ارتکاب جرائم تسهیل شده است. مسعودیان (1391)، بیات‌پور (1396)، سپهری و همکاران (1394)، برادروست و همکاران (2014) به این نتیجه رسیدند که فضای مجازی شرایطی را به‌وجود آورده که مجرمان می‌توانند در مکان‌هایی غیر از جاهایی که آثار و نتایج اعمال آنها ظاهر می‌شود مرتکب جرم شده و به‌راحتی و با کمترین هزینه و اضطراب، بیشترین خسارات و صدمات را به بار آورده و درعین‌حال، ناشناخته باقی بمانند. بینندگان در این فضا، به‌تدریج از چنین ارزش‌های متأثر شده و برای عقب نماندن از ارزش‌های پیشرفته جوامع غربی، ارزش‌های دیگری را چون سبک آرایش و لباس خاص و... را به‌صورت عادت در خود درونی و بخشی از جسم خود کرده و با خود همراه می‌کنند که مهم‌ترین راهکار مقابله با آن، فرهنگ‌سازی و بررسی و تقویت شیوه‌های فرهنگی در پیشگیری از جرائم اخلاقی با همکاری ناجا در فضای مجازی است.

تشکر و قدردانی

بدین‌وسیله از کلیه سازمان‌ها و افرادی که در انجام فرایند تحقیق همکاری کردند، تشکر و قدردانی به عمل می‌آید.

منابع

- بهره‌مند، حمید؛ کوره‌پز، حسین محمد؛ سلیمی، احسان (1393). «راهبردهای وضعی پیشگیری از جرایم سایبری». آموزه‌های حقوق کیفری، شماره هفتم، صص 176-147.
- بیات‌پور، سجاد (1396). «جرم‌شناسی فنی جرایم فضای سایبری». اولین همایش بین‌المللی فقه و حقوق، وکالت و علوم اجتماعی، همدان.
- جاه‌بین، زهرا؛ مظفری، افسانه؛ هاشم زهی، نوروز؛ دادگران، سید محمد (1397). «مطالعه کیفی عوامل ارتکاب جرائم در فضای مجازی (تحلیل محتوای کیفی پرونده‌های جرائم سایبری)». مطالعات علوم اجتماعی ایران، دوره پانزدهم، شماره چهارم، صص 71-48.
- جاه‌بین، زهرا؛ مظفری، افسانه؛ هاشم زهی، نوروز؛ دادگران، سید محمد (1397). «عوامل مؤثر بر ارتکاب جرم در فضای مجازی از دیدگاه قضات دادسرای جرائم رایانه‌ای تهران». فصلنامه علمی پژوهش‌های اطلاعاتی و جنایی، دوره سیزدهم، شماره پنجاه و یکم، صص 36-9.
- جوان‌جعفری، عبدالرضا (1389). «جرایم سایبر و رویکرد افتراقی حقوق کیفری (با نگاهی به قانون مجازات اسلامی‌بخش جرایم رایانه‌ای)». پژوهش‌های اقتصاد پولی، مالی، دوره بیست و ششم، شماره هفدهم، صص 193-169.
- حسین‌پور، جعفر؛ ترکمان، زکریا (1395). «بررسی نقش شیوه‌های فرهنگی پیشگیری از جرایم اخلاقی در فضای مجازی». انتظام اجتماعی، دوره هشتم، شماره چهارم، صص 156-137.
- حیدرنژاد، علیرضا؛ سیاح البرزی، هدایت؛ عامری، محمدعلی (1396). «تأثیر عضویت در شبکه‌های اجتماعی بر سرمایه اجتماعی کاربران با تأکید بر امنیت اجتماعی (موردمطالعه: شهر ورامین)». پژوهشنامه نظم و امنیت انتظامی، دوره دهم، شماره چهلم، صص 50-27.
- داودی دهاقانی، ابراهیم. (1398). «موانع اساسی تحقق پیشگیری از جرایم سایبر». پژوهشنامه نظم و امنیت انتظامی، دوره دوازدهم، شماره چهل و ششم، صص 82-53.
- رضوی، محمد (1386). «جرایم سایبری و نقش پلیس در پشگیری از این جرایم و کشف آنها». دانش انتظامی، دوره نهم، شماره یکم، صص 140-120.
- سپهری، کیاست؛ خواجه‌ای، احمد؛ منصوری، داود؛ هژبریان، لاله (1394). «شناسایی عوامل مؤثر در وقوع و کشف جرائم فضای مجازی در استان بوشهر». فصلنامه علمی تخصصی دانش انتظامی بوشهر، شماره بیستم، صص 99-119.
- صابرنژاد، علی؛ حسین‌پور، پری (1396). «تحلیل حقوقی گونه‌شناسی نقض حریم خصوصی در فضای سایبر». جستارهای حقوق عمومی، شماره سوم، صص 129-111.

- فتاحی، مختار (1397). «بررسی عناصر تشکیل‌دهنده مادی و معنوی مصادیق جرایم رایانه‌ای». قانون یار، دوره دوم، شماره ششم، صص 120-99.
- فرهای آلاشتی، زهرا؛ جوان جعفری بجنوری، علیرضا (1396). «نقض آزادی جریان اطلاعات در فرآیند پیشگیری موقعیت مدار از جرائم سایبری». فصلنامه پژوهش حقوق کیفری، دوره پنجم، شماره هیجدهم، صص 100-69.
- کردعلیوند، روح الله؛ میرزایی، محمد (1397). «گونه‌شناسی جرایم سایبری با نگاهی به قانون جرایم رایانه‌ای و آمار پلیس فتا». مجله حقوقی دادگستری، دوره هشتاد و دوم، شماره یکصد و دوم، صص 207-191.
- کرمی، داود (1397). «سیاست کیفری افتراقی در قلمرو ارکان متشکله جرائم سایبری». مجلس و راهبرد، دوره بیست و پنجم، شماره نود و سوم، صص 368-335.
- محمدی برزگر، جعفر؛ بختیاری، لطفلی؛ محمدی‌مقدم، یوسف؛ شاه‌محمدی، غلامرضا (1398). «شناسایی ابعاد و مؤلفه‌های پیشگیری از جرائم علیه عفت و اخلاق عمومی در فضای مجازی». پژوهشنامه نظم و امنیت انتظامی، دوره دوازدهم، شماره چهل و هشت، صص 232-205.
- مسعودیان، محسن (1391). «نقش پلیس در پیشگیری از جرایم سایبری و تأمین امنیت در فضای مجازی (پلیس فتا)». انتظام اجتماعی، دروه اول، شماره چهارم، صص 126-103.
- وطنی، امیر؛ اسدی، حمید (1395). «سیاست جنایی جمهوری اسلامی ایران در جرائم سایبری با تأکید بر ویژگی‌های خاص این جرائم». پژوهشنامه حقوق اسلامی، دوره هفدهم، شماره چهل و چهارم، صص 126-99.
- Abdullah, Lazim, & Zulkifli, Norsyahida. (2015). Integration of fuzzy AHP and interval type-2 fuzzy DEMATEL: An application to human resource management. Expert Systems with Applications, 42(9), 4397-4409.
- An, Jungkook, & Kim, Hee-Woong. (2018). A data analytics approach to the cybercrime underground economy. Ieee Access, 6, 26636-26652.
- Arief, Budi, Adzmi, Mohd Azeem Bin, & Gross, Thomas. (2015). Understanding cybercrime from its stakeholders' perspectives: Part 1-attackers. IEEE Security & Privacy, 13(1), 71-76.
- Bartholomae, Florian. (2018). Cybercrime and cloud computing. A game theoretic network model. Managerial and Decision Economics, 39(3), 297-305.
- BaykasoğLu, Adil, KaplanoğLu, Vahit, DurmuşOğLu, Zeynep DU, & ŞAhin, Cenk. (2013). Integrating fuzzy DEMATEL and fuzzy hierarchical TOPSIS methods for truck selection. Expert Systems with Applications, 40(3), 899-907.
- Bozbura, F Tunç, Beskese, Ahmet, & Kahraman, Cengiz. (2007). Prioritization of human capital measurement indicators using fuzzy AHP. Expert Systems with Applications, 32(4), 1100-1112.

- Broadhurst, Roderic, Grabosky, Peter, Alazab, Mamoun, Bouhours, Brigitte, & Chon, Steve. (2014). An analysis of the nature of groups engaged in cyber crime. An Analysis of the Nature of Groups engaged in Cyber Crime, International Journal of Cyber Criminology, 8(1), 1-20.
- Bryans, Danton. (2014). Bitcoin and money laundering: mining for an effective solution. Ind. LJ, 89, 441.
- Buckley, JJ. (1985). ǪFuzzy Hierarchical Analysis, ǫFuzzy. Sets and Systems, 17, 233-247.
- Chang, Lennon YC, Zhong, Lena Y, & Grabosky, Peter N. (2018). Citizen co-production of cyber security: Self-help, vigilantes, and cybercrime. Regulation & Governance, 12(1), 101-114.
- Cheng, Cecilia, Chan, Linus, & Chau, Chor-lam. (2020). Individual differences in susceptibility to cybercrime victimization and its psychological aftermath. Computers in Human Behavior, 108, 106311.
- De Kimpe, Lies, Ponnet, Koen, Walrave, Michel, Snaphaan, Thom, Pauwels, Lieven, & Hardyns, Wim. (2020). Help, I need somebody: Examining the antecedents of social support seeking among cybercrime victims. Computers in Human Behavior, 108, 106310.
- Gogus, Ozerk, & Boucher, Thomas O. (1998). Strong transitivity, rationality and weak monotonicity in fuzzy pairwise comparisons. Fuzzy sets and Systems, 94(1), 133-144.
- Holt, Thomas J, & Bossler, Adam M. (2015). Cybercrime in progress: Theory and prevention of technology-enabled offenses: Routledge.
- Kabay, ME. (2009). Understanding studies and surveys of computer crime: Wiley, New York.
- Kizza, Joseph Migga. (2009). Guide to computer network security: Springer.
- Kizza, Joseph Migga. (2013). Understanding Computer Network Security Guide to Computer Network Security (pp. 43-59): Springer.
- Lagazio, Monica, Sherif, Nazneen, & Cushman, Mike. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. Computers & Security, 45, 58-74.
- McGuire, M, & Dowling, S. (2013). Cyber crime: A review of the evidence. Home Office Research Report 75. Tech. Rep., 10.
- McQuade, S. (2009). The Encyclopedia of Cybercrime, Westport: CT: Greenwood Press.
- Nalla, Mahesh. (2014). Theorizing Cybercrime: Applying Routine Activities Theory CJ 801 Spring 2014 Micah-Sage Bolden A49092301.
- Norris, Gareth, Lincoln, Robyn, & Wilson, Paul. (2005). Contemporary comment: An examination of Australian internet hate sites. Bond University.

- Pupillo, Lorenzo. (2018). EU Cybersecurity and the Paradox of Progress. CEPS Policy Insight(2018/06).
- Shcherbak, Sergii. (2014). How should Bitcoin be regulated. Eur. J. Legal Stud., 7, 41.
- Sukhai, Nataliya B. (2004). Hacking and cybercrime. Paper presented at the Proceedings of the 1st annual conference on Information security curriculum development.
- Umanailo, M Chairul Basrun, Fachruddin, Imam, Mayasari, Deviana, Kurniawan, Rudy, Agustin, Dewien Nabielah, Ganefwati, Rini,... Fitriana, Rahmah. (2019). Cybercrime Case as Impact Development of Communication Technology That Troubling Society. Int. J. Sci. Technol. Res, 8(9), 1224-1228.
- Wall, David S. (2001). Cybercrimes and the Internet. Crime and the Internet, 1-17.
- Wall, David S. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. International Review of Law, Computers & Technology, 22(1-2), 45-63.
- Wang, Ying-Ming. (2009). Centroid defuzzification and the maximizing set and minimizing set ranking based on alpha level sets. Computers & Industrial Engineering, 57(1), 228-236.
- Wegberg, RS, Oerlemans, J, & Deventer, O van. (2018). Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin. Journal of Financial Crime, 25, 17.
- Wu, Wei-Wen. (2008). Choosing knowledge management strategies by using a combined ANP and DEMATEL approach. Expert Systems with Applications, 35(3), 828-835.