مقاله پژوهشی

تعیین عوامل راهبردی مؤثر بر پیشگیری از جرایم سایبری با رویکرد دلفی فازی

تاریخ دریافت: ۱۳۹۹/۰۷/۱۷ تاریخ پذیرش: ۱۳۹۹/۱۰/۲۵

فخرالدین توکلی[۱]، سید مرتضی مرتضوی[۲]، محسن کشاورزترک[۳]

از صفحه ۱۱۳ تا ۱۴۰

چکیده

زمینه و هدف: ویژگی‌های محیط سایبر و در نتیجهٔ آن پیچیده‌تر شدن جرایم سایبری موجب زمان‌بر و هزینه‌بر شدن کشف این جرایم شده است در نتیجه توجه به پیشگیری از جرایم سایبری از اهمیت بالایی برخوردار می‌باشد؛ هدف از این پژوهش تعیین عوامل راهبردی مؤثر بر پیشگیری از جرایم سایبری است.

روش‌شناسی: روش پژوهش حاضر از نظر هدف، کاربردی و از نظر روش اجرا، توصیفی- پیمایشی است. جامعهٔ آماری این پژوهش را خبرگان پلیس فتا ناجا به تعداد ۱۵ نفر تشکیل می‌دهند. ابزار گردآوری داده‌ها، پرسشنامهٔ محقق ساخته است که پایایی پرسشنامه از روش ضریب آلفای کرونباخ با مقدار ۰/۸۹ و روایی پرسشنامه با روش محتوایی تأیید شد همچنین با استفاده از روش دلفی فازی، در دو مرحله به جمع‌آوری اطلاعات از خبرگان مورد نظر اقدام گردید و کلیدی‌ترین آنها انتخاب شدند. با توجه به ماهیت این پژوهش، جهت تجزیه و تحلیل داده‌های گردآوری شده از روش دلفی فازی و از نرم‌افزارهای Excel و Spss استفاده گردید.

یافته‌ها: یافته‌های این پژوهش نشان داد که مهمترین عوامل راهبردی مؤثر بر پیشگیری از جرایم سایبری، در ۳۱ عامل و ۷ گروه شامل عوامل فرهنگی، عوامل اجتماعی، عوامل فنی، عوامل ایجابی، عوامل سلبی، عوامل درون سازمانی و عوامل برون سازمانی می‌باشند.

نتیجه‌گیری: با توجه به نتایج پژوهش، فرهنگ‌سازی و تولید رسانه‌ای، آگاه‌سازی خانواده‌ها، استفاده از ابزارهای امنیتی توسط کاربران، در اختیار داشتن نیروهای متخصص و آموزش دیده از جمله عوامل مؤثر و نقش آفرین در پیشگیری از جرایم سایبری می‌باشند که بایستی در طراحی و انتخاب برنامه‌ریزی‌های راهبردی مناسب مورد توجه ویژه قرار گیرند.

واژه‌های کلیدی: محیط سایبر، جرایم سایبری، پیشگیری از جرایم سایبری، دلفی فازی.

۱- دانشجوی دکتری جرم یابی، دانشگاه علوم انتظامی امین، تهران، ایران (نویسنده مسئول). رایانامه: a.tavakol583@gmail.com
۲ - کارشناسی ارشد مدیریت اجرایی، دانشگاه آزاد اسلامی واحد قزوین، قزوین، ایران. رایانامه: mortezam9094@gmail.com
۳ - دکتری آینده‌پژوهی، دانشگاه تهران، تهران، ایران. رایانامه: m_keshavarz@ut.ac.ir

مقدمه

امروز با پا گذاشتن در هزاره سوم میلادی فناوری‌های نوین اطلاعات و ارتباطات به نحوه شگفت‌آوری وارد ساختار زندگی انسان‌ها شده است که تجلی آن فضای تبادل اطلاعات (فضای سایبر) است (جزایری و همکاران، ۱۳۹۸: ۹). ایجاد فضای مجازی برای زندگی بشر، شکل جدیدی از روابط اجتماعی، تجارت، دوستی و... به وجود آورده است (عابدینی، ۱۳۸۸: ۱۴۵). به طوری که در گذشته بسیاری از تجار و افراد به منظور ارسال یک پیش فاکتور ساده مجبور به ارسال آن از طریق پست و یا فکس بودند، اما در حال حاضر به مدد اینترنت و پست الکترونیک قادر به انجام مراودات خود در چند ثانیه می‌باشد. به طوری که می‌توان ادعا نمود هم اکنون بخش اعظم مراودات مالی و تجاری از طریق اینترنت صورت می‌پذیرد (روضه‌ای و همکاران، ۱۳۹۶: ۲). از سوی دیگر با دسترس قرار گرفتن ابزارهایی چون وب سایت‌ها، بانکداری الکترونیک، شبکه‌های اجتماعی و ... ؛ بدیهی است، فضای سایبر قابلیت‌ها و امکانات شگفت‌انگیزی به وجود آورده است؛ اما همانند دیگر عناصر زندگی اجتماعی، از گزند سوءاستفاده، به ویژه جرم، در امان نمانده است (مقیمی، ۱۳۹۷: ۸۲). فضای مجازی محدود به زمان و مکان نیست و محدودیت‌های انجام جرم در محیط فیزیکی را ندارد (شاه محمدی و تاهو، ۱۳۹۳: ۱۰۰)، که این امر موجب شده از بروز جرایم نوین در امان نباشد؛ و ما در فضای سایبر با مفهوم جدیدی از جرم به نام جرم سایبری[1] مواجه گردیم (باباغیبی ازغندی، ۱۳۹۱: ۱۴۶). جرم سایبری مجموعه‌ای از سوءاستفاده‌ها و رفتارهای زیان باری است که «از طریق رایانه و سایر فناوری‌های اطلاعاتی و ارتباطی»، «علیه این نوع فناوری‌ها» یا «در فضای فراهم شده توسط این فناوری‌ها» واقع می‌شود (مقیمی، ۱۳۹۷: ۸۲).

امروزه جرایم سایبری با توجه به گستره فناوری اطلاعات و رشد سریع و مستمر تکنولوژی، با طیف گسترده‌ای در فضای مجازی به وقوع می‌پیوندند (خلفی، ۱۳۹۴: ۲۳-۲۴)؛ و از مهمترین تهدیدات و آسیب‌های اجتماعی که امروزه منجر به ناامنی در جوامع پیشرفته و در حال توسعه از جمله کشور ایران شده است، وقوع جرایم در فضای سایبر است (کاهدی و شرفی تبار، ۱۳۹۵: ۸۵). برابر اعلام رئیس پلیس فتا در نشست خبری، مبنی بر افزایش جرائم فضای مجازی در سال ۱۳۹۶، وی اظهار داشته است:

1 - Cyber crime

برداشت‌های غیرمجاز ۶۱/۵ درصد، مزاحمت‌های اینترنتی ۶۰ درصد، کلاهبرداری‌ها ۵۵ درصد، هتک حیثیت و نشر اکاذیب ۳۱ درصد و انتشار فیلم‌های خصوصی خانوادگی در فضای سایبری ۲۲ درصد نسبت به سال ۱۳۹۵ افزایش داشته است (توکلی و شاه محمدی، ۱۳۹۷: ۱۳۱). ویژگی‌های محیط سایبر از قبیل عدم وابستگی به زمان و مکان خاص، امکان تحصیل هویت‌های گوناگون، گمنامی و سهولت انجام اعمال مختلف، به همراه ماهیت جرایم سایبری، وسعت جغرافیایی کشور و همچنین گستردگی به کارگیری روش‌های علمی و فنی و دستیابی به امکانات و ابزارهای مختلف تسهیل‌کننده جرم، عواملی هستند که شیوه‌های ارتکاب جرایم سایبری را متنوع‌تر و پیچیده‌تر کرده است. به طوری که مجرمان سایبری می‌توانند در مکان‌هایی غیر از جاهایی که آثار و نتایج اعمال آنها ظاهر می‌شود مرتکب جرم شده و به راحتی و با کمترین هزینه و اضطراب، بیشترین خسارات و صدمات را به بار آورده و در عین حال ناشناخته باقی بمانند (جلالی، ۱۳۹۱: ۲۴). که این امر علاوه بر تأثیرهای منفی بی‌شماری که بر زندگی افراد جامعه می‌تواند تحمیل کند، کار تعقیب‌کنندگان آن را مشکل و موجب هدر رفتن هزینه‌های سازمان و اتلاف توان مأموران می‌گردد.

به دلیل بروز پدیده‌های مجرمانه سایبری که کشف آن زمان و هزینه‌های زیادی در پی خواهد داشت؛ در این میان پیشگیری، تدابیری است که از پایه مانع از رخداد جرم شده و از ریشه با علل پیدایی بزه و جرم، مبارزه می‌کند (عشایری و نامیان، ۱۳۹۷: ۳۳)؛ پیشگیری از وقوع این جرایم بسیار با صرفه‌تر و کم‌هزینه‌تر از طی فرآیند رسیدگی کیفری آن‌ها و تحمل خسارات بی‌شمار است (دستور و ملکی، ۱۳۹۳: ۵۸). چرا که بخش عمده‌ای از جرایم سایبری را می‌توان پیشگیری نمود، به عنوان نمونه کلاهبرداری‌های اینترنتی ضررهای اقتصادی هنگفتی به کاربران اینترنت به‌خصوص تجار وارد کرده است که بسیاری از این جرایم به دلیل عدم آگاهی کاربران در خصوص شیوه و شگردهای مورد استفاده مجرمان برای کلاهبرداری اینترنتی، صورت می‌پذیرد (اعلایی و همکاران، ۱۳۹۵). بنابراین موضوع پیشگیری از جرایم سایبری به زمینه‌هایی نیاز دارد که در این خصوص عوامل راهبردی مؤثر بر پیشگیری از جرایم سایبری از اهمیت ویژه‌ای برخوردار است و با شناخت عوامل راهبردی و استفاده از راهکارهای پیشنهادی به منظور برنامه‌ریزی‌های مناسب در این امر، می‌توان در جهت کاهش جرایم

سایبری گام برداشت. پس هرچه اقدامات پیشگیرانه بیش‌تر و با قوت و قدرت بیش‌تر انجام شود، تعداد مجرمان کمتر و جامعه سالم‌تر است (شایگان، ۱۳۹۵: ۱۱).

از طرفی اولین و مهم‌ترین وظیفهٔ پلیس پیش از مقابله با جرائم، پیشگیری از وقوع آن است (محمدی، ۱۳۹۸: ۹۸). از این رو در بهمن ماه ۱۳۸۹ نیروی انتظامی جمهوری اسلامی ایران، با تشکیل پلیس فضای تولید و تبادل اطلاعات (فتا) به مقابله و پیشگیری از جرائم سایبری پرداخته است (محمدی، ۱۳۹۸: ۹۶). تعامل و همکاری مؤثر میان پلیس و سازمان‌های مختلف می‌تواند در جهت نیل به اجرایی ساختن فرآیند پیشگیری از جرایم به ویژه جرایم سایبری کمک کند. همچنین ارائه آموزش همگانی و شناسایی و آموزش‌های خاص به افراد و همچنین سازمان‌هایی که احتمال می‌رود در معرض جرایم سایبری قرار گیرند یکی دیگر از شیوه‌های پیشگیری از این جرایم است که توسط پلیس انجام می‌شود (جعفری و سلیمانی، ۱۳۹۷: ۹۵). در نتیجه بدون توجه به عوامل راهبردی تأثیرگذار بر پیشگیری از جرایم سایبری نمی‌توان در جهت کاهش آمار رو به رشد جرایم سایبری گام برداشت؛ درحالی که مجرمان هرچه بیشتر تلاش خواهند نمود از این ظرفیت عظیم سایبری در عرصه ناامنی‌های اجتماعی استفاده نمایند که موجب گستردگی جرایم سایبری از قبیل انحرافات اخلاقی، سرقت اطلاعات، کلاهبرداری‌های اینترنتی، هک، جعل و تجاوز به حریم خصوصی افراد و ... خواهد شد و در نهایت کاهش امنیت عمومی را به دنبال خواهد داشت که این مهم ضرورت انجام پژوهش را روشن می‌سازد. همچنین شناخت عوامل راهبردی مؤثر بر پیشگیری از جرایم سایبری در جهت بهره‌گیری پلیس فضای تولید و تبادل اطلاعات ناجا و دیگر سیاست‌گذاران فرهنگی و مسئولین کشور، در مسیر برنامه‌ریزی‌های کیفی جهت ارتقاء وضعیت موجود حائز اهمیت می‌باشد چرا که از رهگذر چنین مطالعاتی است که می‌توان آینده‌نگری کرد و افق پیش رو را ترسیم و آینده مطلوب را خلق نمود. بنابر آنچه بیان شد پژوهش حاضر به دنبال پاسخ به این سوال است که «عوامل راهبردی مؤثر بر پیشگیری از جرایم سایبری کدامند؟»

مبانی نظری و پیشینه پژوهش

جرایم سایبری

فضای سایبر به عنوان مجموعه تعامل‌های انسان‌ها از طریق رایانه و فناوری‌های نوین ارتباطات، بدون در نظر گرفتن «زمان» و «مکان»، توسط ویلیام گیبسون نویسنده داستان علمی تخیلی در کتاب «نورومونسر»، در سال ۱۹۸۴ به کار برده شد (خانیکی و بابائی، ۱۳۹۰: ۷۶). فضای سایبر در معنا به مجموعه‌هایی از ارتباطات بین انسان‌ها از طریق رایانه و مسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود (اسلامی، ۱۳۹۵: ۱۵۹). فضای سایبر امکانات و قابلیت‌های بی‌شماری برای جامعه به همراه آورده اما به دلیل ویژگی‌های خاص و منحصر به فرد از گزند سوءاستفاده و جرم در امان نمانده است به طوری که؛ با افزایش مداوم حوادث هک، ویروس و سایر انواع سوءاستفاده‌ها که در سال‌های اخیر گزارش شده است، جرایم سایبری به عنوان یک مشکل بزرگ بین‌المللی شناخته شده است(فرنل[1]، ۲۰۰۳: ۸)؛ و از مهمترین تهدیدات و آسیب‌های اجتماعی که امروزه منجر به ناامنی در جوامع پیشرفته و در حال توسعه از جمله کشور ایران شده است، وقوع جرایم در فضای سایبر است (کاهدی و شرفی تبار، ۱۳۹۵: ۸۵). فضای سایبر به اندازه‌ای گسترده و پیچیده است که مجرمان می‌توانند در مکان‌هایی غیر از جاهایی که آثار و نتایج اعمال آنها ظاهر می‌شود مرتکب جرم شده و به راحتی و با کمترین هزینه و اضطراب، بیشترین خسارات و صدمات را به بار آورده و در عین حال ناشناخته باقی بمانند (جلالی، ۱۳۹۱: ۲۴)؛ بنابراین جرایم سایبری جدیدترین و شاید پیچیده‌ترین مشکل در دنیای سایبر است (داشورا[2]، ۲۰۱۱: ۲۴۲). جرایم سایبری جرایمی است که با استفاده از فناوری‌های رایانه‌ای و ارتباطی انجام شده است (اوکوتان و سبی[3]، ۲۰۱۹: ۲۸۷)؛ و می‌توان هرگونه رخداد توأم و انجام شده با فناوری رایانه که موجب می‌شود بزه‌دیده متحمل ضرر بالقوه یا بالفعل شود و مرتکب عامداً توانسته یا خواهد توانست چیزی کسب کند، تعریف نمود (فتحیان و مهدوی نور، ۱۳۸۹: ۲۷۳). مک گوئیر و داولینگ، بیان می‌دارند که جرایم سایبری به عنوان یک اصطلاح چتری است که برای توصیف دو نوع فعالیت مجرمانهٔ مجزا ولی مربوط به هم

1 - Furnell
2 - Dashora
3 - Okutan & Cebi

می‌باشد؛ جرایم وابسته به فضای سایبری و جرایم ممکن شده توسط فضای سایبری (مک گوئیر و داولینگ[1]، ۲۰۱۳: ۵). وزارت دادگستری ایالات متحده[2] و شورای اروپا از اصطلاح جرایم سایبری برای اشاره به طیف وسیعی از جرایم که شامل رایانه‌ها و شبکه‌ها است، استفاده می‌کنند (کسی[3]، ۲۰۱۱: ۳۷). این جرایم می‌تواند علیه افراد، علیه سازمان و علیه جامعه در کل به وقوع بپیوندد (داشورا، ۲۰۱۱: ۲۴۸). در تبیین ماهیت جرایم سایبری، به نظر می‌رسد که می‌توان این جرایم را در چهار دسته یا طبقهٔ کلی جای داد. این دسته‌بندی تا حدی ماهیت جرایم مزبور را نیز روشن می‌کند: ۱- جرایم کلاسیک(سنتی) با توصیف سایبری؛ ۲- جرایم علیه محرمانه بودن داده‌ها و سیستم‌های رایانه‌ای و مخابراتی؛ ۳- جرایم علیه صحت و تمامیت داده‌ها و سیستم‌های رایانه‌ای و مخابراتی؛ ۴- جرایم مرتبط با محتوا (رضوی، ۱۳۸۶: ۱۲۳- ۱۲۴).

پیشگیری از جرایم سایبری

در جهان امروز پیشگیری از جرم که با هدف کاهش فرصت‌ها و انگیزه‌ای مجرمانه انجام می‌پذیرد، اهمیت بسیاری یافته است؛ زیرا ارتکاب جرم و بزه از راه‌های مختلف صورت می‌گیرد و پیچیدگی و گستردگی خاصی پیدا کرده که کشف آن زمان زیاد و هزینه‌های گزافی در پی خواهد داشت (اکبری جبلی، ۱۳۹۹: ۲۶). پیشگیری از جرم به مجموعه اقداماتی اطلاق می‌گردد که از طریق دستگاه‌ها و عوامل ذیربط انجام می‌گردد تا از وقوع جرایم در جامعه جلوگیری به عمل آید و این پیشگیری به دو صورت کیفری و غیرکیفری مطرح است (انصاری، ۱۳۹۴: ۴۶). به طور کلی، پیشگیری واکنشی یا کیفری، ناظر به اقدام کیفری قبل و بعد از وقوع جرم است که با بهره گرفتن از سازوکارهای نظام عدالت کیفری درصدد کاهش نرخ بزهکاری است و پیشگیری غیرکیفری عبارت است از: «جلوگیری از به فعل در آمدن اندیشه مجرمانه با تغییر دادن اوضاع و احوال خاصی که یک سلسله جرایم مشابه در آن به وقوع پیوسته یا ممکن است در آن اوضاع و احوال ارتکاب یابد» (اسدی فرد و همکاران، ۱۳۹۶: ۱۰). در ایران، پیشگیری از جرم و برنامه‌های پیشگیرانه یکی از محوری‌ترین وظایف و مأموریت‌های پلیس است (درویشی، ۱۳۹۶: ۴۸- ۴۹). در این راستا و در حوزهٔ فضای سایبر نیز، راه

1 - McGuire & Dawling
2 - United States Department of Justice
3 - Casey

محافظت از جرایم سایبری این است که همه هوشمند باشند و اقدامات پیشگیرانه توسط افراد، نهادها و دولت به طور یکسان دنبال گردد (پراسانتی و ایشواریا[1]، ۲۰۱۵: ۴۸). پیشگیری از وقوع این جرایم بسیار با صرفه‌تر و کم هزینه‌تر از طی فرآیند رسیدگی کیفری آن‌ها و تحمل خسارات بی‌شمار است (دستور و ملکی، ۱۳۹۳: ۵۸). به عبارت دیگر پیشگیری اولین و بهترین گام در یک پیاده‌روی طولانی به سوی اینترنتی باز، شفاف، آزاد و در عین حال امن می‌باشد. پیشگیری از جرایم سایبری باید با هدف مختل کردن این نوع جرایم، دستگیری مجرمین و ضبط سودهای غیرقانونی ناشی از آن مورد توجه قرار گیرد. چنین اهدافی تنها با اجرای قانون حاصل نمی‌شود، بلکه نیاز به تلاش تلفیقی تمامی سازمان‌های وابسته به دولت، دستگاه‌های مجری قانون، بخش‌های خصوصی، شهروندان و ... دارد (محمدی و جوانبخت، ۱۳۹۵: ۳۲- ۳۳). 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 نمایند. همچنین به استفاده از ابزارهای «فاوا» برای تأمین امنیت این فضا تأکید نموده است. استفاده از ابزارهای فناوری اطلاعات و ارتباطات در قالب تدابیر پیشگیرانه موقعیت مدار، یکی از سریع‌ترین روش‌های تأمین فضای نسبتاً امن و پیشگیری از خسارات کلان سایبری است (فرهادی آلاشتی و جوان جعفری بجنوردی، ۱۳۹۵: ۷۲).

نظریه‌های مربوط به جرائم سایبری

- **نظریه جامعه شبکه‌ای کاستلز:** اینترنت با توجه به مجتمع‌های رسانه‌ای استقرار یافته در سراسر جهان، ظرفیت تکنولوژیکی خود و جریان اطلاعات و نمادهایی که ساخته است به طور عمده نمی‌تواند تحت کنترل خاص و مقررات وضع شده‌ای قرار گیرد و راه کنترل آن مدیریت و کنترل بیشتر اطلاعات تولیدی در این فضا می‌باشد.
- **نظریه انتقال فضایی کی‌جایشانکار:** هنگامی که افراد از یک فضا خارج و به فضای دیگری وارد می‌شوند، رفتارشان متفاوت خواهد بود. به طوریکه آن دسته از افراد

1 - Prasanthi & Ishwarya

که رفتار مجرمانه آنها در فضای فیزیکی سرکوب شده و فرصت و امکان ارتکاب جرم برای آنها وجود ندارد، میل به ارتکاب جرم در فضای مجازی دارند.

- **نظریه هویت گمنام شری ترکل:** ویژگی‌های خاص فضای مجازی همانند امکان گمنامی و حذف آثار فیزیکی به کاربران این امکان را می‌دهد تا به راحتی نقش‌های متفاوتی را در زمان‌های مختلف و با تنظیمات مورد پسند خود بازی کند.

- **نظریه دهکده جهانی مک لوهان:** از دیدگاه مک لوهان دنیای امروز یک دنیای الکترونیکی می‌باشد و رسانه‌های الکترونیکی با گسترش خود فاصله‌های مکانی و زمانی موجود میان انسان ها را از بین برده‌اند به طوریکه کره زمین به وسیله رسانه‌های جدید، آن قدر کوچک شده است که ابعاد یک دهکده را یافته است (صبوری و ثقفی، ۱۳۹۷: ۱۳۲- ۱۳۳).

نظریه‌های مربوط به پیشگیری از جرائم

- **نظریه فرصت رنجر:** بر طبق این نظریه هرچه فرصت‌های احتمالی وقوع جرم بیشتر باشد، تعداد جرایم نیز بیشتر خواهد شد؛ بنابراین برای پیشگیری از وقوع جرم لازم است فرصت‌ها یا زمینه‌های وقوع آن از میان برداشته شود.

- **نظریه کنترل اجتماعی هیرشی:** این نظریه بیان می‌دارد که پیوند میان افراد و جامعه علت هم‌نوایی و عامل اصلی کنترل رفتارهای فرد می‌باشد و ضعف یا نبود این پیوند دلیل اصلی کج رفتاری و فعالیت‌های انحرافی است و در این میان نهادهایی نظیر خانواده، دوستان، همسایه‌ها و مدرسه نقش زیادی دارند.

- **نظریه انتخاب عقلانی یا منطقی بزهکار کلارک و کورنیش:** بر اساس این نظریه مجرمان بالقوه تصمیم‌گیرندگان عاقلی هستند که به دنبال تأمین منافع اقتصادی خود، پس از ارزیابی میزان خطر و منافع حاصل از طریق ارتکاب جرم، می‌باشند و روند تصمیم‌گیری در جرائم مختلف متفاوت می‌باشد.

- **نظریه فعالیت‌های روزمره کوهن و فلسون:** این نظریه ناظر بر تبیین کیفیت تأثیر فعالیت‌های روزمره و سبک زندگی بر وقوع جرائم است و بر همگرایی زمانی و

محیطی سه رکن اصلی لازم برای وقوع جرم یعنی یک بزهکار بالقوه، یک هدف جذاب و فقدان مراقب توانمند متمرکز است (صبوری و ثقفی، ۱۳۹۷: ۱۳۳- ۱۳۴).

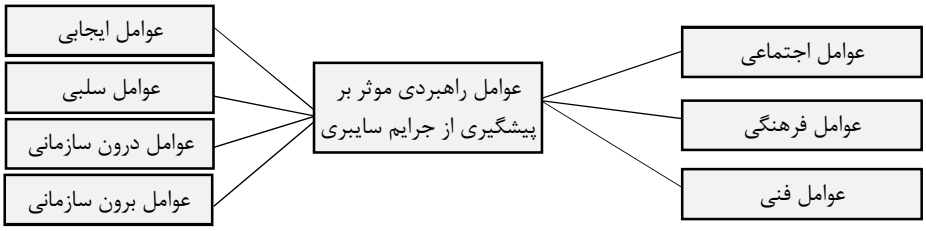
در راستای موضوع مورد مطالعه، بررسی تحقیقات مرتبط نشان می‌دهد که با وجود تحقیقات متعددی که به مباحث فضای سایبر و پیشگیری از جرایم سایبری پرداخته شده است، اما تاکنون هیچ تحقیقی به موضوع تعیین عوامل راهبردی مؤثر بر پیشگیری از جرایم سایبری با رویکرد دلفی فازی نپرداخته است، بنابراین به برخی از پژوهش‌های مرتبط با موضوع تحقیق به اختصار اشاره می‌شود:

محمدی برزگر و همکاران (۱۳۹۹)، در پژوهشی به بررسی وضعیت موجود و مطلوب پیشگیری از جرائم منافی عفت و اخلاق عمومی در فضای سایبر پرداخته‌اند. نتایج پژوهش نشان داد بین مؤلفه‌های وضعیت موجود و مطلوب شکاف معناداری وجود دارد. بیشترین شکاف به ترتیب، در مؤلفه‌های نظارت بر تبلیغات، مشکلات قانونی، اجرایی و قضایی پیشگیری، نظارت بر کسب و کارها و نظارت و ارزیابی اقدامات گذشته می‌باشد. محمدی برزگر و همکاران (۱۳۹۸)، در پژوهشی به شناسایی ابعاد و مؤلفه‌های پیشگیری از جرائم علیه عفت و اخلاق عمومی در فضای مجازی پرداخته‌اند. نتایج پژوهش نشان می‌دهد که برای موفقیت پلیس در پیشگیری از این جرم باید برنامه‌ریزی راهبردی مناسبی در ۹ بُعد اشراف اطلاعاتی، بهره‌وری بهینه از منابع انسانی و سازمانی، ایجاد هماهنگی، طراحی ساختار سازمانی، برنامه‌ریزی پیشگیری، بکارگیری فناوری اطلاعات، اصلاح قوانین و مقررات، نظارت بر منافع مالی کسب و کارهای نامشروع و پیشگیری اجتماعی صورت پذیرد. توکلی و شاه محمدی (۱۳۹۷)، در پژوهشی به تأثیر مدیریت فناوری اطلاعات در پی‌جویی جرائم سایبری پرداخته‌اند. نتایج این پژوهش نشان داد که مدیریت فناوری اطلاعات بر بهبود پی‌جویی جرائم سایبری، افزایش سرعت، افزایش نقش اطلاعات و افزایش دقت پی‌جویی جرائم سایبری تأثیر دارد. بهره‌مند و داودی (۱۳۹۷)، در پژوهشی به پیشگیری اجتماعی از جرایم امنیتی– سایبری پرداخته‌اند. یافته‌های پژوهش نشان می‌دهد که در خصوص برنامه‌های پیشگیرانهٔ اجتماعی می‌توان به برنامه‌های خانواده مدار، تدابیر آموزشی – سایبری، بالابردن سواد رسانه‌ای، تنظیم کدهای رفتاری، اطلاع‌رسانی و اطلاع‌گیری، توجه به حکمرانی خوب و شاخص‌های آن، مشارکت و اجماع‌گیری، ارتقای پاسخگویی و

شفافیت، فرهنگ‌سازی و تولید رسانه‌ای اشاره کرد. روضه‌ای و همکاران (۱۳۹۶)، در پژوهشی به موضوع ابزارهای پیشگیری از جرایم نوظهور در فضای مجازی پرداخته‌اند. نتایج به دست آمده از سمت گروه خبرگان نشان می‌دهد که آیتم‌های آموزش و آگاه‌سازی کاربران اینترنت در خصوص کلاهبرداری اینترنتی، آموزش کاربران در خصوص خدمات بانکداری الکترونیک توسط بانک‌ها و استفاده از نرم‌افزارهای امنیتی و ضدجاسوس افزارها توسط کاربران بیشترین تأثیر را در کاهش کلاهبرداری اینترنتی داشته‌اند. حسین پور و ترکمان (۱۳۹۵)، در پژوهشی به بررسی نقش شیوه‌های فرهنگی پیشگیری از جرایم اخلاقی در فضای مجازی پرداخته‌اند. نتایج پژوهش حاکی از آن است که بین متغیرهای آگاه‌سازی خانواده‌ها، ترویج سبک زندگی اسلامی، نظارت همگانی، راه‌اندازی شبکه ملی اطلاعات و آموزش استفاده صحیح از ابزارهای ارتباط جمعی، با متغیر پیشگیری از جرایم اخلاقی در فضای مجازی رابطه معناداری وجود دارد. شاه محمدی و تاهو (۱۳۹۳)، در پژوهشی به بررسی شیوه‌های پیشگیری از جرایم سایبری؛ مبتنی بر فناوری اطلاعات پرداخته‌اند. نتایج این پژوهش نشان می‌دهد که شیوه‌های مبتنی بر فناوری اطلاعات شامل ردیابی هویت مجازی مهاجمان، گشت فضای مجازی و کنترل و نظارت بر فضای مجازی، جمع‌آوری ادلۀ الکترونیکی جرم و مستندسازی صحنۀ جرم در پیشگیری از جرایم سایبر تأثیر دارد. بهره‌مند و همکاران (۱۳۹۳)، در پژوهشی به موضوع راهبردهای وضعی پیشگیری از جرایم سایبری پرداخته‌اند. نتایج این پژوهش نشان می‌دهد شاید جامع‌ترین و فراگیرترین برنامۀ پیشگیری وضعی، رهنمودهای ۲۵ گانۀ کلارک باشد. گرچه او این رهنمودها را در چارچوب جرایم سنتی مطرح کرد، با این حال می‌توان با پیاده‌سازی و اجرای این رهنمودها، به نحو مطلوبی از جرایم سایبری نیز پیشگیری نمود. عابدینی(۱۳۸۸)، در پژوهشی به موضوع جرم در فضای مجازی، ضرورت آینده‌پژوهی پرداخته است. نتایج پژوهش بیان می‌دارد، پلیس برای پیشگیری، کشف و کنترل فضای مجازی نیاز به سازوکار پلیسی داشته و ساختار چنین سازوکاری اجتناب‌ناپذیر است، بنابراین پیشنهاد می‌شود: ۱- پلیس در اولین اقدام خود ساختار مربوط به مقابله با جرائم فضای مجازی را ایجاد کند؛ ۲- برای برخورد با جرائم فضای مجازی، نیروی انسانی متخصص و کاردان تربیت کند.

اوکوتان و سبی (۲۰۱۹)، در پژوهشی به موضوع چارچوبی برای بررسی جرایم سایبری پرداخته‌اند. نتایج پژوهش حاکی از آن است که در زمینه جرایم سایبری بایستی مقامات اجرای قانون دانش خود را در مورد جرایم سایبری، به ویژه شواهد دیجیتالی افزایش دهند و مجازات‌های عادلانه و مؤثری داشته باشند، به افزایش آگاهی مردم پرداخته شود و همچنین رسانه‌ها می‌توانند با ساختن برنامه‌هایی در مورد جرایم سایبری، راه‌های محافظت از این جرائم و آنچه در حین جرم انجام می‌شود را به شهروندان آموزش دهند و بر لزوم مطالعه بیشتر درباره این موضوع تأکید کنند. پراسانتی و ایشواریا (۲۰۱۵)، در پژوهشی به موضوع جرایم سایبری: پیشگیری و کشف پرداخته‌اند. یافته‌های پژوهش نشان می‌دهد که استفاده از فناوری احراز هویت، افزایش امنیت رایانه، بازیابی اطلاعات، آموزش کودکان، نصب فایروال‌ها، اجتناب از باز کردن پیوست‌ها یا نامه‌های الکترونیکی که از منبع یا فرد ناشناخته‌ای آمده‌اند از جمله اقدامات پیشگیرانه برای مقابله با جرایم سایبری می‌باشند. پونیا، بهارداوج و دانگایاچ[1](۲۰۱۱)، در پژوهشی به موضوع جرایم سایبری: شیوه‌ها و سیاست‌های پیشگیری از آن پرداخته‌اند. یافته‌های مرتبط به شیوه‌های توصیه شده برای پیشگیری از جرایم سایبری نشان می‌دهد که همیشه بهتر است هنگام کار با اینترنت، احتیاط خاصی داشته باشیم و همچنین نصب فایروال‌ها، تغییر رمز عبور به طور مکرر، بررسی‌های مکرر رایانه از ویروس، فیلترهای ایمیل، عدم‌پاسخ‌گویی به ایمیل‌های ناشناس، قطع اتصال هنگام استفاده نکردن از اینترنت، پشتیبان‌گیری اطلاعات از جمله اقدامات پیشگیری از جرایم سایبری می‌باشند.

مدل مفهومی پژوهش



شکل۱. مدل مفهومی پژوهش

1 - Poonia , Bhardwaj & Dangayach

روش‌شناسی پژوهش

پژوهش حاضر از نظر هدف، از نوع پژوهش‌های کاربردی است و به لحاظ اجرا، در قالب تحقیقات توصیفی از نوع پیمایشی محسوب می‌شود. جامعهٔ آماری پژوهش را خبرگان پلیس فتا ناجا منتخب از متخصصان تشکیل می‌دهند و با توجه به هدف پژوهش، نمونه‌گیری هدفمند به روش گلوله برفی و با حجم نمونه ۱۵ نفر صورت گرفت. جهت جمع‌آوری اطلاعات در زمینهٔ مبانی نظری و ادبیات پژوهش موضوع، از مطالعات کتابخانه‌ای و جهت جمع‌آوری داده‌ها به منظور تجزیه و تحلیل و پاسخ به سؤال اصلی پژوهش، از روش میدانی استفاده شد. در این تحقیق از پرسشنامه محقق ساخته جهت جمع‌آوری داده‌ها استفاده گردید. جهت تعیین روایی محتوایی، پرسشنامهٔ تهیه شده در اختیار خبرگان با تجربه قرار گرفت و پس از اصلاحات و تغییرات مورد نظر پرسشنامهٔ نهایی تدوین شد و برای تعیین پایایی پرسشنامه از ضریب آلفای کرونباخ استفاده شد که مطابق جدول۱ و با توجه به مقدار ضریب آلفای کرونباخ بدست آمده، قابلیت اعتماد به پرسشنامه قابل قبول می‌باشد. با توجه به ماهیت این پژوهش، جهت تجزیه و تحلیل داده‌های گردآوری شده از روش دلفی فازی و از نرم افزارهای Excel و Spss استفاده گردید.

جدول۱. آلفای کرونباخ

عوامل راهبردی مؤثر بر پیشگیری از جرایم سایبری	ضریب آلفای کرونباخ
عوامل فرهنگی	۰/۸۷
عوامل اجتماعی	۰/۸۳
عوامل فنی	۰/۷۴
عوامل ایجابی	۰/۸۰
عوامل سلبی	۰/۷۹
عوامل درون سازمانی	۰/۷۶
عوامل برون سازمانی	۰/۸۰
کل پرسشنامه	۰/۸۹

یافته‌های پژوهش

الف) یافته‌های توصیفی

جدول۲. توصیف داده‌ها برحسب ویژگی‌های شخص پاسخ‌دهندگان

ویژگی‌های	جنسیت		سابقه کاری		میزان تحصیلات	
پاسخ‌گویان	مرد	زن	۲۰- ۱۰	بالای ۲۰	لیسانس	فوق لیسانس
فراوانی	۱۵	۰	۱۱	۴	۹	۶
درصد	۱۰۰	۰	۷۳/۳۳	۲۶/۶۷	۶۰/۰۰	۴۰/۰۰

ب) یافته‌های استنباطی

در این تحقیق به منظور تعیین عوامل راهبردی مؤثر بر پیشگیری از جرایم سایبری از روش دلفی فازی استفاده می‌گردد. بدین ترتیب، طی مراحل زیر فرآیند دلفی فازی انجام می‌پذیرد (عرب و همکاران، ۱۳۹۶ و عابدی و عریانی، ۱۳۹۵): در مرحله اول از خبرگان به تعداد ۱۵ نفر خواسته شده است که میزان تأثیرگذار بودن هر یک از عامل‌ها را بر پیشگیری از جرایم سایبری به صورت گزینه‌های کیفی تعریف شده انتخاب نمایند. در مرحله بعد بر اساس نتایج موجود، میانگین میزان تأثیرگذار بودن هر یک از عوامل تأثیرگذار بر پیشگیری از جرایم سایبری طبق روابط زیر محاسبه می‌گردد.

$$A^{(i)} = \left(a_1^i, a_2^i, a_3^i\right), \qquad i = 1,2,3,\ldots,n \qquad (1)$$

$$A_m = \left(a_{m1}^i, a_{m2}^i, a_{m3}^i,\right) = \left(1/n \sum a_1^{(i)}, 1/n \sum a_2^{(i)}, 1/n \sum a_3^{(i)}\right) \qquad (2)$$

در رابطه فوق $A^{(i)}$ بیانگر دیدگاه فرد خبره i ام و A_m بیانگر میانگین دیدگاه‌های خبرگان می‌باشد. مرحله بعدی فازی زدایی می‌باشد. در این پژوهش به منظور فازی زدایی از روش مقدار میانگین، استفاده می‌شود. مقدار فازی‌زدایی به روش مقدار میانگین برابر است با:

$$S(A) = 1/2(S_L(A) + S_R(A))$$

$$S(A) = 1/2\left[(a_{2i} - \int_{a_{1i}}^{a_{2i}} f_{\overline{A}}(x)) + (a_{2i} - \int_{a_{2i}}^{a_{3i}} f_{\overline{A}}(x)) + \right] = \frac{a_{1i} + 2a_{2i} + a_{3i}}{4}$$

جدول۳. عبارت‌های کلامی تکنیک دلفی فازی

متغیر زبانی	عدد فازی
خیلی کم	(۰ ،۰ ،۰/۲۵)
کم	(۰ ،۰/۲۵ ،۰/۵)
متوسط	(۰/۲۵ ،۰/۵ ،۰/۷۵)
زیاد	(۰/۵ ،۰/۷۵ ،۱)
خیلی زیاد	(۰/۷۵ ،۱ ،۱)

سپس می‌توان اختلاف نظر هر یک از خبرگان را طبق رابطه ۳ محاسبه نمود. در حقیقت بر اساس این رابطه هر یک از خبرگان می‌توانند نظر خود را با میانگین نظرات بسنجند و در صورت تمایل نظرات قبلی خود را تعدیل نمایند.

$$e = \left(a_{m1} - a_1^{(i)}, a_{m2} - a_2^{(i)}, a_{m3} - a_3^{(i)}\right)$$
$$= \left(1/n \sum a_1^{(i)} - a_1^i, 1/n \sum a_2^{(i)} - a_2^i, 1/n \sum a_3^{(i)} - a_3^i\right) \quad (3)$$

با استفاده از رابطه ۳ اختلاف نظرات خبرگان محاسبه و در پرسشنامه‌ای تنظیم گردید. سپس هر یک ازخبرگان با توجه به ارزیابی مجدد نظر قبلی خود، نظرات جدید را اعلام نمودند. بدین ترتیب در مرحله دوم با توجه به موارد فوق، پرسشنامه دوم تهیه گردیده و همراه با نقطه نظر قبلی هر فرد و میزان اختلاف آنها با دیدگاه سایر خبرگان، مجدداً به اعضای گروه خبره ارسال گردید. سپس با محاسبه اختلاف میانگین‌های دو مرحله ۱و۲ میزان اجماع نظر خبرگان محاسبه می‌شود. چنانچه اختلاف بین میانگین نظرات دو مرحلهٔ نظرسنجی روش دلفی فازی کمتر از ۰/۲ باشد، فرآیند نظرسنجی متوقف می‌شود، بدین منظور نتایج در جدول۴و۵، بیان شده است:

جدول۴- میانگین دیدگاه‌های خبرگان و فازی‌زدایی در مرحله اول

ردیف	عوامل	اعداد فازی			فازی زدایی
۱	ترویج سبک زندگی اسلامی	۰/۸۷	۰/۶۲	۰/۳۷	۰/۶۲
۲	فرهنگ‌سازی و تولید رسانه‌ای	۰/۹۵	۰/۷۳	۰/۴۸	۰/۷۲
۳	تبیین و نهادینه‌سازی فرهنگ استفاده صحیح از فضای سایبر	۰/۹۵	۰/۷۳	۰/۴۸	۰/۷۲
۴	فعالیت‌های سازمان‌های مردم نهاد	۰/۹۵	۰/۷	۰/۴۵	۰/۷
۵	آگاه‌سازی خانواده‌ها	۱	۰/۹۳	۰/۶۸	۰/۸۹
۶	شناساندن جرایم سایبری و مجازات‌های آن	۱	۰/۹۲	۰/۶۷	۰/۸۸

ردیف	عوامل	اعداد فازی			فازی زدایی
۷	اطلاع‌رسانی و افزایش آگاهی‌های عمومی با ارائه آمار و ارقام	۰/۹۳	۰/۷۸	۰/۵۳	۰/۷۶
۸	افزایش سواد رسانه‌ای	۰/۹۸	۰/۹	۰/۶۵	۰/۸۶
۹	تدابیر آموزشی- سایبری	۰/۹۵	۰/۷۵	۰/۵	۰/۷۴
۱۰	افزایش مشارکت عمومی	۰/۹۷	۰/۸۲	۰/۵۷	۰/۷۹
۱۱	آسیب‌شناسی علل جرم	۰/۹۸	۰/۷۳	۰/۴۸	۰/۷۳
۱۲	استفاده از ابزارهای امنیتی توسط کاربران	۰/۹۵	۰/۸۸	۰/۶۳	۰/۸۳
۱۳	بروزرسانی سیستم و ابزارهای امنیتی توسط کاربران	۰/۹۵	۰/۸۸	۰/۶۳	۰/۸۳
۱۴	افزایش میزان تلاش برای ارتکاب جرم	۰/۹۵	۰/۷۷	۰/۵۲	۰/۷۵
۱۵	افزایش خطر ارتکاب جرم	۱	۰/۹۳	۰/۶۸	۰/۸۹
۱۶	کاهش دستاوردهای جرم	۰/۹۵	۰/۷۵	۰/۵	۰/۷۴
۱۷	کاهش عوامل محرک جرم	۱	۰/۹۵	۰/۷	۰/۹
۱۸	حذف بهانه‌های ارتکاب جرم	۰/۹۸	۰/۹	۰/۶۵	۰/۸۶
۱۹	در اختیار داشتن نرم‌افزارها و سخت افزارهای پیشرفته و به روز	۱	۰/۸۳	۰/۵۸	۰/۸۱
۲۰	در اختیار داشتن نیروهای متخصص و آموزش دیده	۱	۰/۸۸	۰/۶۳	۰/۸۵
۲۱	وجود بانک‌های اطلاعاتی مجرمان سابقه‌دار و حوزهٔ فعالیتی آن	۱	۰/۹۷	۰/۷۲	۰/۹۱
۲۲	مرکز فوریت‌های سایبری	۱	۰/۹۷	۰/۷۲	۰/۹۱
۲۳	تعامل واحدهای درون سازمانی	۰/۸۸	۰/۶۸	۰/۴۳	۰/۶۷
۲۴	آینده‌نگری در حوزهٔ فضای مجازی و جرایم سایبری	۱	۱	۰/۷۵	۰/۹۴
۲۵	کنترل و نظارت بر مراکز عرضه کنندهٔ خدمات اینترنتی	۱	۰/۹	۰/۶۵	۰/۸۶
۲۶	رصد و پایش سایت‌های اینترنتی و شبکه‌های اجتماعی مجازی	۱	۰/۹	۰/۶۵	۰/۸۶
۲۷	تدابیر محدودکننده یا سلب کنندهٔ دسترسی(فیلترینگ)	۰/۹۲	۰/۷۳	۰/۴۸	۰/۷۲
۲۸	وجود قوانین، مقررات و دستورالعمل‌های مدون در سازمان پلیس فتا	۰/۸۷	۰/۶۲	۰/۳۷	۰/۶۲
۲۹	راه‌اندازی سامانه پلیس افتخاری	۰/۹	۰/۷۳	۰/۴۸	۰/۷۱
۳۰	بهره‌برداری از اقدامات فنی و مخابراتی	۱	۰/۸۳	۰/۵۸	۰/۸۱
۳۱	همکاری با دیگر ارگان‌ها (بانک ها، Fcp و ...)	۰/۹۵	۰/۷۷	۰/۵۲	۰/۷۵
۳۲	همکاری بین‌المللی	۰/۹۷	۰/۸۲	۰/۵۷	۰/۷۹
۳۳	استفاده از سیستم عدالت کیفری در بالا بردن میزان مجازات ارتکاب جرایم سایبری	۰/۹۵	۰/۸	۰/۵۵	۰/۷۸
۳۴	راه اندازی اینترنت ملی	۱	۰/۸۸	۰/۶۳	۰/۸۵

جدول۵. فازی‌زدایی در مرحله دوم و اختلاف دیدگاه خبرگان در مرحله اول و دوم

ردیف	عوامل	فازی زدایی (مرحله۲)	اختلاف مرحله اول و دوم
۱	ترویج سبک زندگی اسلامی	۰/۶۷	۰/۰۵
۲	فرهنگ‌سازی و تولید رسانه‌ای	۰/۷۲	۰/۰۰
۳	تبیین و نهادینه‌سازی فرهنگ استفاده صحیح از فضای سایبر	۰/۷۲	۰/۰۰
۴	فعالیت‌های سازمان‌های مردم نهاد	۰/۷۳	۰/۰۳
۵	آگاه‌سازی خانواده‌ها	۰/۸۹	۰/۰۰
۶	شناساندن جرایم سایبری و مجازات‌های آن	۰/۸۸	۰/۰۰
۷	اطلاع‌رسانی و افزایش آگاهی‌های عمومی با ارائه آمار و ارقام	۰/۷۹	۰/۰۳
۸	افزایش سواد رسانه‌ای	۰/۸۶	۰/۰۰
۹	تدابیر آموزشی- سایبری	۰/۸۰	۰/۰۶
۱۰	افزایش مشارکت عمومی	۰/۸۶	۰۷۰
۱۱	آسیب‌شناسی علل جرم	۰/۷۹	۰/۰۶
۱۲	استفاده از ابزارهای امنیتی توسط کاربران	۰/۸۳	۰/۰۰
۱۳	بروزرسانی سیستم و ابزارهای امنیتی توسط کاربران	۰/۸۳	۰/۰۰
۱۴	افزایش میزان تلاش برای ارتکاب جرم	۰/۷۹	۰/۰۴
۱۵	افزایش خطر ارتکاب جرم	۰/۸۹	۰/۰۰
۱۶	کاهش دستاوردهای جرم	۰/۸۰	۰/۰۶
۱۷	کاهش عوامل محرک جرم	۰/۹۰	۰/۰۰
۱۸	حذف بهانه‌های ارتکاب جرم	۰/۸۶	۰/۰۰
۱۹	در اختیار داشتن نرم‌افزارها و سخت افزارهای پیشرفته و به روز	۰/۹۰	۰/۰۹
۲۰	در اختیار داشتن نیروهای متخصص و آموزش دیده	۰/۸۵	۰/۰۰
۲۱	وجود بانک‌های اطلاعاتی مجرمان سابقه‌دار و حوزهٔ فعالیتی آن	۰/۹۱	۰/۰۰
۲۲	مرکز فوریت‌های سایبری	۰/۹۱	۰/۰۰
۲۳	تعامل واحدهای درون سازمانی	۰/۶۹	۰/۰۲
۲۴	آینده‌نگری در حوزهٔ فضای مجازی و جرایم سایبری	۰/۹۴	۰/۰۰
۲۵	کنترل و نظارت بر مراکز عرضه کنندهٔ خدمات اینترنتی	۰/۸۶	۰/۰۰
۲۶	رصد و پایش سایت‌های اینترنتی و شبکه‌های اجتماعی مجازی	۰/۸۶	۰/۰۰
۲۷	تدابیر محدودکننده یا سلب کنندهٔ دسترسی(فیلترینگ)	۰/۷۶	۰/۰۴
۲۸	وجود قوانین، مقررات و دستورالعمل‌های مدون در سازمان پلیس فتا	۰/۶۰	۰/۰۲
۲۹	راه اندازی سامانه پلیس افتخاری	۰/۷۶	۰/۰۵
۳۰	بهره‌برداری از اقدامات فنی و مخابراتی	۰/۸۱	۰/۰۰
۳۱	همکاری با دیگر ارگان‌ها (بانک ها، Fcp و ...)	۰/۸۲	۰/۰۷

ردیف	عوامل	فازی زدایی (مرحله۲)	اختلاف مرحله اول و دوم
۳۲	همکاری بین‌المللی	۰/۸۴	۰/۰۵
۳۳	استفاده از سیستم عدالت کیفری در بالا بردن میزان مجازات ارتکاب جرایم سایبری	۰/۷۴	۰/۰۴
۳۴	راه‌اندازی اینترنت ملی	۰/۸۵	۰/۰۰

در نهایت با توجه به جدول۵، مشاهده می‌گردد که تفاوت مقادیر فازی‌زدایی شده نظرات خبرگان مرحله دوم توزیع پرسشنامه و مرحله اول برای عوامل تأیید شده کمتر از ۰/۲ می‌باشد، بنابراین فرآیند دلفی فازی متوقف می‌شود و عواملی که مقادیر فازی‌زدایی آنها بیشتر از ۰/۷ می‌باشد به عنوان عوامل راهبردی مؤثر بر پیشگیری از جرایم سایبری تأیید می‌گردند که مطابق جدول ۶، شامل ۳۱ عامل و در ۷ گروه می‌باشند:

جدول ۶- عوامل راهبردی مؤثر بر پیشگیری از جرایم سایبری

ابعاد	عوامل
عوامل فرهنگی	فرهنگ‌سازی و تولید رسانه‌ای
	تبیین و نهادینه‌سازی فرهنگ استفاده صحیح از فضای سایبر
	فعالیت‌های سازمان‌های مردم نهاد
عوامل اجتماعی	آگاه‌سازی خانواده‌ها
	شناساندن جرایم سایبری و مجازات‌های آن
	اطلاع‌رسانی و افزایش آگاهی‌های عمومی با ارائه آمار و ارقام
	افزایش سواد رسانه‌ای
	تدابیر آموزشی- سایبری
	افزایش مشارکت عمومی
	آسیب‌شناسی علل جرم
عوامل فنی	استفاده از ابزارهای امنیتی توسط کاربران
	بروزرسانی سیستم و ابزارهای امنیتی توسط کاربران
عوامل ایجابی	افزایش میزان تلاش برای ارتکاب جرم
	افزایش خطر ارتکاب جرم
عوامل سلبی	کاهش دستاوردهای جرم
	کاهش عوامل محرک جرم
	حذف بهانه‌های ارتکاب جرم
عوامل درون سازمانی	در اختیار داشتن نرم افزارها و سخت افزارهای پیشرفته و به روز
	در اختیار داشتن نیروهای متخصص و آموزش دیده

ابعاد	عوامل
	وجود بانک‌های اطلاعاتی مجرمان سابقه‌دار و حوزهٔ فعالیتی آن
	مرکز فوریت‌های سایبری
	آینده‌نگری در حوزهٔ فضای مجازی و جرایم سایبری
	کنترل و نظارت بر مراکز عرضه کنندهٔ خدمات اینترنتی
	رصد و پایش سایت‌های اینترنتی و شبکه‌های اجتماعی مجازی
	تدابیر محدودکننده یا سلب کنندهٔ دسترسی(فیلترینگ)
	راه‌اندازی سامانه پلیس افتخاری
عوامل برون سازمانی	بهره‌برداری از اقدامات فنی و مخابراتی
	همکاری با دیگر ارگان‌ها (بانک‌ها، Fcp و ...)
	همکاری بین‌المللی
	استفاده از سیستم عدالت کیفری در بالا بردن میزان مجازات ارتکاب جرایم سایبری
	راه‌اندازی اینترنت ملی

بحث و نتیجه‌گیری

در پژوهش حاضر با نظر و توجه به این سؤال که عوامل راهبردی مؤثر بر از پیشگیری جرایم سایبری با رویکرد دلفی فازی کدامند، به این موضوع پرداخته شد که انسان عصر حاضر تمایل فراوانی به استفاده از امکانات فضای سایبر و بهره‌مندی از مزایای بی‌شمار آن دارد و این تمایل با سرعت زیادی در حال افزایش است، اما فضای سایبر در کنار مزایای بی‌شماری که برای افراد جامعه به همراه دارد دارای ویژگی‌های خاص از قبیل عدم وابستگی به زمان و مکان خاص، امکان تحصیل هویت‌های گوناگون، گمنامی و ... می‌باشد که همین امر موجب بروز جرایم در فضای سایبر شده است. با توجه به پیچیده‌بودن جرایم سایبری که موجب زمان‌بر و هزینه‌بر شدن کشف این جرایم شده است و با در نظر گرفتن اصل پیشگیری بهتر از درمان است؛ در نتیجه توجه به پیشگیری از جرایم سایبری از اهمیت بالایی برخوردار است و برای حفظ امنیت در این فضا امری ضروری است. در این راستا عوامل مختلفی به منظور پیشگیری از جرایم سایبری وجود دارد. بنابراین به منظور تعیین عوامل راهبردی مؤثر بر پیشگیری از جرایم سایبری از پرسشنامه و نظرات خبرگان و بازخوردهای حاصل از آن در دو مرحله بهره

گرفته شد که در نهایت ۳۱ عامل در ۷ گروه شامل عوامل راهبردی فرهنگی، اجتماعی، فنی، ایجابی، سلبی، درون‌سازمانی و برون‌سازمانی می‌باشند.

طبق یافته‌های این پژوهش عوامل فرهنگی بر پیشگیری از جرایم سایبری مؤثر می‌باشند و یافته‌های این بخش با یافته‌های حسین‌پور و ترکمان (۱۳۹۵)، که بیان می‌دارند آگاه‌سازی خانواده‌ها بیش‌ترین نقش را بر پیشگیری از جرایم اخلاقی در فضای مجازی دارد و در کنار سایر عوامل ذکر شده، آموزش استفاده صحیح از ابزارهای ارتباط جمعی نیز بر پیشگیری از این جرایم تأثیرگذار می‌باشد و یافته‌های بهره‌مند و داودی (۱۳۹۷)، که به فرهنگ‌سازی و تولید رسانه‌ای در پیشگیری از جرایم سایبری اشاره کرده‌اند و همچنین اوکوتان و سبی (۲۰۱۹)، که بیان می‌دارند، رسانه‌ها می‌توانند با ساختن برنامه‌هایی در مورد جرایم سایبری، راه‌های محافظت از این جرائم و آنچه در حین جرم انجام می‌شود را به شهروندان آموزش دهند و بر لزوم مطالعه بیشتر درباره این موضوع تأکید کنند؛ هم راستا است. همچنین طبق یافته‌های تحقیق عوامل اجتماعی بر پیشگیری از جرایم سایبری مؤثر می‌باشند و یافته‌های این بخش با یافته‌های روضه‌ای و همکاران (۱۳۹۶)، که نشان داد، آموزش و آگاه‌سازی کاربران اینترنت در خصوص کلاهبرداری اینترنتی و آموزش کاربران در خصوص خدمات بانکداری الکترونیک توسط بانک‌ها در کاهش کلاهبرداری اینترنتی مؤثر می‌باشند و همچنین برزگر و همکاران (۱۳۹۸)، که پیشگیری اجتماعی را یکی از ابعاد برنامه‌ریزی راهبردی مناسب در پیشگیری از جرائم علیه عفت و اخلاق عمومی در فضای مجازی می‌دانند، هم راستا می‌باشد. طبق یافته‌های این پژوهش عوامل فنی بر پیشگیری از جرایم سایبری مؤثر می‌باشند که یافته‌های این بخش از پژوهش با یافته‌های پونیا و همکاران (۲۰۱۱)، که نشان می‌دهد نصب فایروال‌ها و بررسی‌های مکرر رایانه از ویروس از جمله اقدامات پیشگیرانه از جرایم سایبری می‌باشند و یافته‌های روضه‌ای و همکاران (۱۳۹۶) که نشان داد، استفاده از ابزارهای امنیتی توسط کاربران در کاهش کلاهبرداری اینترنتی مؤثر می‌باشد، هم‌خوانی دارد. همچنین طبق یافته‌های پژوهش عوامل ایجابی و عوامل سلبی از جمله عوامل تأثیرگذار بر پیشگیری از جرایم سایبری می‌باشند که لزوم توجه به آن‌ها با توجه به یافته‌های پژوهش امری ضروری است. یافته‌های این بخش از پژوهش با یافته‌های بهره‌مند و همکاران (۱۳۹۳) که بیان می‌دارند، با بکارگیری عوامل

ایجابی و سلبی می‌توان به نحو مطلوبی از جرایم سایبری پیشگیری نمود و پراسانتی و ایشواریا (۲۰۱۵)، که استفاده از فناوری احراز هویت را در پیشگیری از جرایم سایبری مؤثر می‌دانند، همسو می‌باشد. طبق یافته‌های این پژوهش عوامل درون سازمانی بر پیشگیری از جرایم سایبری مؤثر می‌باشند که با یافته‌های تحقیق توکلی و شاه محمدی (۱۳۹۷)، که نشان داد مدیریت فناوری اطلاعات بر بهبود پی‌جویی جرائم سایبری، افزایش سرعت، افزایش نقش اطلاعات و افزایش دقت پی‌جویی جرائم سایبری تأثیر دارد و شاه محمدی و تاهو (۱۳۹۳) که نشان داد شیوه‌های مبتنی بر فناوری اطلاعات شامل ردیابی هویت مجازی مهاجمان، گشت فضای مجازی و کنترل و نظارت بر فضای مجازی و ... در پیشگیری از جرایم سایبری تأثیر دارند و همچنین عابدینی (۱۳۸۸)، که بیان می‌دارد آینده‌پژوهی برای ترسیم وضعیت جرائم در آینده اجتناب‌ناپذیر به نظر می‌رسد، همسو می‌باشد. در نهایت طبق یافته‌های این پژوهش عوامل برون سازمانی بر پیشگیری از جرایم سایبری مؤثر می‌باشند. یافته‌های این بخش از پژوهش با یافته‌های حسین‌پور و ترکمان (۱۳۹۵)، که بیان می‌دارند بین راه‌اندازی شبکه ملی اطلاعات و پیشگیری از جرایم اخلاقی در فضای مجازی رابطه معناداری وجود دارد و همچنین محمدی برزگر و همکاران (۱۳۹۹) و (۱۳۹۸) که هماهنگی برون سازمانی و هماهنگی بین‌المللی را از جمله مؤلفه‌های پیشگیری از جرائم منافی عفت در فضای سایبر می‌دانند، هم راستا می‌باشد.

پیشنهادها

پیشنهادهای زیر بر اساس عوامل راهبردی شناسایی شده بر پیشگیری از جرایم سایبری ارائه می‌گردد:

- عوامل فرهنگی:

- ظرفیت‌های رسانه و به خصوص شبکه‌های اجتماعی مجازی به منظور فرهنگ‌سازی استفاده درست از فناوری‌های نوین مورد توجه قرار گیرد؛
- برنامه‌های کوتاه‌مدت و بلندمدت برای اقشار مختلف جامعه توسط کارشناسان به منظور نهادینه‌شدن حس احترام به قانون در فعالیت‌های فضای مجازی تدوین گردد؛

- عوامل اجتماعی:

- نشست‌های کارشناسانه توسط متخصصان به منظور شناسایی ریشه‌ای علل ارتکاب جرم و ارائه تدابیر آموزشی در زمینه آگاه‌سازی و اطلاع‌رسانی کاربران برگزار گردد؛

- اطلاع‌رسانی بصورت مستندسازی از جرایم سایبری و شناساندن مجازات‌های آن انجام پذیرد؛

- عوامل فنی:

- در استفاده از برنامه‌های ضد ویروس و به روزرسانی مرتب این برنامه‌ها توسط کاربران به منظور آمادگی مقابله با جرایم سایبری آگاه‌سازی لازم صورت گیرد؛

- سازمان‌های مبتنی بر فناوری اطلاعات به منظور پیشگیری از جرایم سایبری به نرم‌افزارها و تجهیزات قدرتمند در این زمینه مجهز گردند؛

- عوامل ایجابی و سلبی:

- سازوکارهای لازم به منظور حذف تبلیغات‌های تحریک‌آمیز که طبق قانون جرم محسوب می‌شوند و اعمال محدودیت‌ها در این زمینه ایجاد گردد؛

- تدابیر امنیتی لازم برای جلوگیری از نفوذ مجرمان همانند احراز هویت کاربران و ردیابی آنها در فضای مجازی در نظر گرفته شود؛

- عوامل درون سازمانی:

- بر لزوم کنترل، نظارت و آینده‌نگری در حوزه فضای مجازی و جرایم سایبری با استفاده از متخصصان فنی و مخابراتی در سازمان پلیس تأکید گردد؛

- به کارگیری نیروهای متخصص به منظور بهره‌مندی حداکثری از مهارت‌ها و توانایی‌های تخصصی آن‌ها و تهیه و توسعه تجهیزات سازمانی از قبیل نرم‌افزارها و سخت‌افزارهای پیشرفته و به روز مورد توجه و تأکید قرار گیرد؛

- عوامل برون سازمانی:

- همکاری و تعامل پلیس فتا با ارگان‌ها و سازمان‌های مربوطه و لزوم زیرساخت‌های مناسب ارتباطی در این امر مورد توجه قرار گیرد؛

- ابزارهای فنی و مخابراتی جدید در زمینهٔ کشف پیش‌دستانه و پیشگیری از جرایم سایبری استفاده گردند.

تقدیر و تشکر

در پایان، از همهٔ دست‌اندرکاران در پلیس فتا که در انجام این پژوهش همکاری نمودند تشکر و قدردانی می‌گردد.

منابع

- اسدی‌فرد، محمد؛ ذوالفقاری، حسین؛ دعاگویان، داود و هندیانی، عبدالله (۱۳۹۶). مؤلفه‌ها و شاخصه‌های تعاملات اجتماعی پلیس در مدیریت انتظامی پیشگیری از جرم، ۸(۵۱)، صص ۱- ۲۸. بازیابی از:
http://journals.police.ir/article_12036.html
- اسلامی، ابراهیم (۱۳۹۵). جایگاه حمایت از بزه‌دیدگان جرائم سایبری در مقررات کیفری حقوق داخلی و حقوق بین الملل. پژوهشنامهٔ حقوق اسلامی، ۱۷(۱)، صص ۱۵۷- ۱۸۲. بازیابی از:
https://www.sid.ir/fa/journal/ViewPaper.aspx?id=312532
- اعلایی، مهدی؛ حاجی آقائی کشتلی، مصطفی و عموزاد خلیلی، حسین (۱۳۹۵). بررسی روش‌ها و شگردها در کلاهبرداری‌های نوین اینترنتی. کنفرانس بین‌المللی پژوهش‌های نوین در علوم مهندسی، تهران. بازیابی از:
https://civilica.com/doc/506515/
- اکبری جبلی، سعید (۱۳۹۹). پلیس و رویکردهای پیشگیری از وقوع جرم. نشریه علمی دانش انتظامی سیستان و بلوچستان، ۱۱(۳۴)، صص ۲۶- ۴۷. بازیابی از:
http://sbl.jrl.police.ir/article_94311.html
- باباغیبی ازغندی، علی رضا (۱۳۹۱). الگویی نوین برای پیشگیری از جرایم فضای سایبر. فصلنامه مطالعات پیشگیری از جرم، ۸(۲۶)، صص ۱۴۳- ۱۶۸. بازیابی از:
http://cps.jrl.police.ir/article_13591.html
- بهره‌مند، حمید و داودی، ذوالفقار (۱۳۹۷). پیشگیری اجتماعی از جرایم امنیتی- سایبری. مطالعات حقوق کیفری و جرم شناسی، ۴۸(۱)، صص ۲۷- ۴۶. بازیابی از:
https://jqclcs.ut.ac.ir/article_67464.html
- بهره‌مند، حمید؛ کوره پز، حسین محمد و سلیمی، احسان (۱۳۹۳). راهبردهای وضعی پیشگیری از جرایم سایبری. دو فصلنامه آموزه‌های حقوق کیفری، ۱۱(۷)، ۱۴۷- ۱۷۶. بازیابی از:
https://www.sid.ir/fa/journal/ViewPaper.aspx?id=241594
- توکلی، فخرالدین و شاه محمدی غلامرضا (۱۳۹۷). تأثیر مدیریت فناوری اطلاعات در پی جویی جرائم سایبری. فصلنامهٔ پژوهش‌های اطلاعاتی و جنایی، ۱۳(۲)، صص ۱۲۹- ۱۴۸. بازیابی از:
http://icra.jrl.police.ir/article_18852.html
- جزایری، سیدعباس؛ نعمت اللهی، میثم و امیریان فارسانی، امین (۱۳۹۸). پیشگیری از جرایم سایبری و محدودیت های حاکم بر آن. فصلنامه علمی- حقوقی قانون یار، ۳(۱۲)، صص ۹- ۲۴. بازیابی از:
https://www.sid.ir/fa/Journal/ViewPaper.aspx?id=50582

- جعفری، مریم و سلیمانی، فرزاد (۱۳۹۷). نقش پلیس در تأمین امنیت و سالم سازی فضای سایبر با رویکرد پیشگیری اجتماعی از جرایم سایبری. فصلنامه دانش انتظامی زنجان، ۸(۲۹)، صص ۸۵-۱۰۹. بازیابی از:
http://journals.police.ir/article_92872.html
- جلالی، علی اکبر (۱۳۹۱). رفتارشناسی مجرمان در فضای سایبر. فصلنامه کارآگاه، ۶(۲۱)، صص ۶-۲۵. بازیابی از:
http://journals.police.ir/article_10464.html
- حسین پور، جعفر و ترکمان، زکریا (۱۳۹۵). بررسی نقش شیوه‌های فرهنگی پیشگیری از جرایم اخلاقی در فضای مجازی. فصلنامهٔ انتظام اجتماعی، ۸(۴)، صص ۱۳۷- ۱۵۶. بازیابی از:
https://www.sid.ir/fa/journal/ViewPaper.aspx?id=298042
- خانیکی، هادی و بابائی، محمود (۱۳۹۰). فضای سایبر و شبکه‌های اجتماعی؛ مفهوم و کارکردها. فصلنامهٔ انجمن ایرانی مطالعات جامعه اطلاعاتی، ۱(۱)، صص ۷۱- ۹۶. بازیابی از:
https://irandoc.ac.ir/sites/fa/files/attach/article/829-2541-1-pb.pdf
- خلفی، ابوذر (۱۳۹۴). پیشگیری از جرایم سایبری با محوریت جرم‌یابی. فصلنامهٔ کارآگاه، ۹(۳۴)، صص ۲۳- ۳۸. بازیابی از:
http://det.jrl.police.ir/article_10698.html
- درویشی، صیاد (۱۳۹۶). بررسی دانش و مهارت مورد نیاز پلیس در پیشگیری وضعی از جرم. فصلنامه پژوهش‌های دانش انتظامی، ۱۹(۷۱)، صص ۴۷- ۶۸. بازیابی از:
journals.police.ir/article_11442.html
- دستور، علی و ملکی، عزیزاله (۱۳۹۳). وظایف پلیس در پیشگیری از جرایم سایبری (موانع و چالش‌ها). فصلنامه علمی دانش انتظامی مرکزی، (۶)، صص ۳۷- ۶۴. بازیابی از:
http://markazi.jrl.police.ir/article_14273.html
- رضوی، محمد (۱۳۸۶). جرایم سایبری و نقش پلیس در پیشگیری از این جرایم و کشف آن‌ها. فصلنامه دانش انتظامی، ۹(۱)، صص ۱۲۰- ۱۴۰. بازیابی از:
https://www.sid.ir/Fa/Journal/ViewPaper.aspx?ID=74998
- روضه‌ای، منصور؛ توانبخش، جعفر و حسن زاده کرد احمد، حمید (۱۳۹۶). ابزارهای پیشگیری از جرایم نوظهور در فضای مجازی. فصلنامه علمی پژوهشی مطالعات امنیت اجتماعی، ۸(۵۰)، صص ۱- ۲۲. بازیابی از:
http://sss.jrl.police.ir/article_12027.html
- شاه‌محمدی، غلامرضا و تاهو، منصور (۱۳۹۳). بررسی شیوه‌های پیشگیری از جرایم سایبری؛ مبتنی بر فناوری اطلاعات. فصلنامهٔ پژوهش‌های اطلاعاتی و جنایی، ۹(۳)، صص ۹۹- ۱۲۰. بازیابی از:
https://www.sid.ir/fa/journal/ViewPaper.aspx?id=251136

- شایگان، فریبا (۱۳۹۵). نقش سازمان‌های مردم نهاد در پیشگیری اجتماعی از جرم (با تأکید بر نهادهای مذهبی). فصلنامه مطالعات پیشگیری از جرم، ۱۱(۳۹)، صص ۹- ۴۱. بازیابی از:
http://cps.jrl.police.ir/article_13678.html
- صبوری، رضا و ثقفی، کامیار (۱۳۹۷). بررسی جرائم سایبری حوزه اجتماعی و راهبردهای پیشگیری و مقابله با آن در جمهوری اسلامی ایران. فصلنامهٔ علمی امنیت ملی، ۹(۳۴)، صص ۱۲۵- ۱۵۲. بازیابی از:
https://www.sid.ir/fa/Journal/ViewPaper.aspx?id=514653
- عابدی، صادق و عریانی، بهاره (۱۳۹۵). عوامل مؤثر بر ایجاد پدیده شلاق چرمی در زنجیره تأمین: مطالعه موردی شرکت ملی پخش فرآورده‌های نفتی منطقه قزوین. فصلنامه پژوهش‌های سیاستگذاری و برنامه‌ریزی انرژی، ۲(۵)، صص ۷۵- ۹۵. بازیابی از:
https://www.sid.ir/fa/Journal/ViewPaper.aspx?id=351849
- عابدینی، زین العابدین (۱۳۸۸). جرم در فضای مجازی، ضرورت آینده پژوهی. فصلنامه علمی کارآگاه، ۳(۹)، صص ۱۴۴- ۱۵۶. بازیابی از:
http://det.jrl.police.ir/article_10586.htm
- عرب انصاری، مهدی (۱۳۹۴). آینده‌پژوهی و پیشگیری از جرم. فصلنامه دانش انتظامی سیستان و بلوچستان، ۶(۱۴)، صص ۴۳- ۶۴. بازیابی از:
http://journals.police.ir/article_15664.html
- عرب، علیرضا؛ جعفر نژاد چقوشی، احمد و قاسمیان صاحبی، ایمان (۱۳۹۶). مدل‌سازی شاخص‌های سنجش تاب‌آوری تأمین‌کنندگان با رویکرد خبره محورتفسیری: گامی در جهت افزایش بهروه‌وری صنعت قطعه‌سازی خودرو. فصلنامه مدیریت بهره‌وری، ۱۲(۴۶)، صص ۷- ۳۷. بازیابی از:
https://www.sid.ir/fa/journal/ViewPaper.aspx?id=495232
- عشایری، طاها و نامیان، فاطمه (۱۳۹۷). فرا تحلیل عوامل مؤثر بر پیشگیری از وقوع جرم. فصلنامهٔ پژوهش‌های مدیریت انتظامی، ۱۴(۱)، صص ۳۳- ۵۴. بازیابی از:
https://www.sid.ir/fa/journal/ViewPaper.aspx?id=472341
- فتحیان، محمد و مهدوی نور، سید حاتم (۱۳۸۹). مبانی و مدیریت فناوری اطلاعات. تهران: انتشارات دانشگاه علم و صنعت ایران.
- فرهادی آلاشتی، زهرا و جوان جعفری بجنوردی، عبدالرضا (۱۳۹۵). نقض آزادی جریان اطلاعات در فرآیند پیشگیری موقعیت مدار از جرائم سایبری. فصلنامه پژوهش حقوق کیفری، ۵(۱۸)، صص ۶۹- ۱۰۰. بازیابی از:
http://jclr.atu.ac.ir/article_7400.html
- کاهدی، شهربانو و شرفی تبار، بهنام (۱۳۹۵). جایگاه پلیس فتا در پیشگیری از جرم در فضای مجازی. فصلنامهٔ دانش انتظامی پلیس استان مرکزی، ۶(۱)، صص ۸۳- ۱۱۴. بازیابی از:

http://journals.police.ir/article_14323.html

- محمدی برزگر، جعفر؛ بختیاری، لطفعلی؛ محمدی مقدم، یوسف و شاه محمدی، غلامرضا (۱۳۹۸). شناسایی ابعاد و مؤلفه های پیشگیری از جرائم علیه عفت و اخلاق عمومی در فضای مجازی. پژوهش نامه نظم و امنیت انتظامی، ۱۲(۴)، صص ۲۰۵- ۲۳۲. بازیابی از:

http://osra.jrl.police.ir/article_۹۳۵۳۸.html

- محمدی برزگر، جعفر؛ بختیاری، لطفعلی؛ محمدی مقدم، یوسف و شاه محمدی، غلامرضا (۱۳۹۹). بررسی وضعیت موجود و مطلوب پیشگیری از جرائم منافی عفت و اخلاق عمومی در فضای سایبر. پژوهش نامه نظم و امنیت انتظامی، ۱۳(۳)، صص ۱۰۳- ۱۲۸. بازیابی از:

http://journals.police.ir/article_۹۴۳۴۴.html

- محمدی، سهیلا و جوانبخت، محمد (۱۳۹۵). فضای سایبری امن (بررسی نقش پلیس و ارائه شیوه‌های کاربردی پیشگیری از جرایم سایبری). دانش انتظامی خراسان رضوی، ۸(۳۳)، صص ۲۵- ۴۸. بازیابی از:

http://journals.police.ir/article_15186.html

- محمدی، علی (۱۳۹۸). نقش و جایگاه پلیس در سیاست جنایی ایران در پیشگیری از جرائم سایبری. فصلنامۀ دانش انتظامی خراسان جنوبی، ۸(۱)، صص ۹۶- ۱۱۵. بازیابی از:

http://journals.police.ir/article_20490.html

- مقیمی، مهدی (۱۳۹۷). پیشگیری اجتماعی از جرائم سایبری (در پرتو اجماع بین‌المللی بر منشورهای رفتاری). فصلنامۀ پژوهش‌های اطلاعاتی و جنایی، ۱۳(۳)، صص ۸۱- ۱۰۰. قابل بازیابی از:

http://icra.jrl.police.ir/article_20152.html

- Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press.

- Dashora, K. (2011). Cyber crime in the society: Problems and preventions. Journal of Alternative Perspectives in the social sciences, 3(1), 240-259. Retrieved from:

https://www.japss.org/upload/11._Dashora%5B1%5D.pdf

- Furnell, S. (2003, July). Cybercrime: vandalizing the information society. In International Conference on Web Engineering (pp. 8-16). Springer, Berlin, Heidelberg. Retrieved from:

https://link.springer.com/chapter/10.1007/3-540-45068-8_2

- McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. Summary of key findings and implications. Home Office Research report, 75.

- Okutan, A. (2019). A framework for cyber crime investigation. Procedia Computer Science, 158, 287-294. Retrieved from:

https://doi.org/10.1016/j.procs.2019.09.054

- Poonia, A. S., Bhardwaj, A., & Dangayach, G. S. (2011). Cyber Crime: Practices and Policies for Its Prevention. In The First International Conference on Interdisciplinary Research and Development, Special No. of the International Journal of the Computer, the Internet and Management (Vol. 19, pp. 1-5). Retrieved from: http://www.ijcim.th.org/SpecialEditions/v19nSP1/02_49_23A_Ajeet%20Singh%20Poonia_[9].pdf
- Prasanthi, M. L., & Ishwarya, T. A. (2015). Cyber Crime Prevention & Detection. IJARCCE, 4(3), 45-48. Retrieved from: DOI 10.17148/IJARCCE.2015.4311