# تعیین عوامل تأثیرگذار در کشف جرایم سایبری با رویکرد دلفی فازی

فخرالدین توکلی[1]، سید مرتضی مرتضوی [2]

تاریخ دریافت: ۱۳۹۸/۱۲/۲۰ تاریخ پذیرش: ۱۳۹۹/۲/۲۵

از صفحه ۱۲۸ تا ۱۴۸

**چکیده**

ویژگی‌های محیط سایبر از قبیل عدم وابستگی به زمان و مکان خاص، امکان تحصیل هویت‌های گوناگون، گمنامی و ... عواملی هستند که شیوه‌های ارتکاب جرایم سایبری را متنوع‌تر و کشف جرایم سایبری و به دام انداختن مجرمان را سخت‌تر کرده است؛ لذا این تحقیق با هدف تعیین عوامل تأثیرگذار بر کشف جرایم سایبری انجام پذیرفته است. روش پژوهش حاضر از نظر هدف، کاربردی و از نظر روش اجرا، توصیفی- پیمایشی است. جامعهٔ آماری این تحقیق را خبرگان پلیس فتا ناجا به تعداد ۱۴ نفر تشکیل می‌دهند. ابزار گردآوری داده‌ها، پرسشنامهٔ محقق ساخته است که بر اساس مطالعات کتابخانه ای، بررسی پژوهش‌های قبلی و اعلام نظر خبرگان تهیه و با توجه به استفاده از روش دلفی فازی در سه مرحله به جمع‌آوری اطلاعات از خبرگان مورد نظر اقدام گردید و کلیدی‌ترین آنها انتخاب شدند. با توجه به ماهیت این پژوهش، برای تجزیه و تحلیل داده‌های گردآوری شده از نرم افزار اکسل استفاده گردید. یافته‌های این پژوهش نشان داد که مهمترین عوامل تأثیرگذار در کشف جرایم سایبری، در ۲۶ عامل و ۶ گروه شامل تعامل سازمانی، تجهیزات سازمانی، آشنایی قضات با مبانی فنی و حقوقی، توانمندی نیروی انسانی و کارآگاهان، فناوری‌های نوین ارتباطی؛ و فناوری اطلاعات و فضای مجازی می‌باشند. نتایج این تحقیق نشان می‌دهد که در کشف جرایم سایبری بایستی، تعامل سازمانی، تجهیزات سازمانی، آشنایی قضات با مبانی فنی و حقوقی، توانمندی نیروی انسانی و کارآگاهان، فناوری‌های نوین ارتباطی؛ و فناوری اطلاعات و فضای مجازی به منظور موفقیت هرچه بیشتر در این زمینه مورد توجه قرار گیرند.

**واژگان کلیدی:** محیط سایبر، جرایم سایبری، کشف جرایم سایبری، دلفی فازی

۱.دانشجوی دکتری جرم یابی دانشگاه علوم انتظامی امین، Fakhrodin.tavakoli@chmail.ir

۲. گروه مدیریت اجرایی، دانشکده مدیریت و حسابداری، واحد قزوین، دانشگاه آزاد اسلامی، قزوین، ایران.

**مقدمه:**

در حالی که بیش از چند دهه از ورود رایانه به زندگی اجتماعی بشـــر نگذشـــته که شـــاهد تغییرات اساســـی در زندگی اجتماعی بشر هستیم و این تغییرات روز به روز شتاب بیشتری بر خود گرفته و تغییرات لحظه ایی در زندگی بشر دور از ذهن نمی‌باشد. با ایجاد شبکه‌های رایانه ایی و ارتباط جهانی، این شـــبکه‌ها زندگی اجتماعی بشـــر را وارد مرحله تازه ایی کرده و فضای مجازی را برای زندگی که زندگی دوم[1] نامیده می‌شود، به ارمغان آورده است. در نتیجه ایجاد فضای مجازی برای زندگی بشر، شکل جدیدی از روابط اجتماعی، تجارت، دوستی و... به وجود آورده اســـت(عابدینی، ۱۳۸۸: ۱۴۵). در گذشـــته 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 پســـت الکترونیک قادر به انجام مراودات خود در چند ثانیه می‌باشـــد. لذا اینترنت و فناوری با کاهش هزینه‌ها و افزایش سرعت در انجام فعالیت‌های تجاری محدودیت‌های زمانی و مکانی را رفع نموده اســـت(روضه ای، توانبخش و حســـن زاده کرد احمد، ۱۳۹۶: ۲). رایانه‌ها و شـــبکه‌های بین المللی ارتباطات فراوانی را در جامعه جهانی شـــکل داده‌اند. این امر ضمن داشـــتن محاســـن خاص خود، ناگزیر همراه با معایبی بوده است و در این راستا موجب ایجاد جرایم مربوط به آن شـــده اســـت که به عنوان جرایم سایبری (رایانه‌ای و اینترنتی) شناخته می‌شـــوند. امروزه جرایم ســـایبری با توجه به گستره فناوری اطلاعات و رشد سریع و مستمر تکنولوژی، با طیف گســـترده‌ای در فضای مجازی بـــه وقوع می‌پیوندند(خلفی، ۱۳۹۴: ۲۳). برابر اعلام رئیس پلیس فتا در نشست خبری، مبنی بر افزایش جرائم فضای مجازی در سال ۱۳۹۶، وی اظهار داشته است: برداشت‌های غیرمجاز، مزاحمت‌های اینترنتی، کلاهبرداری‌ها، هتک حیثیت و نشـــر اکاذیب و انتشـــار فیلم‌های خصوصی خانوادگی در فضای ســـایبری نســـبت به سال ۱۳۹۵ افزایش داشته است(توکلی و شـــاه محمدی، ۱۳۹۷: ۱۳۱). با وجود سیاســـت‌های عام و مشترک موجود در کشف تمام جرائم، به دلیل وجود تفاوت‌های ماهوی میان محیط فیزیکی و فضای مجازی، روش‌های پی‌جویی و کشـــف جرائم ســـایبری متفاوت از جرایم ســـنتی است. جرایم سایبری به لحاظ ماهیت مجازی و غیر واقعی خود، دقیقاً نمود عینی و ملموسی، شبیه آنچه در جرایم سنتی مثل ضرب و جرح و سرقت مشاهده می‌کنیم، از خود به نمایش نمی‌گذارد، بلکه جرم ســـایبر در واقع در بســـتر مبادلات الکترونیکی و بر روی داده‌ها و اطلاعات و به ندرت بر روی سامانه‌های فیزیکی و سخت‌افزاری ارتکاب می‌یابد. در جایـــی که جرم ســـایبر بر روی داده‌ها ارتکاب یافتـــه تعیین محل ارتکاب جرم کاری بس دشوار و در برخی موارد حتی غیرممکن به نظر می‌رسد که این امر، کار تعقیب‌کنندگان آن

1 - second life

را مشکل می‌کند (کاهدی و شرفی تبار، ۱۳۹۵: ۹۶). در فضای سایبر، همانگونه که فعالیت‌ها سریع‌تر و ارزان‌تر انجام می‌شود، جرائم نیز پیچیده تر، سریع‌تر و کم هزینه‌تر است. جرائمی از قبیل انحرافات اخلاقی، سرقت اطلاعات، کلاهبرداری‌های اینترنتی، هک، جعل و تجاوز به حریم خصوصی افراد که در این شرایط و با توجه به گستردگی، تنوع، وقوع آسان، پیوستگی و سازمان یافتگی جرایم ارتکابی توسط مجرمان حرفه‌ای در فضای سایبر و همچنین گستردگی به کارگیری روش‌های علمی و فنی و دستیابی به امکانات و ابزارهای مختلف تسهیل کننده در وقوع جرم توسط این مجرمان و تأثیرهای منفی بی شماری که این جرائم بر زندگی افراد جامعه می‌توانند تحمیل کنند، مقابله جدی و مؤثر پلیس را می‌طلبد(توکلی و شاه محمدی، ۱۳۹۷: ۱۳۰). 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 گسترش ارتکاب جرایم سایبری؛ عواملی هستند که شیوه‌های ارتکاب جرایم سایبری را متنوع‌تر و کشف جرایم سایبری و به دام انداختن مجرمان را سخت‌تر کرده است. در شرایط حاضر ضرورت و اهمیت کشف جرایم سایبری در برابر انواع تهدیدات و تهاجمات بر کسی پوشیده نیست و برای حفظ امنیت عمومی ضروری است. این امر مستلزم شناخت عوامل تأثیرگذار در کشف جرائم سایبری است و لازمهٔ چنین حرکتی، وجود آگاهی و شناخت نسبت به آن می‌باشد و هر اندازه نیروهای پلیس در این فضا با تکیه بر سه اصل سرعت، دقت و صحت بتوانند قدرت عمل خود را در پی جویی و کشف جرائم و ناهنجاری‌ها نشان دهند، از زمینه‌های گسترش نا امنی کاسته می‌شود.

با توجه به پیچیدگی‌های مسیر کشف جرم و لزوم تسریع کشف و دستگیری مجرمان و تأثیر آن در کاهش میزان وقوع جرائم، لازم است در حیطه جرم یابی، راهکارهای علمی متعدد و متنوعی جهت کشف جرم مطرح شده و بکار گرفته شود(هندیانی و مرشدی، ۱۳۹۵: ۱۳۵). در این راستا نهاد پلیس در طول زمان با توجه به تغییر و تحولات محیط‌های پیرامونی و انتقال جرایم به محیط سایبر دچار تغییرات و دگرگونی‌هایی در جهت پاسخ دهی به جرایم شده اند و راهبردها، ساختارها و مدل‌های مختلفی را در پیش گرفته و اجرا نموده‌اند. بدین ترتیب در کشف جرایم سایبری، بدلیل پیچیدگی‌ها و مشکلات پیش روی آن، روش‌ها و ابزارهای مختلفی نیاز است و مقابلهٔ جدی و مؤثر پلیس را می‌طلبد که با توسل به مدرن ترین وسایل و روش‌ها، بتواند توان مقابله با مجرمانی که مرتکب این جرایم می‌شوند را داشته باشد. بنابراین شناسایی عوامل تأثیرگذار بر کشف جرایم سایبری از اهمیت ویژه‌ای برخوردار است، به طوریکه بر سرعت کشف این جرایم می‌افزاید و بدون توجه به این موضوع نمی‌توان در جهت کاهش آمار رو به رشد جرایم سایبری گام برداشت و به منظور ردیابی، تعقیب و تحت پیگرد قرار دادن

و کشف ادله و اثبات جرم مجهز شد؛ درحالی که مجرمان هرچه بیشتر تلاش خواهند نمود از این ظرفیت عظیم سایبری در عرصه ناامنی‌های اجتماعی استفاده نمایند. بنابرین این تحقیق به دنبال تعیین عوامل تأثیرگذار در کشف جرایم سایبری با رویکرد دلفی فازی می‌باشد و از رهگذر چنین مطالعاتی است که می‌توان آینده نگری کرد و افق پیش رو را ترسیم نمود و بتوانیم با برنامه ریزی‌های مناسب و دقیق زمینهٔ کشف و کاهش هرچه بیشتر این جرایم را فراهم نماییم. این مقاله به دنبال پاسخ دادن به این سؤال است که عوامل کلیدی تأثیرگذار بر کشف جرایم سایبری با رویکرد دلفی فازی کدامند؟

بررسی تحقیقات مرتبط نشان می‌دهد که با وجود تحقیقات متعددی که به مباحث فضای مجازی پرداخته شده است، اما تاکنون هیچ تحقیقی به موضوع تعیین عوامل تأثیرگذار در کشف جرایم سایبری با رویکرد دلفی فازی نپرداخته است، بنابراین به برخی از پژوهش‌های مرتبط با موضوع تحقیق به اختصار اشاره می‌شود:

نظری منظم، مجیدی، هندیانی و وفادار(۱۳۹۸)، در مقاله‌ای به بررسی عوامل مؤثر بر جرم یابی کلاهبرداری در فضای سایبر پرداخته‌اند. هدف اصلی این مقاله، تبیین شیوه‌های مؤثر در کشف جرم کلاه برداری سایبری و نحوهٔ جرم یابی آن است. نتایج این پژوهش نشان می‌دهد که همکاری پلیس با مقامات جرم یابی، تجهیزات مدرن، علم و آگاهی از علوم رایانه‌ای توسط کارآگاهان سایبری و آشنایی مقامات قضایی با مبانی فنی و حقوقی کلاهبرداری سایبری در کشف جرم کلاه برداری سایبری تأثیر دارد. توکلی و شاه محمدی(۱۳۹۷)، در مقاله‌ای به تأثیر مدیریت فناوری اطلاعات در پی جویی جرائم سایبری پرداخته‌اند. هدف این پژوهش، بررسی تأثیر مدیریت فناوری اطلاعات در پی جویی جرائم سایبری است. نتایج این پژوهش نشان داد که با توجه به حجم گستردهٔ مأموریت‌های ناجا، مدیریت فناوری اطلاعات بر بهبود پی جویی جرائم سایبری، افزایش سرعت، افزایش نقش اطلاعات و افزایش دقت پی جویی جرائم سایبری تأثیر دارد که پیشنهادهایی نیز برای افزایش نقش فناوری اطلاعات در پی جویی جرائم سایبری ارائه شده است. الهی منش و تبریزی(۱۳۹۷)، در مقاله‌ای به کشف علمی جرایم با توسل به ادله نوین و مدارک الکترونیکی(دیجیتال) پرداخته‌اند. این مقاله بیان می‌دارد که پلیس به عنوان نهاد کشف جرایم همان گونه که در محیط فیزیکی و عادی وظیفه کشف جرایم را با برخی اختیارات، وظایف و البته محدودیت‌ها بر عهده دارد در محیط سایبری نیز همان وظایف و اختیارات برای پلیس متصور است هر چند موضوع و نوع عملکرد در فضای مجازی بسیار پیچیده و سخت‌تر از فضای حقیقی است. پلیس در کشف این گونه جرایم با بهره‌گیری از روش‌های علمی و فن‌آوری اطلاعات و جمع‌آوری ادله و مدارک الکترونیکی به دنبال مدارک دیجیتال جهت شناسائی مجرمان سایبری و تبیین شگرد و روش‌های ارتکاب جرم در فضای

مجازی با رویکرد جرم شناسانه هستند. در بین پلیس‌های تخصصی، وظیفه کشف جرایم مرتبط با رایانه بر عهده پلیس آگاهی بود ولی در سال‌های اخیر با تشکیل پلیس فتا به عنوان پلیس تخصصی ویژه جرایم رایانه‌ای و سایبری این وظیفه به پلیس فتا محول شده است.

ذبیح الله نژاد(۱۳۹۶)، در مقاله‌ای به ماهیت جرایم رایانه‌ای و مجازی(سایبری) و نقش پلیس فتا در پیشگیری و کشف این جرایم پرداخته است. نتایج پژوهش حاکی از آن می‌باشند که پلیس فتا با توجه به رشد فناوری و به موازات آن، افزایش بی رویهٔ جرم و الکترونیکی بودن ارتکاب آن در فضای مجازی، توانسته است با بهره‌گیری از آموزه‌های جرم شناسی، آموزش همگانی، تدابیر نظارتی و استفاده از نرم افزارهای تخصصی پلیسی در تقابل و پیشگیری از وقوع جرایم اشاره شده به عنوان حافظ نظم و امنیت در این حوزه، نقشی مؤثر داشته باشد. همچنین؛ ذبیح اله نژاد(۱۳۹۷)، در مقاله‌ای به کشف علمی جرایم سایبری و نقش پلیس فتا استان مازندران در حوزهٔ پیش گیری و امنیت سایبری پرداخته است. یافته‌های پژوهش حاکی از آن است که ماهیت و ویژگی‌های خاص جرایم سایبری از جمله داشتن ابعاد جهانی و فراملی، فقدان رویه‌های مشخص پیرامون همکاری‌های متقابل و تعریف قانونی واحد از جرایم سایبری، بالا بودن سرعت ارتکاب و هزینه‌های کشف این جرایم، مراجع قضایی و انتظامی را با چالش‌های جدیدی مواجه کرده است. نتایج پژوهش نشان می‌دهد که پلیس فتا با حضور تخصصی و هوشمندانه و اطلاع رسانی و گسترش آموزش همگانی به رعایت نظم وامنیت و قوانین در دنیای مجازی و اینترنت کمک می‌کند و از وقوع جرایم می‌کاهد و یا در صورت وقوع جرم به پیگیری و کشف آن می‌پردازد. نیازخانی، طالبیان و عرجی(۱۳۹۶)، در مقاله‌ای به ارزیابی میزان اثر بخشی شیوه‌های کشف علمی جرم در کشف سرقت‌های منزل(مطالعه موردی: شهر قزوین)، پرداخته‌اند. نتایج تحقیق نشان می‌دهد از میان گویه‌های مختلف مورد بررسی، گویه توانمندی نیروی انسانی با اختصاص میانگین رتبه‌ای برابر ۴,۲۳ بیشترین تأثیر را در کشف علمی جرم سرقت از منزل دارد، ارتقای ساختار سازمانی با ۴,۰۹ در رتبه دوم و فناوری‌های نوین ارتباطی با میانگین ۳,۹۱ در رتبه آخر قرار دارد، گویه زیست فناوری و عوامل نوین اطلاعاتی نیز با میانگین‌های ۴,۰۷ و ۳,۹۳ در رتبه‌های سوم و چهارم اهمیت قرار دارند. جهانشیری، حسینی و ابراهیمی(۱۳۹۴)، در مقاله‌ای به تبیین فرآیند تحقیقات مقدماتی در جرایم سایبری پرداخته‌اند. به دلیل اهمیت فرآیند پی جویی در تحقیقات قضایی و رسیدگی به علل وقوع و کشف جرم در این تحقیق تلاش بر آن است تا فرآیند تحقیقات مقدماتی جرایم سایبری در جمهوری اسلامی ایران بررسی شود. این مقاله عنوان کرده است که در بحث اقدامات قبل از وقوع جرم، موضوع پیشگیری، اطلاع‌رسانی و آموزشی و در مباحث اقدامی حین و بعد از وقوع جرم سایبری، به بحث پی‌جویی و مبارزه با جرایم، شناسایی مجرم

و شگرد مجرمان و جمع‌آوری دلایل و مدارک و اموال مالباخته در کنار رعایت اصول قانونی و حقوقی کاملاً ضروری است.

آذرپرند و نیازخانی(۱۳۹۳)، در مقاله‌ای به بررسی عوامل مؤثر بر کشف سرقت از اماکن دولتی استان البرز پرداخته‌اند. پس از تجزیه و تحلیل داده‌ها نتایج تحقیق نشان می‌دهد که بین عوامل انسانی، عوامل تعاملی، عوامل عملیاتی، عوامل اطلاعاتی و کشف سرقت از اماکن دولتی استان البرز رابطه معنا داری وجود دارد همچنین تحقیقات حاکی از تایید هر چهار فرضیه بوده و نتایج عمده تحقیق نشان از آن دارد که بیشترین رابطه را عوامل عملیاتی و کمترین رابطه را عوامل تعاملی با کشف سرقت از اماکن دولتی دارد. وروایی و میرزکی(۱۳۹۰)، در مقاله‌ای به بررسی عوامل مؤثر بر کشف جرم کلاهبرداری رایانه‌ای پلیس آگاهی تهران سال ۸۷- ۱۳۸۶ پرداخته‌اند. بر همین اساس، فرضیه‌های تحقیق نیز پیرامون چهار محور اساسی شامل میزان توانمندی کارآگاهان، میزان تجهیزات سازمانی، میزان تعامل پلیس با مقامات قضایی، میزان آشنایی قضات با مبانی فنی و حقوقی این جرم، با استفاده از آزمون علامت و آزمون مربع خی دو مورد بررسی قرار گرفته است که نتایج حاصل از آزمون‌ها در رابطه با ارزیابی فرضیه‌ها نشانگر تأثیر عوامل مذکور در کشف این جرم توسط افسران و کارآگاهان بوده است. عابدینی(۱۳۸۸)، در مقاله‌ای با عنوان «جرم در فضای مجازی، ضرورت آینده پژوهی» بیان می‌دارد با ورود رایانه به زندگی اجتماعی بشر، تغییرات شگرفی را در جامعه بشری شاهد بودیم. به تبع این تغییرات زندگی بشر به فضای جدیدی منتقل شده و یا در حال انتقال است به همین سبب جرائم در اجتماع شکل جدیدی یافته و روش‌های جدیدی را برای پیشگیری و کشف می‌طلبد و آینده پژوهی برای ترسیم وضعیت جرائم در آینده اجتناب ناپذیر به نظر می‌رسد. به نظر می‌رسد پلیس برای پیشگیری، کشف و کنترل فضای مجازی نیاز به سازوکار پلیسی داشته و ساختار چنین سازوکاری اجتناب ناپذیر 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.

**جرائم سایبری:** از لحاظ لغوی، سایبر به معنی مجازی و غیرملموس است. 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، یک دنیای جدید، یک دنیای موازی است که با خطوط ارتباطی و کامپیوترهای جهان خلق و نگهداری می‌شود. دنیایی که در آن تردد جهانی دانش، رموز، سنجش‌ها، شاخص‌ها، سرگرمی‌ها و عاملیت دیگر انسانی شکل می‌گیرد(بل[1]، ۱۳۸۹: ۲۲-۲۳). فضای مجازی از جمله پدیده‌هایی

1 - Bell

اســـت که تعریف جدیدی از زمان و مکان را ایجاب می کند که تغییرات شـــگرفی را در جامعه و زندگی اجتماعی به وجود آورده و دگرگونی‌های فزاینده و حیرت انگیز دور از انتظار نیســـت. انتقال فضای فیزیکی به فضای مجازی در دهه‌های اخیر در زمینه‌های متعدد اجتماعی صورت گرفتـــه و به مرور زمان زندگـــی در فضای مجازی به واقعیتی انکارناپذیر تبدیل می‌شـــود که بـــه ناچار تمامی نهادهای اجتماعی برای مواجهه با فضـــای جدید زندگی برنامه ریزی و اقدام می کنند(عابدینی، ۱۳۸۸: ۱۴۸). اما فضای سایبری جنبه‌های منفی و خطرناک نیز دارد؛ زیرا این فضا موقعیتی منحصربه فرد پیش روی مجرمان قرار می‌دهد، تا بدون دغدغه‌های ناشـــی از احســـاس خطرهای گوناگون حین ارتکاب جرم در دنیای فیزیکی، در فضای ســـایبری، تنها به نتایج حاصل از اقدامات مجرمانه‌ای که عایدشـــان می‌شود توجه کنند(ذبیح اله نژاد، ۱۳۹۷: ۱۳۶).

از آن جـــا کـــه جرایم اینترنتی در رایانه و در محیط مجازی[1] صورت می گیرند، می‌توان گفت کـــه جرم اینترنتی(ســـایبری)، به هر گونه فعالیتی می گویند که بـــه منظور انجام فعالیت‌های تبهکاری در شـــبکه‌های رایانه‌ای صورت می گیرد(کرم زاده، ۱۳۹۲: ۱۰۴). طبق تعریف ارائه شده از سوی گروهی از کارشناسان سازمان همکاری و توسعهٔ اقتصادی در سال ۱۹۸۳ ، جرائم رایانه‌ای را » هر عمل غیرقانونی، غیراخلاقی یا غیرمجاز نســـبت به پردازش خودکار یا انتقال داده‌ها « عنوان کرده اند(زیبر[2]، ۱۳۹۰: ۱۸). فعالیت‌های به واســـطهٔ رایانه که هم غیرقانونی و هم نامشروع هستند، با بخش‌های خاص می‌توانند از میان شبکه‌های الکترونیک جهانی هدایت شوند(گرکی[3]، ۱۳۸۹: ۳۲). مک گوئیر و داولینگ[4]، بیان می‌دارند که جرایم سایبری به عنوان یک اصطلاح چتری[5] اســـت که برای توصیف دو نوع فعالیت مجرمانهٔ مجزا ولی مربوط به هم می‌باشـــد؛ جرایم وابســـته به فضای سایبری و جرایم ممکن شـــده توسط فضای سایبری(مک گوئیر و داولینگ، ۲۰۱۳: ۵).

بدین ترتیب پلیس فتا باید با هوشیاری و آگاهی کامل نسبت به این فضا با دقت و سرعت عمل در جهت پیشـــگیری از این جرایم گام‌های مؤثری برداشته و به منظور کشف جرایم سایبری و امنیت هر چه بیشتر در این فضا اقدام نماید.

**کشـــف جرائم سایبری:** از مهمترین تهدیدات و آسیب‌های اجتماعی که امروزه منجر

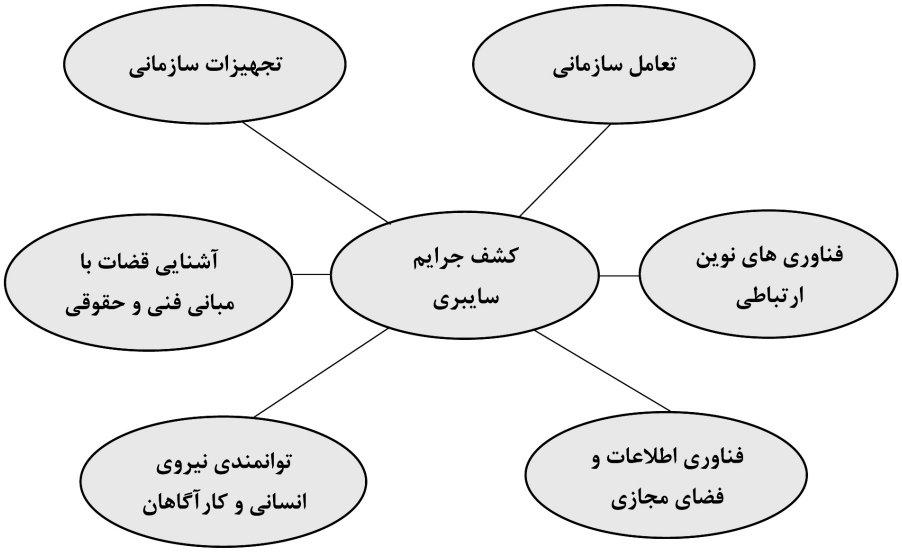
1 - Cyber
2. Sieber Ulrech
3. Marco Gercke
3. McGuire & Dawling
4. Umbrella term

به ناامنی در جوامع پیشـــرفته و در حال توســـعه از جمله کشـــور ایران شـــده است، وقوع جرایم در فضای ســـایبر اســـت(کاهدی و شـــرفی تبار، ۱۳۹۵: ۸۵). محیط سایبر محیطی مخفی می‌باشـــد و گمنامی و ســـهولت انجام اعمال مختلف باعث شـــده مجرمان سایبری از ایـــن فضـــا به منزله‌ی کانون مخفی امن و مطمئن خود بهره‌گیرند و در چنین شـــرایطی تمایـــل ویژۀ افراد مســـتعد برای بزهکاری و گســـتردگی جرائم در ایـــن فضا افزایش یافته اســـت و ضرورت کشـــف و مقابله با این جرایم از اهمیت بالایی برخوردار است. پلیس برای ایفای نقش خویش در این جایگاه باید به کشـــف جرایم چه کلاســـیک و چه مدرن بپردازد اما به دلیل وجود تفاوت‌های ماهوی میان دنیای واقعی و دنیای مجازی روش‌های کشـــف جرم در آنها دارای تفاوت‌های بســـیاری اســـت (وروایی و میرزکی، ۱۳۹۰: ۷۶). از آنجا که این جرائم در فضای مجازی انجام می‌شـــوند و مانند ســـایر جرائم ملموس نیستند، مراجع قضایی و انتظامی برای پیشـــگیری از وقوع این جرائم و کشـــف آنها با موانع و چالش‌های نوینی روبرو هســـتند(نظری منظم و همکاران، ۱۳۹۸: ۲۳۹). دلایل ارتکاب جرم در فضای مجازی، عمدتاً الکترونیک هســـتند. این دلایل در صورتـــی توان اثباتی دارند که نیروهای پلیس در مرحلۀ کشـــف و جمع‌آوری آنها، ابزار و روش‌های خاص ادلۀ مذکور را که مرکب از چهار مرحلۀ جمع آوری، بررســـی، تجزیه و تحلیل و ارئۀ گزارش به مقام قضایی می‌باشد به نحو صحیحی رعایت بکنند(رضوی، ۱۳۸۶: ۱۳۹). فرآیند کشـــف جرم فرآیندی اســـت که پس از طی مراحل هشـــتگانه : ۱- تحقیقات اولیه ۲- عکس برداری و ترســـیم کروکی از صحنه جرم ۳- یادداشـــت‌ها و گزارش‌ها ۴- جستجو و بازرسی ۵- مدارک عینی ۶- کسب اطلاعات ۷- شناســـایی و بازداشـــت مظنونین ۸- آمادگی و ارائه پرونده‌ها در دادگاه منجر به تشـــخیص جرم و هویت مجرم می‌گردد. فرآیند کشـــف جرم، فرآیند کشف، جمع آوری، آماده ســـازی، شناسایی و ارائه شواهد و مدارک برای تشخیص اینکه چه اقداماتی رخ داده و مســـئول کیســـت، می‌باشد(یادگارنژاد، حبیب زاده و نیک نفس، ۱۳۹۳: ۹۰- ۹۱). بدین صورت فرآیند پی جویی و کشـــف جرایم سایبری مطابق جدول ۱، می‌باشد.

**جدول ۱- مستندات قانونی در موضوع پی جویی جرایم سایبری کشور**
**(منبع: جهانشیری و همکاران، ۱۳۹۴: ۲۲)**

| فصول | مواد | مباحث | |
|---|---|---|---|
| صلاحیت‌ها | ماده ۲۸ | الف) ارتکاب جرم در سامانه‌های رایانه‌ای و مخابراتی یا حامل‌های داده موجود در قلمرو حاکمیت زمینی، دریایی و هوایی جمهوری اسلامی ایران؛<br>ب) ارتکاب جرم از طریق تارنماهای (وبسایت‌های) دارای دامنه کد کشوری ایران؛<br>ج) جرم توسط هر ایرانی یا غیر ایرانی در خارج از ایران علیه سامانه‌های رایانه‌ای و مخابراتی و تارنماها(وب سایت‌ها)؛<br>د) سوءاستفاده از اشخاص کمتر از ۱۸ سال، اعم از آنکه مرتکب یا بزه دیده ایرانی یا غیرایرانی باشد. | |
| | ماده ۲۹ | صلاحیت دادسرای محل کشف چنانچه محل وقوع آن معلوم نباشد. | |
| جمع آوری ادله الکترونیکی | ماده ۳۲ و ۳۳ | نگهداری داده‌ها | نگهداری داده‌های ترافیک را حداقل تا شش ماه پس از ایجاد و اطلاعات کاربران را حداقل تا شش ماه پس از خاتمه اشتراک. |
| | ماده ۳۴ | حفظ فوری داده‌های | حفظ داده‌های رایانه‌ای ذخیره شده برای تحقیق یا دادرسی خطر آسیب دیدن یا تغییر یا از بین رفتن داده‌ها |
| | ماده ۳۵ | ارائه داده‌ها | در اختیار قرار دادن داده‌های حفاظت شده به ضابطان برابر دستور قضایی. |
| | مواد ۳۹-۴۷ | تفتیش و توقیف داده‌ها و سامانه‌های رایانه‌ای و مخابراتی و رعایت تناسب، نوع، اهمیت و نقش آن‌ها در ارتکاب جرم، به روش‌هایی از قبیل چاپ داده‌ها، کپی برداری یا تصویر برداری. | |
| | ماده ۴۸ | شنود محتوا | شنود محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی و دسترسی به محتوای ارتباطات غیرعمومی ذخیره شده، نظیر پست الکترونیکی یا پیامک. |
| استناد پذیری | ماده ۴۹ | حفظ صحت و تمامیت، اعتبار و انکارناپذیری ادله الکترونیکی جمع آوری شده مطابق آئین نامه. | |
| سایر | ماده ۵۲ | سامانه رایانه‌ای یا مخابراتی به عنوان وسیله ارتکاب جرم باشد و در قانون جرایم رایانه‌ای مجازات پیش بینی نشده باشد مطابق قوانین جزائی عمل خواهد شد. | |
| | | در مواردی که برای رسیدگی به جرایم رایانه‌ای مقررات خاصی از جهت آئین دادرسی پیش بینی نشده است طبق مقررات قانون آئین دادرسی کیفری اقدام خواهد شد. | |

با توجه به مطالعات انجام شده، شکل ۱، مدل مفهومی تحقیق را نشان می‌دهد:




**شکل۱- اجزای مدل مفهومی تحقیق**

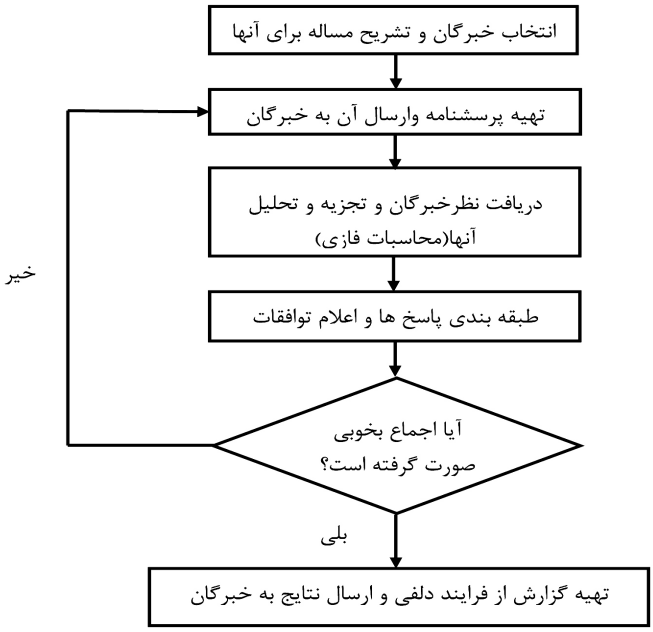
**روش شناسی تحقیق**

تحقیـــق حاضـــر از نظر هدف، کاربردی و از لحاظ گردآوری داده‌ها و اطلاعات و روش تجزیه و تحلیل یک تحقیق توصیفی- پیمایشـــی محســـوب می‌شود. بدین منظور، جهت جمع‌آوری اطلاعات در زمینهٔ مبانی نظری و ادبیات تحقیق موضوع، از مطالعات کتابخانه‌ای و جهت جمع آوری داده‌ها و اطلاعات، از روش میدانی اســـتفاده شد. جامعهٔ آماری تحقیق را خبرگان پلیس فتا ناجا منتخب از متخصصان به تعداد ۱۴ نفر تشـــکیل می‌دهند. در این تحقیق از پرسشنامه جهت جمع‌آوری داده‌ها اســـتفاده شـــد، بدین ترتیب که در تحقیق حاضر بعد از تعیین عوامل تأثیرگذار بر کشـــف جرایم سایبری بر اساس مطالعات کتابخانه ای، بررسی پژوهش‌های قبلی و اعـــلام نظر خبرگان، با توجه به اســـتفاده از روش دلفی فـــازی در چند مرحله به جمع‌آوری اطلاعات از خبرگان مورد نظر اقدام گردید و کلیدی‌ترین آنها انتخاب شدند. با توجه به ماهیت این پژوهش، برای تجزیه و تحلیل داده‌های گردآوری شده از نرم افزار اِکسل استفاده گردید.

یافته‌های تحقیق

در این تحقیق به منظور تعیین عوامل تأثیرگذار در کشـــف جرایم ســـایبری از روش دلفی فازی استفاده می‌گردد.

مراحل اجرای روش دلفی فازی مطابق شکل۲، می‌باشد:




**شکل۲- مراحل اجرای روش دلفی فازی(میرسپاسی، ۱۳۸۹)**

بدین ترتیب، طی مراحل زیر فرآیند دلفی فازی انجام می‌پذیرد(عابدی و عریانی، ۱۳۹۵):

در مرحله اول در بررســـی دیدگاه خبرگان، با توجه به شـــاخص‌های پیشـــنهادی و تعریف متغیرهای زبانی، پرسشـــنامه مورد نظر طراحی شد. در این مرحله از خبرگان به تعداد ۱۴ نفر خواســـته شـــده است که میزان تأثیرگذار بودن هر یک از شاخص‌ها را بر کشف جرایم سایبری به صورت گزینه‌های کیفی تعریف شـــده انتخاب نمایند. در مرحله بعد بر اساس نتایج موجود، میانگین میزان تأثیرگذار بودن هر یک از شاخص‌های تأثیرگذار بر کشف 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.

مرحلـــه بعدی فازی زدایی می‌باشـــد. در این پژوهش به منظور فـــازی زدایی از روش مقدار میانگین، اســـتفاده می‌شـــود. در این روش از تفکیک‌های چپ و راست، که علاوه بر ساده بودن از همه اطلاعات تابع عضویت نیز اســـتفاده می‌شـــود، برای فازی زدایی استفاده می‌شود. مقدار فازی زدایی به روش مقدار میانگین برابر است با:

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

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

ســـپس می‌توان اختلاف نظر هر یک از خبرگان را طبق رابطه ۳ محاســـبه نمود. در حقیقت بر اســـاس این رابطه هر یک از خبرگان می‌توانند نظر خود را با میانگین نظرات بســـنجند و در صورت تمایل نظرات قبلی خود را تعدیل نمایند.

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

با اســـتفاده از رابطه ۳ اختلاف نظرات خبرگان محاســـبه و در پرسشـــنامه‌ای 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. فازی زدایی حاصل از پرسشـــنامه فوق در جدول زیر مشـــاهده می‌شود. سپس با محاسبه اختلاف میانگین‌های دو مرحله ۱ و ۲ با استفاده از روابط فاصله میان اعداد فازی (رابطه ۴) میزان اجماع نظر خبرگان محاســـبه می‌شـــود. در صورتی که اختلاف محاسبه شده از ۰/۲ کمتر باشد، فرایند دلفی فازی متوقف می‌شود. بدین منظور نتایج در جدول ۲، بیان شده است:

$$S(A_{m2}, A_{m1}) = \left|\frac{1}{3}[(a_{m2} \ + a_{m2} \ + a_{m3} \ +) - (a_{m1} \ + a_{m2} \ + a_{m3} \ )]\right| \qquad (4)$$

**جدول۲- میانگین دیدگاه‌های خبرگان و فازی زدایی در مرحله اول و دوم**

| ردیف | شاخص‌ها | فازی زدایی (مرحله۱) | فازی زدایی (مرحله۲) | اختلاف مرحله اول و دوم |
|---|---|---|---|---|
| ۱ | تعامل واحدهای درون سازمانی | ۸,۴۶ | ۸,۶۱ | ۰,۱۴ |
| ۲ | تعامل با واحدهای برون سازمانی | ۸,۱۴ | ۸,۲۹ | ۰,۱۴ |
| ۳ | تعامل کارآگاهان با واحدهای پشتیبانی پلیس فتا | ۷,۳۲ | ۷,۵۰ | ۰,۱۸ |
| ٤ | تعامل کارآگاهان پی جویی پرونده با مقام قضایی | ۷,۵۴ | ۷,۶۴ | ۰,۱۱ |
| ۵ | حضور مقامات قضایی در پلیس فتا و پیگیری نزدیک پرونده‌ها | ۵,۸۹ | ۶,۰۷ | ۰,۱۸ |
| ٦ | برگزاری جلسات مشترک | ۵,۷۱ | ۵,۶۱ | ۰,۱۱ |
| ۷ | در اختیار داشتن نرم افزارها و سخت‌افزارهای پیشرفته و به روز (مثل لپ تاب و گوشی) | ۶,۵۷ | ۷,۲۵ | ۰,۶۸ |
| ۸ | استفاده از تجهیزات قابل حمل در جمع‌آوری ادله | ۷,۰۷ | ۷,۱۴ | ۰,۰۷ |
| ۹ | تأمین منابع مالی مورد نیاز | ۶,۴۶ | ۶,۲۵ | ۰,۲۱ |
| ۱۰ | آشنایی مقامات قضایی با شگردهای ارتکاب جرایم | ۶,۶۱ | ۷,۰۰ | ۰,۳۹ |
| ۱۱ | انتصاب قضات با تحصیلات مرتبط | ۷,۱۴ | ۷,۲۱ | ۰,۰۷ |
| ۱۲ | آشنایی قضات با نحوه پی جویی | ۶,۵۴ | ۶,۶۴ | ۰,۱۱ |
| ۱۳ | تجمیع پرونده‌ها در یک دادسرا | ۶,۶۱ | ۷,۴۶ | ۰,۸۶ |
| ۱٤ | آشنایی کاراگاهان با تکنیک و فنون و نحوه تحقیق و بازجویی از متهمان سایبری | ۶,۷۱ | ۷,۰۷ | ۰,۳۶ |
| ۱۵ | نحوه ی جمع‌آوری و مستندسازی دلایل الکترونیکی | ۶,۶۸ | ۷,۲۵ | ۰,۵۷ |

| | | | | |
|---|---|---|---|---|
| ۱۶ | آشنایی با امور فنی رایانه | ۷,۲۱ | ۷,۳۲ | ۰,۱۱ |
| ۱۷ | آشنایی با مبانی حقوقی | ۶,۱۸ | ۶,۱۴ | ۰,۰۴ |
| ۱۸ | نیروی انسانی از نظر کمی | ۶,۵۴ | ۶,۵۴ | ۰,۰۰ |
| ۱۹ | انگیزه پرسنل | ۶,۲۵ | ۶,۳۶ | ۰,۱۱ |
| ۲۰ | آموزش | ۶,۵۴ | ۷,۳۲ | ۰,۷۹ |
| ۲۱ | تخصص و توانایی نیروی انسانی | ۷,۶۴ | ۷,۷۹ | ۰,۱۴ |
| ۲۲ | تجربه | ۶,۱۱ | ۶,۲۵ | ۰,۱۴ |
| ۲۳ | کارگروهی و تیمی | ۶,۶۸ | ۶,۸۶ | ۰,۱۸ |
| ۲۴ | بهره برداری از اقدامات فنی و مخابراتی | ۶,۷۱ | ۷,۱۸ | ۰,۴۶ |
| ۲۵ | وجود بانک‌های اطلاعاتی مجرمین سابقه دار و حوزه فعالیتی آن | ۶,۸۶ | ۷,۰۰ | ۰,۱۴ |
| ۲۶ | دسترسی پلیس فتا به سامانه جامع اطلاعاتی سایر پلیس‌های تخصصی | ۶,۷۱ | ۷,۱۸ | ۰,۴۶ |
| ۲۷ | روش‌های نوین شناسایی IP | ۷,۸۲ | ۷,۸۹ | ۰,۰۷ |
| ۲۸ | دسترسی به اطلاعات مجرمین از طریق اینترنت | ۶,۳۹ | ۶,۹۳ | ۰,۵۴ |
| ۲۹ | دسترسی به اطلاعات مرتبط با جرم از طریق اینترنت | ۶,۱۸ | ۶,۳۶ | ۰,۱۸ |
| ۳۰ | سایت اینترنتی پلیس فتا جهت تبادل اطلاعات | ۶,۱۱ | ۶,۲۹ | ۰,۱۸ |
| ۳۱ | مرکز فوریت‌های سایبری | ۷,۱۸ | ۷,۱۸ | ۰,۰۰ |
| ۳۲ | رصد و پایش سایت‌های اینترنتی و شبکه‌های اجتماعی مجازی | ۶,۷۱ | ۷,۴۳ | ۰,۷۱ |
| ۳۳ | استفاده از منابع و مخبرین | ۵,۸۹ | ۶,۰۰ | ۰,۱۱ |
| ۳۴ | افزایش دسترسی اطلاعاتی | ۷,۵۰ | ۷,۴۶ | ۰,۰۴ |

بدین ترتیب در مرحله سوم، ضمن اعمال تغییرات لازم در شاخص‌ها، پرسشنامه سوم 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 که نتایج آن در جدول۳، ارائه شده است.

**جدول۳- میانگین دیدگاه‌های خبرگان و فازی زدایی در مرحله سوم**

| ردیف | شاخص‌ها | فازی زدایی (مرحله۳) | اختلاف مرحله دوم و سوم |
|---|---|---|---|
| ۱ | در اختیار داشتن نرم افزارها و سخت‌افزارهای پیشرفته و به روز (مثل لپ تاب و گوشی) | ۷,۴۳ | ۰,۱۸ |
| ۲ | تأمین منابع مالی مورد نیاز | ۶,۲۵ | ۰,۰۰ |
| ۳ | آشنایی مقامات قضایی با شگردهای ارتکاب جرایم | ۷,۱۱ | ۰,۱۱ |
| ۴ | تجمیع پرونده‌ها در یک دادسرا | ۷,۴۶ | ۰,۰۰ |
| ۵ | آشنایی کاراگاهان با تکنیک و فنون و نحوه تحقیق و بازجویی از متهمان سایبری | ۷,۰۰ | ۰,۰۷ |
| ۶ | نحوه ی جمع‌آوری و مستندسازی دلایل الکترونیکی | ۷,۱۴ | ۰,۱۱ |
| ۷ | آموزش | ۷,۳۲ | ۰,۰۰ |
| ۸ | بهره برداری از اقدامات فنی و مخابراتی | ۷,۲۱ | ۰,۰۴ |
| ۹ | دسترسی پلیس فتا به سامانه جامع اطلاعاتی سایر پلیس‌های تخصصی | ۷,۲۵ | ۰,۰۷ |
| ۱۰ | دسترسی به اطلاعات مجرمین از طریق اینترنت | ۷,۰۷ | ۰,۱۴ |
| ۱۱ | رصد و پایش سایت‌های اینترنتی و شبکه‌های اجتماعی مجازی | ۷,۴۶ | ۰,۰۳ |

در نهایت مطابق جدول۴، مهمترین عوامل تأثیرگذار در کشف جرایم سایبری، شامل ۲۶ عامل و ۶ گروه می‌باشند:

**جدول٤- عوامل تأثیرگذار در کشف جرایم سایبری**

| ابعاد | عوامل |
|---|---|
| **تعامل سازمانی** | تعامل واحدهای درون سازمانی |
| | تعامل با واحدهای برون سازمانی |
| | تعامل کارآگاهان با واحدهای پشتیبانی پلیس فتا |
| | تعامل کارآگاهان پی جویی پرونده با مقام قضایی |
| **تجهیزات سازمانی** | در اختیار داشتن نرم افزارها و سخت‌افزارهای پیشرفته و به روز (مثل لپ تاب و گوشی) |
| | استفاده از تجهیزات قابل حمل در جمع‌آوری ادله |
| **آشنایی قضات با مبانی فنی و حقوقی** | آشنایی مقامات قضایی با شگردهای ارتکاب جرایم |
| | انتصاب قضات با تحصیلات مرتبط |
| | تجمیع پرونده‌ها در یک دادسرا |
| **توانمندی نیروی انسانی و کارآگاهان** | آشنایی کاراگاهان با تکنیک و فنون و نحوه تحقیق و بازجویی از متهمان سایبری |
| | نحوه ی جمع‌آوری و مستندسازی دلایل الکترونیکی |
| | آشنایی با امور فنی رایانه |
| | آموزش |
| | تخصص و توانایی نیروی انسانی |

| | |
|---|---|
| **فناوری اطلاعات و فضای مجازی** | وجود بانک‌های اطلاعاتی مجرمین سابقه دار و حوزه فعالیتی آن |
| | دسترسی پلیس فتا به سامانه جامع اطلاعاتی سایر پلیس‌های تخصصی |
| | دسترسی به اطلاعات مجرمین از طریق اینترنت |
| | مرکز فوریت‌های سایبری |
| | رصد و پایش سایت‌های اینترنتی و شبکه‌های اجتماعی مجازی |
| | افزایش دسترسی اطلاعاتی |

**بحث و نتیجه گیری**

در این مقاله با توجه به این سؤال که عوامل کلیدی تأثیرگذار بر کشف جرایم سایبری با رویکرد دلفی فازی کدامند، به این موضوع پرداخته شد که با افزایش رویکرد جامعه به فضای مجازی با توجه به رفع محدودیت‌های زمانی و مکانی و تحت تأثیر قرار دادن فعالیت‌های گوناگون اجتماعی، اقتصادی، سیاسی، فرهنگی، علمی و هنری و در نهایت تشکیل ارتباطات فراوان، محیط سایبر در کنار مزایای بی شماری که برای بشر به همراه آورده ناگزیر همراه با معایبی بوده که زمینه سوءاستفاده و بستر مناسبی را در جهت انجام جرم در این محیط به وجود آورده است. بنابراین کشف جرایم سایبری برای حفظ امنیت در این فضا امری ضروری است و عوامل مختلفی به منظور کشف جرایم سایبری وجود دارد.

بنابراین به منظور تعیین عوامل مؤثر بر کشف جرایم سایبری از پرسشنامه و نظرات خبرگان و بازخوردهای حاصل از آن در سه مرحله بهره گرفته شد که در نهایت ۲۶ عامل در ۶ گروه شامل تعامل سازمانی، تجهیزات سازمانی، آشنایی قضات با مبانی فنی و حقوقی، توانمندی نیروی انسانی و کارآگاهان، فناوری‌های نوین ارتباطی؛ و فناوری اطلاعات و فضای مجازی می‌باشند.

طبق یافته‌های این تحقیق تعامل سازمانی، تجهیزات سازمانی، آشنایی قضات با مبانی فنی و حقوقی، توانمندی نیروی انسانی و کارآگاهان عوامل مؤثر در کشف جرایم سایبری می‌باشند و یافته‌های این بخش با یافته‌های تحقیقات نظری منظم و همکاران(۱۳۹۸)، ذبیح الله نژاد(۱۳۹۶)، ورویی و میرزکی(۱۳۹۰) و همچنین عابدینی(۱۳۸۸)، که بیان می‌دارد پلیس برای برخورد با جرائم فضای مجازی، نیروی انسانی متخصص و کاردان تربیت کند، هم راستا می‌باشد. همچنین فناوری‌های نوین ارتباطی شامل بهره برداری از اقدامات فنی و مخابراتی، استفاده از اقدامات فنی موقعیت یابی سارقین سابقه دار از طریق خطوط و ... و

فناوری اطلاعات و فضای مجازی شامل روش‌های نوین شناسایی IP، مرکز فوریت‌های سایبری و ... نیز از جمله عوامل تأثیرگذار در کشف جرایم سایبری هستند که لزوم توجه به آنها با توجه به یافته‌های پژوهش امری ضروری می‌باشد. یافته‌های این بخش از تحقیق با تحقیق توکلی و شاه محمدی(۱۳۹۷)، که یافته‌های آن نشان داد مدیریت فناوری اطلاعات بر بهبود پی جویی جرائم سایبری، افزایش سرعت، افزایش نقش اطلاعات و افزایش دقت پی جویی جرائم سایبری تأثیر دارد و الهی منش و تبریزی(۱۳۹۷)، که بیان می‌دارند پلیس در کشـــف این گونه جرایم با بهره‌گیری از روش‌های علمی و فن‌آوری اطلاعات و جمع‌آوری ادله و مدارک الکترونیکی به دنبال مدارک دیجیتال جهت شناســـائی مجرمان ســـایبری و تبیین شگرد و روش‌های ارتکاب جرم در فضای مجازی با رویکرد جرم شناسانه هستند؛ هم راستا می‌باشد. پیشنهادهای زیر بر اساس عوامل شناسایی شده در کشف جرایم سایبری ارائه می‌گردد:

- تعامل ارگان‌ها و نهادهای دولتی و خصوصی و ســـایر ســـازمان‌های خارج از پلیس فتا با پلیس فتا و تعامل هر چه بیشـــتر کارآگاهان با واحدهای پشـــتیبانی پلیس فتا و مراجع قضایی و لزوم زیرساخت‌های مناسب ارتباطی در این امر؛
- لزوم توجه و تأکید بر تهیه و توســـعه تجهیزات ســـازمانی از قبیل نرم افزارها و ســـخت‌افزارهای پیشرفته و به روز؛
- بـــه کارگیـــری نیروهای متخصص در این زمینه به منظور بهره مندی حداکثری از مهارت‌ها و توانایی‌های تخصصی آنها؛
- لزوم توجه و تأکید بر فناوری‌های نوین ارتباطی به منظور بهره برداری از آن در جهت کشف جرایم سایبری؛
- لزوم توجه و تأکید بر فناوری اطلاعات و افزایش مهارت‌ها و توانایی‌های تخصصی در استفاده و به کارگیری مؤثر و بهینه اطلاعاتِ حوزه فضای مجازی.

**References**

1. ESlami, Ebrahim (1395), "The Position of Supporting the Victims of Cyber Crimes in Local and International Penal Laws", Islamic Law Studies, (1)17, Pages, 157-182.
2. Elahi Manesh, Mohammad Reza and Tabrizi, Sadegh (1397), "Scientific Crime Detection Using Modern and Electronic Evidence (digital)", Karagah Scientific Quarterly, (44) 11, Pages 80-100.
3. Azar Parand, Naser and Niazkhani, Morteza (1393), "Investigating the Effective Factors in Detecting Theft from Governmental Buildings in Alborz Province", Alborz Police Knowledge Quarterly,(3) 2, Pages 79-97.
4. Bell David. (1389), "An Introduction to Cyber Dictionaries (Translated by Masoud Kosari and Husein Hasani)", Tehran, Jamee Shenasan Publications.
5. Tavakoli, Fakhroddin and Shah Mohammadi Gholam Reza (1397), "The Impact of IT Management in Cyber Crime Investigations", Information and Criminal Studies Quarterly, (2) 13, Pages 129-148.
6. Jahanshiri, Javad, Huseini, Seyed Mohammad Reza and Ebrahimi, Ahmad (1394), "Determining the Process of Preliminary Investigations in Cyber Crimes", Information and Criminal Studies Quarterly, (39) 10, Pages 9-34.
7. Khalafi Abouzar (1394), "Cyber Crimes Detection Centering on Crime Detection", Karagah Quarterly, (34) 9, Pages 23-38.
8. Zabi Allah Nejad, Vahid (1397), "Cyber Crime Scientific Detection and the Role of Mazandaran Province Cyber Police in the Field of Prevention and Cyber Security", Mazandaran Police Specialized Scientific Knowledge, (33) 9, Pages 135-170.
9. Zabi Allah Nejad, Vahid (1397), "Nature of Computer and Virtual Crimes (Cyber) and the Role of Cyber Police in Preventing and Detecting These Crimes", Tehran Police Knowledge Quarterly, (34) 10, Pages 8-27.
10. Razavi, Mohammad (1386), "Cyber Crimes and the Role of Police in Preventing These Crimes and Their Detection", Police Knowledge Quarterly, (1) 9, Pages 120-140.
11. Rozehie, Mansour, Tavan Bakhsh, Jafar and Hasan ZAdeh Kord Ahmad, Hamid (1396), "Modern Tools of Preventing Emerging Crimes in Cyberspace", Social Security Studies Quarterly, (50) 8, Pages 1-22.
12. Ziber Olrich (1390), "Cyber Crimes (Translated by Mohammad Ali Nouri, Reza Nakhjavani, Mostafa Bakhtiar Vand and Ahmad Rahimi Moghadam)" ,

Tehran, Ganje Danesh Publicati ons.
13. Abedi, SAdegh and Oryani Bahare (1395), "The Effective Factors in Creating the Phenomenon of Leather Whip in the Supply Chain: Case Study in Qazvin Oil Distribution Company", Energy Policy Making and Planning Studies Quarterly, (5) 2, Pages 75-95.
14. Abedini, Zeinol Abedin (1388), "Crime in Cyberspace: The Necessity of Future Studies", Karagah Quarterly, (9) 3, Pages 144-156.
15. Kahedi, Shahre Banou and Sharafi Tabar Behnam (1395),"The Position of FATA Cyber Police in Crime Prevention in Cyberspace", Central Province Police Knowledge Quarterly, (1) 6, Pages 83-114.
16. Karam Zadeh Esmail (1392), "Police and the Media", Tehran: NAJA University Publications.
17. Gorki Marco (1389), "Cyber Crimes: A Guide for Developing Countries (Translated by Morteza Akbari)", NAJA FATA Police Publications.
18. Mir Sepasi, Naser, Tolouie AShraghi, Abbas, Memar Zadeh Gholam Reza and Peidaie Mr Mehrdad (1389), "Designing a Model of Excellence of Personnel in Iran's Governmental Organizations Using Phase Delphi Technique", Management Studies Magazine, (87) 21, Winter 1389, Pages 1-23.
19. Nazari Monazam. Mahdi, Majidi Abdollah, Hendiani Abdollah and Vafadar Husein (1398), "Investigating the Effective Factors in the Detection of Fraud in Cyberspace", Police Knowledge Studies Quarterly, (2) 21, Pages 217-246.
20. Niazkhani, Morteza, Talebian Husein and Arji Roh Allah (1396), "Assessing the Extent of Efficacy of Scientific Crime Detection Methods in Detecting Burglaries (Case Study: the City of Qazvin)", Qazvin Police Knowledge Quarterly.
21. Varvaie, Akbar and Mirzaki Seyed Shamsodin (1390), "Investigating the Effective Factors in Tehran CID Detection of Fraud in Cyberspace within 1386-76", Karagah Quarterly, (14) 4, Pages 62-87.
22. Hendiani, Abdollah and Morshedi Masoud (1395), "The Position of Future Studies in Crime Detection", Criminal and Information Studies Quarterly, (3) 12, Pages 135-156.
23. Yadgar Nejad, Amin, Habib Zadeh, Ashab and Nik Nafs Ali (1393), "The Role of Information Exchange Management in the Process of Crime Detection", Kerman Police Command, Ploice Knowledge Quarterly, (9) 5, Pages 87-108.
24- McGuire, M & Dowling, S. (2013). "*Cyber crime: A review of the evidence*", Home Office Research Report 75.

# Determining Effective Factors in Cyber Crime Detection with Phase Delphi Approach

*Fakhrodin Tavakoli, Seyed Morteza Mortazavi*

**Abstract**

Features of cyber environment such as lack of dependence on particular time and place, the possibility of obtaining various identities, anonymity and ….. are all factors that make cyber crime commitment more different and cyber crime detection and pinning criminals, more difficult. Therefore; this research has been conducted with the aim of determining effective factors in the detection of cyber crimes. The research method is of applied type from objective perspective and of descriptive-survey type from implementation perspective. The statistical community of this research is formed by 12 NAJA Cyber Police Experts. The data collection tools is a questionnaire made based on library studies, reviewing early studies and experts' views and among which, their most vital ones have been selected. In regards to the nature of this research, Excel software was used to analyze the collected data. The findings of the research show that the most effective factors in cyber crime detection, among 26 factors and 6 groups, include organizational interaction, organic equipment, judges' familiarization with technical and legal principles, personnel and detectives' capabilities, modern communications technologies, IT and cyberspace. The findings show that in detecting cyber crimes, such issues as organizational interaction, organic equipment, judges' familiarization with the technical and legal principles, personnel and detectives' capabilities, modern communications technologies, IT and cyberspace should be taken into considerations.

Key Words: Cyberspace, Cyber crimes, Cyber Crimes Detection, Phase Delphi