

تأثیر مدیریت فناوری اطلاعات در پی‌جویی جرائم سایبری^۱

تاریخ پذیرش: ۹۷/۰۲/۳۰

تاریخ دریافت: ۹۶/۱۰/۱۶

از صفحه ۱۲۹ تا ۱۴۸

فخرالدین توکلی^۱، غلامرضا شاه‌محمدی^۳

چکیده

امروزه فناوری اطلاعات و ارتباطات تأثیر بسزایی در زندگی مردم جامعه داشته است. تشکیل فضای جدیدی به نام فضای مجازی، دنیایی است که فعالیت‌های گوناگون اجتماعی، اقتصادی، سیاسی، فرهنگی، علمی و هنری را تحت تأثیر قرار داده و موجب افزایش رویکرد جامعه به آن شده است. محیط سایبر، محیطی مخفی با ویژگی‌هایی از قبیل عدم وابستگی به زمان و مکان خاص، امکان تحصیل هویت‌های گوناگون، گمنامی و سهولت انجام اعمال مختلف است که موجب مهاجرت بسیاری از جرائم به فضای مجازی شده است. هدف این پژوهش، بررسی تأثیر مدیریت فناوری اطلاعات در پی‌جویی جرائم سایبری است. روش پژوهش حاضر از نظر هدف، کاربردی و از نظر روش اجرا، پیمایشی است. جامعه آماری این تحقیق را کارشناسان، متخصصان و صاحب‌نظران مطلع حوزه فناوری اطلاعات و ارتباطات پلیس فتا ناجا در سال ۱۳۹۵ به تعداد ۳۰۰ نفر تشکیل می‌دهند که به صورت تمام شمار انتخاب شدند. ابزار گردآوری داده‌ها، پرسشنامه محقق ساخته است که متناسب با موضوع و فرضیه‌های تحقیق تنظیم شده است. برای تجزیه و تحلیل فرضیه‌ها، از آزمون T تک نمونه‌ای و همچنین آزمون رتبه‌بندی فریدمن استفاده شد. نتایج نشان داد که با توجه به حجم گسترده مأموریت‌های ناجا، مدیریت فناوری اطلاعات بر بهبود پی‌جویی جرائم سایبری، افزایش سرعت، افزایش نقش اطلاعات و افزایش دقت پی‌جویی جرائم سایبری تأثیر دارد که پیشنهادهایی نیز برای افزایش نقش فناوری اطلاعات در پی‌جویی جرائم سایبری ارائه شد.

کلیدواژه‌ها: مدیریت فناوری اطلاعات، فضای مجازی، پی‌جویی، جرائم سایبری.

استناد: توکلی، فخرالدین و شاه محمدی، غلامرضا (تابستان ۱۳۹۷). تأثیر مدیریت فناوری اطلاعات در پی‌جویی جرائم سایبری. فصلنامه پژوهش‌های اطلاعاتی و جنایی. ۱۳(۵۰)، صص ۱۴۸-۱۲۹.

۱. مستخرج از پایان‌نامه کارشناسی ارشد فرماندهی و مدیریت انتظامی دانشگاه علوم انتظامی امین

۲. کارشناسی ارشد فرماندهی و مدیریت انتظامی دانشگاه علوم انتظامی امین، Fakhroddin.tavakoli@chmail.ir

۳. دانشیار دانشگاه علوم انتظامی امین، نویسنده مسئول: Drshahmohammadi@chmail.ir

مقدمه

با پیدایش رایانه، اینترنت و فناوری‌های مرتبط با آن در اقصی نقاط جهان، شبکه عظیمی از اطلاعات و سیستم‌های ارتباطی تشکیل شده که امروزه از آن به فضای مجازی تعبیر می‌شود. فضای مجازی، مرزهای فردی، اجتماعی و فرهنگی را در نور دیده و تا بدان جا پیش رفته که گاه غالب بر فضای واقعی شده است. این دستاورد بشری از هنگامی که قدم به زندگی انسان گذاشته، در عرصه‌های مختلفی نقش‌آفرینی می‌کند و تحولات شگرفی در روند فعالیت جامعه بشری به وجود آورده است؛ به گونه‌ای که امروزه دیگر انجام بسیاری از فعالیت‌های روزمره بدون آن میسر نیست (بهزاد، ۱۳۹۵، ص ۹۴). رایانه‌ها با توجه به قابلیت‌های بسیار زیاد مانند دقت بالا، سرعت زیاد، قابلیت ذخیره‌سازی حجم زیاد اطلاعات، تبادل سریع اطلاعات، دسترسی آسان و محاسن بی‌شمار دیگر، امکانات زیادی را در اختیار بشر قرار داده است و از منظر دیگر، با گسترش اینترنت و ظهور فضای مجازی، به دلیل ویژگی‌های خاص این فضا، مانند امکان تحصیل هویت‌های گوناگون، گمنامی و سهولت انجام اعمال مختلف، ضمن مهاجرت بسیاری از جرائم از فضای فیزیکی به فضای مجازی، موجب بروز جرائم جدیدی نیز شده است که قابل مقایسه با هیچ یک از جرائم موجود کلاسیک نبوده و چه بسا از نظر دامنه تأثیر، خطرناک‌تر است (شاه‌محمدی و تاهو، ۱۳۹۳، ص ۱۰۰).

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 سازمان‌یافتگی جرائم ارتكابی توسط مجرمان حرفه‌ای در فضای سایبر و همچنین گستردگی به‌کارگیری روش‌های علمی و فنی و دستیابی به امکانات و ابزارهای مختلف تسهیل‌کننده در وقوع جرم توسط این مجرمان و تأثیرهای منفی بی‌شماری که این جرائم بر زندگی افراد جامعه می‌توانند تحمیل کنند، مقابله جدی و مؤثر پلیس را می‌طلبد که با توسل به مدرن‌ترین وسایل، بتواند توان مقابله با مجرمانی که مرتکب این جرائم می‌شوند را داشته باشد. بهره‌گیری مفید از فناوری اطلاعات به‌عنوان یک منبع و ابزار در کنار سایر منابع و ابزارها، موضوع مهمی است که با گسترش حجم سرمایه‌گذاری‌ها بر فناوری اطلاعات، نقش مضاعف پیدا می‌کند (نصر اصفهانی، ۱۳۹۰، ص ۳۴).

در شرایط حاضر، ضرورت و اهمیت پی‌جویی جرائم سایبری در برابر انواع تهدیدات و تهاجمات بر کسی پوشیده نیست و برای حفظ امنیت عمومی ضروری است. این امر با وجود وسعت جغرافیایی کشور و گسترش ارتکاب جرائم سایبری، بدون تجهیز پلیس به فناوری اطلاعات و ارتباطات و ابزارهای نوین پی‌جویی و کشف جرائم سایبری امکان‌پذیر نیست و هر اندازه نیروهای پلیس در این فضا با تکیه بر سه اصل سرعت، دقت و صحت بتوانند قدرت عمل خود را در پی‌جویی و پیشگیری از جرائم و ناهنجاری‌ها نشان دهند، از زمینه‌های گسترش نا امنی کاسته می‌شود. گستره و میزان استفاده از فناوری اطلاعات در سازمان‌ها و گروه‌های مختلف مردم با سرعت بالایی همراه است و مجرمان سایبری نیز با برخورداری از دانش فناورانه و ویژگی‌های منحصر به فرد فضای مجازی، به ارتکاب جرائم سایبری مبادرت می‌ورزند؛ به نحوی که اگر اهتمام ویژه‌ای صرف مبارزه با جرائم سایبری مبتنی بر فناوری اطلاعات و ارتباطات نشود، به‌طور قطع، توان کاهش آمار رو به رشد جرائم سایبری میسر نخواهد شد. لازمه چنین حرکتی، وجود آگاهی و شناخت نسبت به تأثیر گسترده فناوری اطلاعات در مأموریت‌های مختلف ناجا و از آن جمله، مدیریت جرائم سایبری است.

برابر اعلام رئیس پلیس فتا در نشست خبری، مبنی بر افزایش جرائم فضای مجازی در سال ۱۳۹۶، وی اظهار داشته است: 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 (روزنامه ایران، ۱۳۹۷). دلایل افزایش جرائم سایبری را می‌توان در مواردی همچون ضعف در بهره‌گیری مناسب از فناوری اطلاعات و نبود مدیریت مناسب بر فناوری اطلاعات به منظور استفاده مناسب از آن، برای کشف و پیشگیری از جرائم سایبری دانست که هر دو دلیل، به‌صورت مستقیم و غیرمستقیم بر نبود مدیریت مناسب بر فناوری اطلاعات به منظور بهره‌برداری مناسب از فناوری اطلاعات برای کشف و پیشگیری از جرائم سایبری تکیه دارد. با توجه به این موارد و از آنجا که مدیریت فناوری به عنوان اداره‌کننده تمامی منابع فناوری سازمان‌ها، مطابق با نیازمندی‌ها و اولویت‌های فناورانه، می‌تواند نقش برجسته‌ای در کلیه حوزه‌ها از جمله پی‌جویی جرائم سایبری داشته باشد، این تحقیق به دنبال بررسی تأثیر مدیریت فناوری اطلاعات در پی‌جویی جرائم سایبری است.

بررسی تحقیقات مرتبط نشان می‌دهد، تاکنون هیچ تحقیقی به موضوع تأثیر مدیریت فناوری اطلاعات در پی‌جویی جرائم سایبری پرداخته است و این تحقیق مقدمه مطالعات آتی در حوزه بررسی تأثیر مدیریت فناوری اطلاعات در سایر حوزه‌ها است.

جهانشیری و همکاران (۱۳۹۴)، در مقاله‌ای به تبیین فرآیند تحقیقات مقدماتی در جرائم سایبری پرداخته‌اند. به دلیل اهمیت فرآیند پی‌جویی در تحقیقات قضایی و رسیدگی به علل وقوع و کشف جرم در این تحقیق، تلاش بر آن است تا فرآیند تحقیقات مقدماتی جرائم سایبری در کشور بررسی شود. این مقاله در بحث اقدامات قبل از وقوع جرم، موضوع پیشگیری، اطلاع‌رسانی و آموزشی و در حین و بعد از وقوع جرم سایبری، پی‌جویی و مبارزه با جرائم، شناسایی مجرم و شگرد مجرمان و جمع‌آوری دلایل و مدارک و اموال مالباخته در کنار رعایت اصول قانونی و حقوقی را کاملاً ضروری می‌داند. اسراری و مشیر احمدی (۱۳۹۴) نیز در مقاله‌ای به نقش پلیس در حفظ حریم خصوصی فضای سایبر پرداخته‌اند. مقاله حاضر تبیین می‌کند که پلیس فضای تولید و تبادل اطلاعات (فتا) می‌تواند به موازات اقدامات تقنینی، با اخذ تدابیر پیشگیرانه، نقشی مؤثر در شناسایی و مقابله با این‌گونه جرائم ایفا کند.

شاه‌محمدی و اکباتانی (۱۳۹۴)، در مقاله‌ای، روشی برای پیشگیری از آسیب‌های فضای مجازی مبتنی بر فناوری اطلاعات ارائه دادند. نتایج این تحقیق نشان داد که در زمینه راهکارهای پیشگیری مبتنی بر فناوری اطلاعات از آسیب‌های فضای مجازی، مؤلفه‌های پیشگیری مبتنی بر اطلاع‌رسانی امنیتی، پیشگیری مبتنی بر روش‌های پایشی، پیشگیری مبتنی بر امن‌سازی و پیشگیری مبتنی بر ایجاد و استفاده از ابزارهای بومی در فضای مجازی در پیشگیری از مسائل فضای مجازی تأثیرگذار است. همچنین، شاه‌محمدی و تاهو (۱۳۹۳)، در مقاله‌ای دیگر با عنوان «بررسی شیوه‌های پیشگیری از جرائم سایبری؛ مبتنی بر فناوری اطلاعات»، نشان دادند که شیوه‌های مبتنی بر فناوری اطلاعات شامل ردیابی هویت مجازی مهاجمان، گشت مجازی و نظارت بر فضای سایبر، جمع‌آوری ادله الکترونیکی جرم و مستندسازی صحنه جرم در پیشگیری از جرائم سایبر تأثیر دارد.

احمدوند و عطایی جعفری (۱۳۸۳)، در مقاله‌ای به بررسی نقش و راهبرد فناوری اطلاعات در سیستم پلیس و فضاهای مجازی جرائم در ایران پرداخته‌اند. این مقاله سعی در بررسی نقش فناوری اطلاعات در سیستم پلیس و فضاهای مجازی جرائم در ایران و

تدوین راهبرد فناوری اطلاعات در سیستم پلیس جمهوری اسلامی ایران دارد. در نتایج این تحقیق آمده است، با توجه به نقش اطلاعات در سازمان‌های پلیسی و به‌طور خاص پلیس ایران، تدوین راهبرد در حوزه نظم و امنیت عمومی ضروری به نظر می‌رسد. همان‌گونه که مشاهده می‌شود، با وجود تحقیقات متعددی که به مباحث فضای مجازی پرداخته شده است، اما هیچ تحقیقی، مشابه تحقیق حاضر به موضوع تأثیر مدیریت فناوری اطلاعات در پی‌جویی جرائم سایبری نپرداخته است.

فناوری اطلاعات: واژه فناوری اطلاعات اولین بار از سوی لویت و وایزler^۱ در سال ۱۹۵۸ به منظور بیان نقش رایانه در پشتیبانی از تصمیم‌گیری‌ها و پردازش اطلاعات در سازمان بکار گرفته شد (حاجی‌زاده، ۱۳۸۹، ص ۲). فناوری اطلاعات، دانشی است که برای توصیف فناوری‌هایی به کار می‌رود که ما را در ضبط، ذخیره‌سازی، پردازش، بازیابی، انتقال و دریافت اطلاعات یاری می‌دهد و شامل سخت‌افزار، نرم‌افزار، مغز افزار (انسان افزار) و شبکه افزار است و موضوع آن کاربرد سیستم‌های اطلاعات، ارتباطات و رایانه است (بهان و هولمز، ۱۳۸۸، ص ۱۳). همان‌طور که به‌وسیله انجمن فناوری اطلاعات آمریکا (ITAA)^۲ تعریف شده است، «فناوری اطلاعات، به مطالعه، طراحی، توسعه، پیاده‌سازی، پشتیبانی یا مدیریت سامانه‌های اطلاعاتی مبتنی بر رایانه، به‌خصوص برنامه‌های نرم‌افزاری و سخت‌افزاری رایانه می‌پردازد». به‌طور کوتاه، فناوری اطلاعات با مسائلی مانند استفاده از رایانه‌های الکترونیکی و نرم‌افزار سروکار دارد تا تبدیل، ذخیره، حفاظت، پردازش، انتقال و بازیابی اطلاعات به شکلی مطمئن و امن انجام پذیرد (محمدی مقدم و معدنی، ۱۳۹۴، ص ۴). اجزای فناوری اطلاعات عبارتند از: ارتباطات^۳، رایانه^۴ و مهارت فنی^۵ که نقش رایانه در توسعه فناوری اطلاعات به مراتب پررنگ‌تر از نقش ارتباطات است (طالبیان، ۱۳۹۱، ص ۱۳۹). فناوری اطلاعات در «عصر اطلاعات» با سرعت فزاینده در چهار بعد سخت‌افزاری، نرم‌افزاری، داده‌ها و مخابرات در حال پیشرفت و دگرگونی است (مدهوشی، ۱۳۸۲، ص ۲۱۲).

مدیریت فناوری اطلاعات^۶ (ITM): دانشی میان‌رشته‌ای است که در آن، تمام منابع

1. Leavitt & whisler

2. Information Technology Association of America

3. Communications

4. Computer

5. Know How

6. Information Technology Management

فناوری، مطابق با نیازها و اولویت‌های فناورانه نوین، اداره می‌شود. این منابع ممکن است شامل سرمایه‌گذاری‌های محسوس مانند نرم‌افزار، داده‌ها، شبکه و امکانات مرکز داده که توسط کارکنان از آن منابع نگهداری می‌شود، باشد. مسئولیت مدیریت فناوری اطلاعات در یک شرکت شامل بسیاری از توابع اساسی مدیریت‌هایی مانند بودجه، نیروی انسانی و سازمان‌دهی و کنترل است و همراه با مواردی که به فناوری مربوط است، مانند مدیریت تغییر، طراحی نرم‌افزار، برنامه‌ریزی شبکه، پشتیبانی فنی و غیره (مک نورلین و همکاران^۱، ۲۰۰۹). مدیریت فناوری اطلاعات، روندی است که به موجب آن تمام منابع مربوط به فناوری اطلاعات با توجه به اولویت‌ها و نیازهای سازمان اداره می‌شود. این مدیریت، شامل منابع محسوس مانند شبکه، کامپیوتر و تجهیزات داده و همچنین به‌عنوان منابع نامشهود مانند نرم‌افزار و داده‌های وسیع است. هدف اصلی مدیریت فناوری اطلاعات برای تولید ارزش از طریق استفاده از فناوری است. برای رسیدن به این هدف، استراتژی‌های کسب و کار و فناوری باید هم تراز شوند.

پلیس و فناوری اطلاعات: استفاده سازمان پلیس از فناوری اطلاعات و ارتباطات نه تنها متخصصان فناوری اطلاعات و کارکنانی که فناوری اطلاعات را در محیط کارشان به طور منظم استفاده می‌کنند، تحت تأثیر قرار داده، بلکه محیط سازمان، خود سازمان و به‌طور کلی دنیای اجتماعی مرتبط با سازمان پلیس را نیز تحت تأثیر قرار داده است. فرماندهان و مدیران باید از این تغییرات آگاهی یافته و برای درک و سازگاری مناسب با آن‌ها تلاش کنند (مردی، ۱۳۹۴، ص ۱۱۱). در حقیقت، در سازمان پلیس، فناوری اطلاعات و ارتباطات شامل مجموعه‌ای از سخت‌افزار و نرم‌افزار است که گردش اطلاعات را میسر ساخته و بهره‌برداری از آن را فراهم می‌سازد. فناوری اطلاعات و ارتباطات سازمان پلیس را قادر کرده است که آنچه را انجام می‌دهند، تغییر دهند و حتی نحوه انجام عمل را نیز دگرگون سازند. با توجه به رشد روز افزون این فناوری و استفاده مفید از این فنون نوین، پلیس وارد عرصه جدیدی شده است (مردی، ۱۳۹۴، ص ۱۰۱). امروزه تقریباً هریک از بخش‌های پلیس از نوعی سامانه فناوری اطلاعات استفاده می‌کند. از سویی، مسئولان برای کارآمدی بیشتر، استفاده از فناوری اطلاعات را امری ضروری می‌دانند؛ زیرا فراگیری استفاده از فناوری اطلاعات و تغییر شکل جرائم سنتی به جرائم الکترونیکی ایجاب

1. McNurlin

می‌کند، اطلاعات طبقه‌بندی شده و داده‌های ارزشمند در مقابل تهدید مجرمان حمایت شود (محمدی مقدم و معدنی، ۱۳۹۴، ص ۶)؛ برای مثال، پلیس نیاز دارد که از فناوری اطلاعات برای مبارزه با انواع جرم‌هایی که توسط این فناوری ایجاد می‌شود، از قبیل سرقت نرم‌افزار رایانه‌ای، حمله‌های هکرها و سرقت هویت وبلاگی استفاده کند. علاوه بر این، سازمان‌های پلیس از فناوری اطلاعات برای تکالیف اجرایی از قبیل بودجه‌بندی و تخصیص منابع و وظایفی از قبیل بررسی جرم، تحلیل جرم، جرم‌نگاری، دسترسی به اینترنت، فراهم آوردن اطلاعات برای نیروهای پلیس و ثبت مشخصات کارکنان استفاده می‌کند (مرادی، مهرانی و برومند، ۱۳۸۹، ص ۸۰).

فضای مجازی: از لحاظ لغوی، سایبر به معنی مجازی و غیرملموس است. فضای سایبر در معنا به مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق رایانه و مسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود (اسلامی، ۱۳۹۵، ص ۱۵۹). این فضا به عنوان مجموعه تعامل‌های انسان‌ها از طریق رایانه و فناوری‌های نوین ارتباطات، بدون در نظر گرفتن «زمان» و «مکان»، توسط ویلیام گیبسون^۱ نویسنده داستان علمی تخیلی در کتاب «نورومونسر»^۲ در سال ۱۹۸۴ به کار برده شد. وی فضای سایبر را بازنمایی گرافیکی از داده‌ها از نظام‌های رایانه‌ای می‌داند. این سخن درستی است که با گسترش استفاده از مفهوم نوین سایبر، هر آنچه پس یا پیش از واژه سایبر قرار گیرد، به‌نوعی به بیان رابطه انسان و رایانه می‌پردازد. در عین حال، رویکردهای گوناگون به فضای سایبر قابل‌انکار نیست. مفهوم فضای سایبر، معطوف به فضای ساختگی و خیالی واقعیت مجازی و اینترنت است که انسان از طریق آن به فضای واقعیت مجازی وارد می‌شود. بدون فناوری، فضای سایبر بی‌معنا خواهد بود (خانیک و بابائی، ۱۳۹۰، صص ۷۶-۷۷). 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، ۱۳۸۹، صص ۲۲-۲۳). فضای سایبر در کنار برخورداری از مزایا و اثرات مثبت فراوان، منشأ تهدیداتی جدی برای کلیه افراد، سازمان‌ها و کشورهای جهان از توسعه‌یافته و غیر توسعه‌یافته شده است

1. William Gibson
2. Neuromancer

(جلالی، ۱۳۹۱، ص ۷). امروزه بسیاری از جرائم سنتی، هم‌زمان با پیشرفت فناوری اطلاعات و ارتباطات به شدت متحول شده و به جرائم سایبری تبدیل شده‌اند (پرویزی، ۱۳۸۴، ص ۴۶). محیط سایبر، محیطی مخفی است و مجرمان سایبری از این فضا به منزله کانون مخفی امن و مطمئن خود بهره می‌گیرند. جرم سایبری را می‌توان هرگونه رخداد توأم و انجام شده با فناوری رایانه که موجب می‌شود، بزه دیده متحمل ضرر بالقوه یا بالفعل شود و مرتکب، عمداً توانسته یا خواهد توانست چیزی کسب کند، تعریف کرد (فتحیان و مهدوی نور، ۱۳۸۹، ص ۲۷۳).

جرائم سایبری: جرم عبارت است از هر فعل یا ترک فعلی که در قانون برای آن مجازات تعیین شده است و جامعه با ابزار مجازات، آن را نکوهش می‌کند (اردبیلی، ۱۳۸۰، ص ۱۲۰). امروزه بسیاری از جرائم سنتی، هم‌زمان با پیشرفت فناوری اطلاعات و ارتباطات، به شدت متحول شده و به جرائم سایبری تبدیل شده‌اند (پرویزی، ۱۳۸۴، ص ۴۶). جرائم سایبری در اصطلاح به جرائمی گفته می‌شود که در محیطی غیر فیزیکی علیه فناوری اطلاعات ارتکاب می‌یابند (رضوی، ۱۳۸۶، ص ۱۲۲). طبق تعریف ارائه شده از سوی گروهی از کارشناسان سازمان همکاری و توسعه اقتصادی در سال ۱۹۸۳، جرائم رایانه‌ای را «هر عمل غیرقانونی، غیراخلاقی یا غیرمجاز نسبت به پردازش خودکار یا انتقال داده‌ها» عنوان کرده‌اند (زیبر^۱، ۱۳۹۰، ص ۱۸). فعالیت‌های به‌واسطه رایانه که هم غیرقانونی و هم نامشروع هستند، با بخش‌های خاص می‌توانند از میان شبکه‌های الکترونیک جهانی هدایت شوند (گرکی^۲، ۱۳۸۹، ص ۳۲).

با گسترش استفاده از اینترنت به عنوان ابزار ورود به فضای مجازی، با توجه به «محدود نبودن فضای مجازی به مکان و زمان خاص، گسترش استفاده روز افزون کودکان، نوجوانان و جوانان و آحاد جامعه از این فضا، عدم اشراف خانواده‌ها به این فضا و آسیب‌های آن، اندک بودن تعداد سازمان‌های مروج فرهنگ اصیل اسلامی و سازمان‌های مسئول مبارزه و پاسخگو به انواع و اقسام شبهات و اندیشه‌های الهادی و انحرافی موجود در این فضا، امکان حضور افراد با چهره‌های غیرواقعی و فریب کارانه و در نهایت، سهولت و گستردگی ارتکاب انواع و اقسام سوءاستفاده‌ها و کلاهبرداری‌ها در این فضا»، انواع جرائم

1. Sieber Ulrech
2. Marco Gercke

آسیب‌ها، تهدیدها و کلاهبرداری‌ها در این فضا ظهور یافته که تبعات ناشی از آن خیلی گسترده‌تر از فضای فیزیکی و با توجه به آمار موجود در پلیس فتا، با گذشت زمان بر میزان وقوع انواع جرائم در فضای مجازی و آسیب‌ها، افزوده می‌شود (شاه‌محمدی و اکباتانی، صص ۲۹-۳۰).

پی‌جویی جرائم سایبری: پی‌جویی یا پیگیری انتظامی، مجموعه اقداماتی است که پلیس تحت نظارت و تعلیمات مقام قضایی در کشف جرم، بازجویی مقدماتی، حفظ آثار و دلایل جرم، جلوگیری از فرار و مخفی شدن متهم و تشکیل پرونده قضایی در چهارچوب قانون و اصول و فنون انتظامی انجام می‌دهد (گل محمدی خامنه، ۱۳۸۵، ص ۶). در فضای سایبر، همان‌گونه که فعالیت‌ها، سریع‌تر و ارزان‌تر انجام می‌شود، جرائم نیز پیچیده‌تر، سریع‌تر و کم‌هزینه‌تر است. برای مثال، در دنیای واقعی، محیط فیزیکی، محدودیت‌ها و موانع بزرگی را برای مجرمان و تبهکاران ایجاد می‌کند، اما در فضای سایبر چنین موانع فیزیکی وجود ندارد. پس لازم است در سطح ملی، منطقه‌ای و بین‌الملل، توجه کامل به مراحل زمانی وقوع جرم اعم از (قبل، حین و پس از وقوع جرم) انجام و با آمادگی لازم نسبت به تدوین فرآیندهای عملیات نسبت به پیش‌بینی، پیشگیری، تشخیص و مبارزه و مقابله با جرائم سایبری اقدام شود.

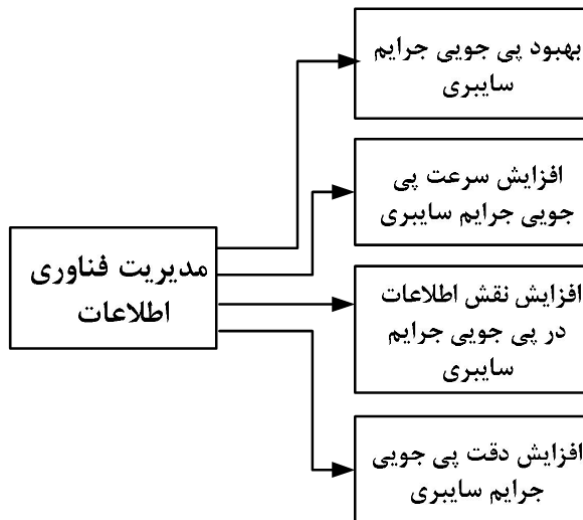
در مرحله قبل از وقوع، مأموریت با رصد، پایش و تشخیص تهدیدها، آسیب‌ها و جرائم احتمالی اقدامات عملی می‌شود. پیشگیری از وقوع جرم، نوعی پی‌جویی و مقابله است. در حین وقوع، تأثیر جرم کامل نشده است و پلیس برای مقابله وارد عمل می‌شود و تلاش برای ممانعت از ادامه فعالیت مجرمانه می‌کند. در مرحله بعد از وقوع نیز پلیس و دستگاه قضایی با تجسس و پاسخگویی عمل کرده و به منظور تکمیل تحقیقات و پرونده، وارد مرحله تعقیب مجرمان براساس این مراحل می‌شود: الف) اخذ مجوز قضایی؛ ب) تشکیل تیم تحقیق؛ ج) تحقیق در مورد جرم سایبری (بازرسی صحنه جرم، شناسایی هویت در فضای سایبر، ادله الکترونیک، بازجویی از مظنونان)؛ د) استفاده از کارشناسان فنی رایانه به‌عنوان مشاور و ه) بازسازی صحنه جرم.

در بخش دوم قانون جرائم رایانه‌ای مصوب ۱۳۸۸/۰۳/۰۵ مجلس شورای اسلامی، ضمن اشاره به آیین دادرسی، مراحل تحقیقات مقدماتی و پی‌جویی جرائم سایبری اعم از مباحث صلاحیت‌ها، جمع‌آوری ادله جرم و استناد پذیری اشاره شده است (جهانشیری و همکاران، ۱۳۹۴، صص ۲۳-۲۱).

جدول ۱ - مستندات قانونی در موضوع پی‌جویی جرائم سایبری کشور (جهانشیری و همکاران، ۱۳۹۴، ص 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؛ ب) ارتکاب جرم از طریق تارنماهای (وبسایت‌های) دارای دامنه کد کشوری ایران؛ ج) جرم توسط هر ایرانی یا غیر ایرانی در خارج از ایران علیه سامانه‌های رایانه‌ای و مخابراتی و تارنماها (وبسایت‌ها)؛ د) سوءاستفاده از اشخاص کمتر از ۱۸ سال، اعم از آنکه مرتکب یا زه‌دهیده، ایرانی یا غیرایرانی باشد.
	ماده ۲۹	صلاحیت دادسرای محل کشف، چنانچه محل وقوع آن معلوم نباشد.
جمع‌آوری ادله الکترونیکی	مواد ۳۲ و ۳۳	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 داده‌های رایانه‌ای ذخیره‌شده برای تحقیق یا دادرسی خطر آسیب دیدن یا تغییر یا از بین رفتن داده‌ها
	ماده ۳۵	ارائه داده‌ها در اختیار قرار دادن داده‌های حفاظت‌شده 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، با روش‌هایی از قبیل چاپ داده‌ها، کپی‌برداری یا تصویربرداری.
	ماده ۴۸	شوند محتوای ارتباطات غیر عمومی در حال انتقال ارتباطات غیر عمومی در سامانه‌های رایانه‌ای یا مخابراتی و دسترسی به محتوای ارتباطات غیر عمومی ذخیره‌شده نظیر پست الکترونیکی یا پیامک.
	ماده ۴۹	حفظ صحت و تمامیت، اعتبار و انکارناپذیری ادله الکترونیکی جمع‌آوری شده مطابق آئین‌نامه.
	ماده ۵۲	سامانه رایانه‌ای یا مخابراتی به‌عنوان وسیله ارتکاب جرم باشد و در قانون جرائم رایانه‌ای مجازات پیش‌بینی نشده باشد، مطابق قوانین جزائی عمل خواهد شد. در مواردی که برای رسیدگی به جرائم رایانه‌ای، مقررات خاصی از جهت آئین دادرسی پیش‌بینی نشده است، طبق مقررات قانون آئین دادرسی کیفری اقدام خواهد شد.

با توجه مطالعات انجام‌شده، نمودار ۱، مدل مفهومی تحقیق را نشان می‌دهد.



نمودار ۱ - مدل مفهومی تحقیق

روش‌شناسی تحقیق

این پژوهش از نظر هدف، کاربردی و با ماهیت پیمایشی است. در این تحقیق، جهت جمع‌آوری اطلاعات در زمینه مبانی نظری و ادبیات تحقیق موضوع، از مطالعات کتابخانه‌ای و جهت جمع‌آوری داده‌ها و اطلاعات، از روش میدانی استفاده شد. جامعه آماری این تحقیق را کارشناسان، متخصصان و صاحب‌نظران مطلع حوزه فناوری اطلاعات و ارتباطات پلیس فتا ناجا در سال ۱۳۹۵ تشکیل می‌دهند که تعداد آن‌ها ۳۰۰ نفر است و از شیوه تمام شماری جهت پاسخگویی به سؤالات استفاده شد. ابزار گردآوری داده‌ها، پرسش‌نامه محقق ساخته است که متناسب با موضوع تحقیق و فرضیه‌های اصلی و فرعی بر مبنای طیف لیکرت تنظیم شده است. به منظور تعیین روایی محتوایی، پرسش‌نامه تهیه شده در اختیار اساتید و متخصصان و خبرگان با تجربه قرار گرفت و اصلاحات و تغییرات موردنظر اعمال و پرسش‌نامه نهایی تدوین شد. برای محاسبه پایایی این پرسش‌نامه، از ضریب آلفای کرونباخ استفاده شد. بدین منظور، ضریب آلفای کرونباخ برای هر بخش به طور جداگانه محاسبه می‌شود:

جدول ۲ - ضریب آلفای کرونباخ

شماره سؤال	مقدار ضریب
۶-۱	۰/۸۱۱
۱۴-۷	۰/۷۶۴
۱۹-۱۵	۰/۷۷۲
۲۶-۲۰	۰/۷۵۲

همچنین، ضریب آلفای کرونباخ برای کل پرسش‌نامه، ۰/۷۹۴ به دست آمد. بنابراین، با توجه به مقدار ضریب آلفای کرونباخ، قابلیت اعتماد به پرسش‌نامه قابل قبول است.

یافته‌های تحقیق

در خصوص توصیف جمعیت شناختی یافته‌ها، از تعداد ۳۰۰ نفر، ۶۱ درصد پاسخگویان ۲۰ الی ۳۰ ساله، ۳۶/۳۳ درصد ۳۰ الی ۴۰ ساله و ۲/۶۷ درصد ۴۰ الی ۵۰ ساله و همگی آن‌ها مرد هستند. همچنین، ۱۵/۳۳ درصد پاسخگویان فوق‌دیپلم، ۷۵/۳۳ درصد لیسانس و ۹/۳۴ درصد دارای مدرک فوق‌لیسانس هستند. در خصوص سابقه خدمت نیز ۶۹/۶۷ درصد پاسخگویان زیر ۱۰ سال، ۲۷/۶۷ درصد ۱۰ الی ۲۰ سال و ۲/۶۶ درصد بالاتر از ۲۰ سال سابقه خدمت دارند.

برای سنجش فرضیه‌های پژوهش از آزمون تی تک نمونه استفاده می‌شود. فرضیه اول: مدیریت فناوری اطلاعات بر بهبود پی‌جویی جرائم سایبری تأثیر دارد. داده‌های حاصل از جدول ۳ نشان می‌دهد که میانگین نمونه از میانگین نظری بزرگ‌تر است. همچنین، سطح معناداری از $0/05$ کمتر است. بنابراین، فرض صفر در این آزمون رد می‌شود و می‌توان چنین استنباط کرد که مدیریت فناوری اطلاعات بر بهبود پی‌جویی جرائم سایبری تأثیر مثبت دارد و فرضیه اول تأیید می‌شود.

جدول ۳- نتایج حاصل از آزمون تی تک نمونه تأثیر مدیریت فناوری اطلاعات بر بهبود پی‌جویی جرائم سایبری

Test Value = ۳						
گوبه	فراوانی	میانگین	انحراف استاندارد	مقدار آماره	درجه آزادی	سطح معنی‌داری
۱	۳۰۰	۴/۳۷۲۳	۰/۴۸۴۵	۰/۸۴۷۸۱	۲۹۹	۰/۰۰۰
۲	۳۰۰	۴/۱۲۶۷	۰/۷۵۶۶	۲۵/۷۹۰	۲۹۹	۰/۰۰۰
۳	۳۰۰	۴/۱۲۰۰	۰/۷۰۲۷	۲۷/۶۰۳	۲۹۹	۰/۰۰۰
۴	۳۰۰	۴/۴۱۶۷	۰/۴۹۳۸	۴۹/۶۸۸	۲۹۹	۰/۰۰۰
۵	۳۰۰	۴/۲۸۰۰	۰/۴۴۹۷	۴۹/۲۹۵	۲۹۹	۰/۰۰۰
۶	۳۰۰	۴/۰۸۳۳	۰/۸۴۷۸	۲۲/۱۳۲	۲۹۹	۰/۰۰۰

همچنین، جدول ۴ رتبه‌بندی فریدمن برای تأثیر مدیریت فناوری اطلاعات بر شاخص‌های پی‌جویی جرائم سایبری را نشان می‌دهد. مطابق داده‌های این جدول، شاخص‌های افزایش کارایی فرآیندهای پی‌جویی و افزایش کنترل فرآیند پی‌جویی دارای بالاترین رتبه را هستند.

جدول ۴- رتبه‌بندی فریدمن برای تأثیر مدیریت فناوری اطلاعات بر شاخص‌های پی‌جویی جرائم سایبری

گوبه	شاخص‌های پی‌جویی جرائم سایبری	میانگین رتبه‌ای
۱	افزایش کنترل فرآیند پی‌جویی	۳/۹۲
۲	بهبود فرآیند تصمیم‌گیری در واحدها	۳/۱۸
۳	تسهیل تجزیه و تحلیل اطلاعات جرم	۳/۱۶
۴	افزایش کارایی فرآیندهای پی‌جویی	۴/۰۵
۵	بهبود و افزایش سطح توانایی پی‌جویی جرائم سایبری	۳/۶۴
۶	بهبود ارتباط بین واحدهای مختلف در پی‌جویی	۳/۰۵

فرضیه دوم: مدیریت فناوری اطلاعات بر افزایش سرعت پی‌جویی جرائم سایبری تأثیر دارد.

داده‌های حاصل از جدول ۵ نشان می‌دهد که میانگین نمونه از میانگین نظری بزرگ‌تر است و همچنین سطح معناداری از $0/05$ کمتر است. بنابراین، فرض صفر در این آزمون رد می‌شود و می‌توان چنین استنباط کرد که مدیریت فناوری اطلاعات بر افزایش سرعت

پی‌جویی جرائم سایبری تأثیر مثبت دارد. بنابراین، فرضیه دوم تأیید می‌شود.

جدول ۵- نتایج حاصل از آزمون تی تک نمونه تأثیر مدیریت فناوری اطلاعات بر افزایش سرعت پی‌جویی جرائم سایبری

Test Value = ۳						
گویه	فراوانی	میانگین	انحراف استاندارد	مقدار آماره	درجه آزادی	سطح معنی‌داری
۷	۳۰۰	۱۷۳۳/۴	۳۷۹۱۷/۰	۵۹۸/۵۳	۲۹۹	۰/۰۰۰
۸	۳۰۰	۴۹/۴	۵۰۰۷۴/۰	۵۳۹/۵۱	۲۹۹	۰/۰۰۰
۹	۳۰۰	۳۹/۴	۴۸۸۵۶/۰	۲۷۸/۴۹	۲۹۹	۰/۰۰۰
۱۰	۳۰۰	۰۰۳/۴	۷۴۷۳۴/۰	۲۵۳/۲۳	۲۹۹	۰/۰۰۰
۱۱	۳۰۰	۹۷۶۷/۳	۵۰۶۹۳/۰	۳۷۰/۳۳	۲۹۹	۰/۰۰۰
۱۲	۳۰۰	۳۸/۴	۴۸۶۲/۰	۱۶۲/۴۹	۲۹۹	۰/۰۰۰
۱۳	۳۰۰	۲۱/۴	۶۹۳۴۲/۰	۲۲۴/۳۰	۲۹۹	۰/۰۰۰
۱۴	۳۰۰	۹۶۶۷/۳	۸۰۰۶۴/۰	۹۱۲/۲۰	۲۹۹	۰/۰۰۰

همچنین، جدول ۶ رتبه‌بندی فریدمن برای تأثیر مدیریت فناوری اطلاعات بر افزایش سرعت پی‌جویی جرائم سایبری را نشان می‌دهد. مشاهده می‌شود که شاخص‌های افزایش سرعت رصد و پایش سایت‌های اینترنتی و شبکه‌های اجتماعی و تشخیص جرم در فضای مجازی، دارای بالاترین رتبه هستند.

جدول ۶- رتبه‌بندی فریدمن برای تأثیر مدیریت فناوری اطلاعات بر افزایش سرعت پی‌جویی جرائم سایبری

گویه	شاخص‌های سرعت پی‌جویی جرائم سایبری	میانگین رتبه‌ای
۷	افزایش سرعت کنترل و نظارت بر ارائه‌دهندگان سرویس‌های اینترنتی	۴/۴۰
۸	افزایش سرعت رصد و پایش سایت‌های اینترنتی و شبکه‌های اجتماعی در فضای مجازی	۵/۶۷
۹	افزایش سرعت تشخیص جرم در فضای مجازی	۵/۲۷
۱۰	افزایش سرعت پیشگیری از فعالیت‌های مجرمانه در فضای مجازی	۳/۷۲
۱۱	افزایش سرعت اقدامات لازم در زمینه تشکیل پرونده قضایی	۳/۶۱
۱۲	افزایش سرعت مستندسازی صحنه جرم سایبری در فضای مجازی	۵/۲۳
۱۳	افزایش سرعت جمع‌آوری ادله جرائم سایبری	۴/۵۵
۱۴	کاهش زمان تصمیم‌گیری	۳/۵۷

فرضیه سوم: مدیریت فناوری اطلاعات بر افزایش نقش اطلاعات در فرآیند پی‌جویی جرائم سایبری تأثیر دارد.

داده‌های حاصل از جدول ۷ نشان می‌دهد که میانگین نمونه از میانگین نظری بزرگ‌تر است. همچنین، سطح معناداری از ۰/۰۵ کمتر است. بنابراین، فرض صفر در این آزمون رد می‌شود و می‌توان چنین استنباط کرد که مدیریت فناوری اطلاعات بر افزایش نقش اطلاعات در پی‌جویی جرائم سایبری تأثیر مثبت دارد و فرضیه سوم تأیید می‌شود.

جدول ۷- نتایج حاصل از آزمون تی تک نمونه تأثیر مدیریت فناوری اطلاعات بر افزایش نقش اطلاعات در

فرآیند پی‌جویی جرائم سایبری

Test Value = ۳						
گویه	فراوانی	میانگین	انحراف استاندارد	مقدار آماره	درجه آزادی	سطح معنی داری
۱۵	۳۰۰	۹۱۳۳/۳	۷۷۵۳۴/۰	۴۰۳/۲۰	۲۹۹	۰/۰۰۰
۱۶	۳۰۰	۴۴/۴	۴۹۷۲۲/۰	۱۶۲/۵۰	۲۹۹	۰/۰۰۰
۱۷	۳۰۰	۳۷/۴	۴۸۳۶۱/۰	۰۶۶/۴۹	۲۹۹	۰/۰۰۰
۱۸	۳۰۰	۹۸۳۳/۳	۶۷۶۶۹/۰	۱۶۹/۲۵	۲۹۹	۰/۰۰۰
۱۹	۳۰۰	۳۶/۳	۴۸۰۸/۰	۴۸/۹۹۳	۲۹۹	۰/۰۰۰

همچنین، جدول ۸ رتبه‌بندی فریدمن برای تأثیر مدیریت فناوری اطلاعات بر افزایش نقش اطلاعات در فرآیند پی‌جویی جرائم سایبری را نشان می‌دهد. مشاهده می‌شود که شاخص‌های سهولت دسترسی به اطلاعات مرتبط با جرم و افزایش توانایی انتخاب اطلاعات، دارای بالاترین رتبه هستند.

جدول ۸- رتبه‌بندی فریدمن برای تأثیر مدیریت فناوری اطلاعات بر افزایش نقش اطلاعات

در فرآیند پی‌جویی جرائم سایبری

گویه	شاخص‌های نقش اطلاعات در فرآیند پی‌جویی جرائم سایبری	میانگین رتبه‌ای
۱۵	ایجاد بانک اطلاعات مجرمین، شگردها و سوابق جرائم و به‌کارگیری در پی‌جویی جرم	۲/۲۵
۱۶	سهولت دسترسی به اطلاعات مرتبط با جرم	۳/۵۷
۱۷	افزایش سرعت دسترسی به اطلاعات جرائم	۳/۳۹
۱۸	افزایش توانایی انتخاب اطلاعات	۲/۴۳
۱۹	طبقه‌بندی اطلاعات و تهیه گزارشات در پی‌جویی	۳/۳۷

فرضیه چهارم: مدیریت فناوری اطلاعات بر افزایش دقت پی‌جویی جرائم سایبری تأثیر دارد.

داده‌های حاصل از جدول ۹ نشان می‌دهد که میانگین نمونه از میانگین نظری بزرگ‌تر است. همچنین، سطح معناداری از ۰/۰۵ کمتر است. بنابراین، فرض صفر در این آزمون رد می‌شود و می‌توان چنین استنباط کرد که مدیریت فناوری اطلاعات بر افزایش دقت پی‌جویی جرائم سایبری تأثیر مثبت دارد و فرضیه چهارم تأیید می‌شود.

جدول ۹ - نتایج حاصل از آزمون تی تک نمونه تأثیر مدیریت فناوری اطلاعات بر افزایش دقت

پی‌جویی جرائم سایبری

Test Value = ۳						
گوبه	فراوانی	میانگین	انحراف استاندارد	مقدار آماره	درجه آزادی	سطح معنی‌داری
۲۰	۳۰۰	۴/۳۲۶۷	۰/۴۶۹۷۸	۴۸/۹۱۴	۲۹۹	۰/۰۰۰
۲۱	۳۰۰	۴/۴۷	۰/۴۹۹۹۳	۵۰/۹۲۹	۲۹۹	۰/۰۰۰
۲۲	۳۰۰	۴/۲۶	۰/۴۳۹۳۷	۴۹/۶۷۱	۲۹۹	۰/۰۰۰
۲۳	۳۰۰	۳/۸۷۶۷	۰/۶۹۵۰۳	۲۱/۸۴۷	۲۹۹	۰/۰۰۰
۲۴	۳۰۰	۳/۹۹	۰/۶۵۶۷۶	۲۶/۱۰۹	۲۹۹	۰/۰۰۰
۲۵	۳۰۰	۳/۹۸۶۷	۰/۶۰۰۸۵	۲۸/۴۴۲	۲۹۹	۰/۰۰۰
۲۶	۳۰۰	۴/۴۵۶۷	۰/۴۹۸۹۵	۵۰/۵۶۷	۲۹۹	۰/۰۰۰

همچنین، جدول ۱۰ رتبه‌بندی فریدمن برای تأثیر مدیریت فناوری اطلاعات بر افزایش دقت پی‌جویی جرائم سایبری را نشان می‌دهد. مشاهده می‌شود که افزایش دقت رصد و پایش سایت‌های اینترنتی و شبکه‌های اجتماعی در فضای مجازی و افزایش دقت جمع‌آوری ادله جرائم سایبری، دارای بالاترین رتبه هستند.

جدول ۱۰ - رتبه‌بندی فریدمن برای تأثیر مدیریت فناوری اطلاعات بر افزایش دقت پی‌جویی جرائم سایبری

گوبه	شاخص‌های دقت پی‌جویی جرائم سایبری	میانگین رتبه‌ای
۲۰	افزایش دقت کنترل و نظارت بر ارائه‌دهندگان سرویس‌های اینترنتی	۴/۴۶
۲۱	افزایش دقت رصد و پایش سایت‌های اینترنتی و شبکه‌های اجتماعی در فضای مجازی	۴/۹۶
۲۲	افزایش دقت تشخیص جرم در فضای مجازی	۴/۲۳
۲۳	افزایش دقت جلوگیری از فعالیت‌های مجرمانه در فضای مجازی	۲/۸۹
۲۴	افزایش دقت اقدامات لازم در زمینه تشکیل پرونده قضایی	۳/۲۸
۲۵	افزایش دقت مستندسازی صحنه جرائم سایبری در فضای مجازی	۳/۲۷
۲۶	افزایش دقت جمع‌آوری ادله جرائم سایبری	۴/۹۲

بحث و نتیجه‌گیری

در این مقاله تأکید شد که فضای سایبر با وجود مزایا و اثرات مثبت فراوان، منشاء تهدیدهایی جدی برای افراد، سازمان‌ها و کشورهای جهان است و بسیاری از جرائم سنتی با پیشرفت فناوری اطلاعات و ارتباطات به شدت متحول شده و به جرائم سایبری تبدیل شده‌اند. از طرفی، اشاره شد که فناوری اطلاعات بر ابعاد مختلف زندگی بشر تأثیرگذار بوده و با گذشت زمان، گستره و میزان این تأثیر در حال افزایش است. همچنین، اشاره شد که مدیریت فناوری اطلاعات به‌عنوان اداره‌کننده تمامی منابع فناوری مطابق با نیازمندی‌ها و اولویت‌های فناورانه، می‌تواند نقش برجسته‌ای در کلیه حوزه‌ها از جمله پی‌جویی جرائم سایبری داشته باشد. لذا در این تحقیق، به بررسی تأثیر فناوری اطلاعات

در پی جویی جرائم سایبری پرداخته شد.

با توجه به نتایج این پژوهش، مدیریت فناوری اطلاعات باعث افزایش نقش اطلاعات در پی جویی جرائم سایبری می‌شود که به سهولت دسترسی به اطلاعات مرتبط با جرم و افزایش سرعت دسترسی به اطلاعات جرائم، می‌توان اشاره کرد. با وجود سیاست‌های عام و مشترک موجود در کشف تمام جرائم، به دلیل وجود تفاوت‌های ماهوی میان محیط فیزیکی و فضای مجازی، روش‌های پی‌جویی و کشف جرائم سایبری نیز متفاوت خواهد بود. برای مثال، صحنه جرائم ارتكابی در محیط فیزیکی، به‌طور معمول، متمرکز بوده و پراکندگی جغرافیایی نخواهند داشت، اما در جرائم سایبری، پراکندگی جغرافیایی صحنه جرم بسیار زیاد و معمولاً دور از هم است. دلایل ارتكاب جرائم سایبری، غالباً ادله الکترونیک است که با سرعت قابل‌ملاحظه‌ای، امکان تغییر و از بین بردن آن‌ها وجود دارد. در فضای سایبر، همانگونه که فعالیت‌ها سریع‌تر و ارزان‌تر انجام می‌شود، جرائم نیز پیچیده‌تر، سریع‌تر و کم‌هزینه‌تر است. بنابراین، سرعت عمل و دقت در پی‌جویی جرائم سایبری بسیار ضروری است. مدیریت فناوری اطلاعات نیز موجب افزایش سرعت و دقت پی‌جویی جرائم سایبری در مواردی از قبیل افزایش سرعت رصد و پایش سایت‌های اینترنتی و شبکه‌های اجتماعی در فضای مجازی، افزایش سرعت تشخیص جرم در فضای مجازی، افزایش دقت رصد و پایش سایت‌های اینترنتی و شبکه‌های اجتماعی در فضای مجازی و افزایش دقت جمع‌آوری ادله جرائم سایبری می‌شود. از آنجا که گشت زنی و مراقبت در فضای مجازی، تا حدی از وقوع جرائم سایبری پیشگیری می‌کند، در نتیجه، مدیریت فناوری اطلاعات نقش مؤثری در این امر ایفا می‌کند. بررسی نتایج حاصل از تحقیقات انجام شده، با توجه به موضوع پژوهشی حاضر (نقش مدیریت فناوری اطلاعات در پی‌جویی جرائم سایبری) و نظر به اینکه حضور و به‌کارگیری فناوری اطلاعات، سبب شده است تا نتایج ارزنده و رضایت‌بخشی به وجود آید که از جمله آن، می‌توان به بهبود پی‌جویی جرائم سایبری، افزایش سرعت، افزایش نقش اطلاعات و افزایش دقت پی‌جویی جرائم سایبری اشاره داشت. لذا نتایج این پژوهش با بررسی جهانشیری و همکاران (۱۳۹۴) که به تبیین فرآیند تحقیقات مقدماتی در جرائم سایبری پرداخته‌اند و 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 جرائم، شناسایی مجرم و شگرد مجرمان و جمع‌آوری دلایل و مدارک و اموال مالباخته در کنار رعایت

اصول قانونی و حقوقی کاملاً ضروری می‌دانند، هم‌راستا است. همچنین، با تحقیقات احمدوند و عطایی جعفری (۱۳۸۳) که به بررسی نقش و راهبرد فناوری اطلاعات در سیستم پلیس و فضاهای مجازی جرائم در ایران پرداختند و نقش فناوری اطلاعات را دارای اهمیت دانستند، هم‌راستا است. مدیریت فناوری اطلاعات بر پی‌جویی جرائم سایبری تأثیر مثبتی دارد و لذا این نقش را می‌توان در افزایش کارایی و کنترل فرآیند پی‌جویی، افزایش سرعت و دقت رصد و پایش سایت‌های اینترنتی و شبکه‌های اجتماعی در فضای مجازی، افزایش سرعت تشخیص جرم در فضای مجازی، سهولت دسترسی به اطلاعات مرتبط با جرم، افزایش سرعت دسترسی به اطلاعات جرائم و افزایش دقت جمع‌آوری ادله جرائم سایبری مشاهده کرد. مدیریت فناوری اطلاعات در پی‌جویی جرائم سایبری نقش مؤثری دارد و سبب تعیین استراتژی مناسب و تحقق نظم و امنیت اجتماعی می‌شود. با توجه به نتایج بیان شده، پیشنهادهای زیر ارائه می‌شود:

- لزوم توجه و تأکید بر فناوری اطلاعات و مدیریت آن، با توجه به نقش مؤثری که در پی‌جویی جرائم سایبری داشته و در نتایج این تحقیق بیان شد؛

- تدوین راهبرد فناوری اطلاعات در حوزه نظم و امنیت عمومی با توجه به اهمیت نقش مدیریت فناوری اطلاعات؛

- استانداردسازی وضعیت فناوری اطلاعات در دستگاه‌های دولتی و خصوصی به منظور افزایش ارتقای سطح مراقبتی و امنیتی سیستم‌ها و جلوگیری از نفوذ غیرمجاز به سیستم‌های مذکور با محوریت پلیس فتا ناجا؛

- نظارت و کنترل بر سایت‌های اینترنتی و شبکه‌های اجتماعی در فضای مجازی با تبیین نقش مدیریت فناوری اطلاعات در این زمینه؛

- به‌کارگیری مؤثر اطلاعات توسط مدیران و متخصصان با در نظر گرفتن تأثیر مدیریت فناوری اطلاعات بر افزایش نقش اطلاعات در فرآیند پی‌جویی جرائم سایبری؛

- به‌کارگیری و آموزش نیروهای متخصص و ارتقای سطح علمی در زمینه مدیریت فناوری اطلاعات در امر پی‌جویی جرائم سایبری؛

- لزوم به‌کارگیری ابزارها و روش‌های نوین برای پی‌جویی جرائم سایبری؛

- تعامل ارگان‌ها و نهادهای دولتی و خصوصی با پلیس فتا در برنامه‌ریزی برای برگزاری کلاس‌های آگاه‌سازی و ارائه راهکارهای پیشگیرانه در زمینه جرائم سایبری.

منابع

منابع فارسی

- احمدوند، علی محمد و عطایی جعفری، امیرمسعود (پاییز و زمستان ۱۳۸۳). نقش و راهبرد فناوری اطلاعات (IT) در سیستم پلیس و فضاهای مجازی جرائم در ایران. *فصلنامه توسعه سازمانی پلیس*. ۱(۳)، صص ۵-۲۸. بازیابی از: <http://journals.police.ir/content.php>
- اردبیلی، محمدعلی (۱۳۸۰). حقوق جزای عمومی. تهران: انتشارات میزان.
- اسراری، مهناز و مشیر احمدی، علیرضا (۱۳۹۴). نقش پلیس در حفظ حریم خصوصی فضای سایبر. همایش ملی سبک زندگی، نظم و امنیت. دانشگاه زنجان. بازیابی از: https://www.civilica.com/Paper-LSOS01-LSOS01_126.html
- اسلامی، ابراهیم (بهار و تابستان ۱۳۹۵). جایگاه حمایت از بزه‌دیدگان جرائم سایبری در مقررات کیفری حقوق داخلی و حقوق بین‌الملل. *پژوهشنامه حقوق اسلامی*. ۱۷(۱)، صص ۱۵۷-۱۸۲. بازیابی از: <http://www.ensani.ir/fa/content/360092/default.aspx>
- بل، دیوید (۱۳۸۹). درآمدی بر فرهنگ‌های سایبر (مسعود کوثری و حسین حسینی، مترجمان). تهران: انتشارات جامعه شناسان.
- بهان، کیت و هولمز، دیانا (۱۳۸۸). *آشنایی با تکنولوژی اطلاعات* (مجید آذرخش و جعفر مهرداد، مترجمان). تهران: انتشارات سمت
- پرویزی، رضا (۱۳۸۴). *پی‌جویی جرائم رایانه‌ای*. تهران: انتشارات جهان جام جم.
- جلالی، علی‌اکبر (زمستان ۱۳۹۱). رفتارشناسی مجرمان در فضای سایبر. *فصلنامه کارآگاه*. ۶(۲۱)، صص ۶-۲۵. بازیابی از: <http://journals.police.ir/content.php>
- جهانشیری، جواد؛ حسینی، سید محمدرضا و ابراهیمی، احمد (پاییز ۱۳۹۴). تبیین فرآیند تحقیقات مقدماتی در جرائم سایبری. *فصلنامه پژوهش‌های اطلاعاتی و جنایی*. ۱۰(۳)، صص ۹-۳۴. بازیابی از: <http://journals.police.ir/content.php>
- حاجی‌زاده، پیمان (۱۳۸۹). سطح همسویی استراتژی فناوری اطلاعات و استراتژی کسب‌وکار سازمان. *چهارمین کنفرانس ملی مدیریت تکنولوژی ایران*. بازیابی از: www.sid.ir/fa/VEWSSID/s_pdf/24513890488.pdf
- خانیکی، هادی و بابائی، محمود (پاییز و زمستان ۱۳۹۰). فضای سایبر و شبکه‌های اجتماعی؛ مفهوم و کارکردها. *فصلنامه انجمن ایرانی مطالعات جامعه‌اطلاعاتی*. ۱(۱)، صص ۷۱-۹۶. بازیابی از: <https://irandoc.ac.ir/article/786>

- رضوی، محمد (بهار ۱۳۸۶). جرائم سایبری و نقش پلیس در پیشگیری از این جرائم و کشف آن‌ها. *فصلنامه دانش انتظامی*. ۹(۱)، صص ۱۲۰-۱۴۰. بازیابی از: <http://fa.journals.sid.ir/ViewPaper.aspx?id=74998>
- روزنامه ایران (۱۳۹۷). *افزایش جرائم فضای مجازی*. نشست خبری رئیس پلیس فتا با خبرنگاران. دهم اردیبهشت‌ماه. بازیابی از: <http://yon.ir/k9aUo>
- زیبر، اولریش (۱۳۹۰). *جرائم رایانه‌ای (محمدعلی نوری، رضا نخجوانی، مصطفی بختیاروند و احمد رحیمی مقدم، مترجمان)*. تهران: انتشارات گنج دانش.
- شاه‌محمدی، غلامرضا و اکباتانی، سمیه (بهار ۱۳۹۴). پیشگیری مبتنی بر فناوری اطلاعات از آسیب‌های فضای مجازی. *پژوهش‌های نظم و امنیت انتظامی*. ۸(۱)، صص ۲۹-۳۹. بازیابی از: <http://yon.ir/urYMP>
- شاه‌محمدی، غلامرضا و تاهو، منصور (پاییز ۱۳۹۳). بررسی شیوه‌های پیشگیری از جرائم سایبری، مبتنی بر فناوری اطلاعات. *فصلنامه پژوهش‌های اطلاعاتی و جنایی*. ۹(۳)، صص ۹۹-۱۱۹. بازیابی از: <http://fa.journals.sid.ir/ViewPaper.aspx?id=251136>
- طالبیان، حسین (تابستان ۱۳۹۱). تبیین فرآیند تشکیل ابر اطلاعاتی پلیس در کشف جرم. *فصلنامه کارآگاه*. ۵(۱۹)، صص ۱۲۶-۱۵۷. بازیابی از: <http://journals.police.ir/content.php>
- فتحیان، محمد و مهدوی نور، سید حاتم (۱۳۸۹). *مبانی و مدیریت فناوری اطلاعات*. تهران: انتشارات دانشگاه علم و صنعت ایران.
- گل محمدی خامنه، علی (۱۳۸۵). *پی‌جویی انتظامی*. تهران: دانشگاه علوم انتظامی امین.
- گرگی، مارکو (۱۳۸۹). *جرائم سایبری؛ راهنمایی برای کشورهای در حال توسعه* (مرتضی اکبری، مترجم). تهران: انتشارات پلیس فضای تولید و تبادل اطلاعات ناجا. بازیابی از: <https://www.cyberpolice.ir/en/node/1191>
- محمدی مقدم، یوسف و معدنی، جواد (پاییز ۱۳۹۴). فناوری اطلاعات در پشتیبانی از پلیس جامعه‌محور. *فصلنامه توسعه مدیریت منابع انسانی و پشتیبانی*. ۱۰(۳۷)، صص ۱-۳۸. بازیابی از: <http://journals.police.ir/content.php>
- مدهوشی، مهرداد (زمستان ۱۳۸۱ و بهار ۱۳۸۲). نقش نظام اطلاعاتی و فناوری اطلاعات در تصمیم‌گیری مؤثر. *دوفصلنامه علوم انسانی دانشگاه الزهراء (س)*. ۱۳(۴۵) و

- ۴۶)، صص ۱۹۳-۲۱۷. بازیابی از: <http://fa.journals.sid.ir/ViewPaper.aspx?id=1211>
- مرادی، مرتضی؛ مهرانی، کامینه و برومند، مجتبی. (بهار ۱۳۸۹). بررسی عوامل مؤثر بر پذیرش فناوری اطلاعات از سوی نیروهای پلیس، دو ماهنامه توسعه انسانی پلیس. (۷)، صص ۲۸. بازیابی از: <http://www.sid.ir/FileServer/JF/30913882804>
- مردی، صفر (بهار ۱۳۹۴). بررسی نقش فناوری اطلاعات در افزایش بهره‌وری کارکنان ناجا. فصلنامه توسعه مدیریت منابع انسانی و پشتیبانی. ۱۰(۳۵)، صص ۹۷-۱۱۶. بازیابی از: <http://journals.police.ir/content.php>
- نصر اصفهانی، محمد و ترابی، حمیده (بهار ۱۳۹۰). ارزیابی عملکرد سازمان‌های مبتنی بر فناوری اطلاعات (IT). نشریه مدیریت فردا. ۱۰(۲۶)، صص ۳۳-۵۴. بازیابی از: <http://www.ensani.ir/fa/content/285967/default.aspx>

منابع انگلیسی

- McNurlin, B., Sprague, R. and Bui, T. (2009). Information Systems Management in Practice, 8th edition, Prentice Hall.