فصلنامه پژوهش‌های حفاظتی ـ امنیتی دانشگاه جامع امام حسین(علیه‌السلام)
سال سوم، شماره‌ی ۱۳ (بهار ۱۳۹۴): صص ۶۹ – ۸۹

نقش آموزش کارکنان در پیشگیری از جرائم فضای مجازی (مطالعه موردی کارکنان فرماندهی انتظامی تهران بزرگ)

سعید کوچی[۱]
ابراهیم داودی[۲]

تاریخ دریافت: ۱۳۹۳/۰۹/۲۰
تاریخ پذیرش: ۱۳۹۳/۱۱/۰۵

چکیده

این پژوهش با هدف شناخت جایگاه آموزش در ارتقای توانمندی کارکنان در پیشگیری از وقوع جرم در فضای مجازی و برای حفاظت از این فضا و پیشگیری از جرائم خاص فضای مجازی انجام گرفته است. قدر مسلم، این یکی از پژوهش‌هایی است که می‌تواند مدیران را در کاهش وقوع جرائم رایانه‌ای در فضای مجازی رهنمون سازد. در این راستا از روش توصیفی و کاربردی استفاده شده است. با استفاده از آمار توصیفی و استنباطی، داده‌ها تجزیه شده و فرضیه‌های پژوهش، مورد بررسی و تحلیل قرار گرفته است.

جامعهٔ آماری این تحقیق، رؤسا، فرماندهان، مدیران رده‌های میانی، کارشناسان فنی و کارکنان مرتبط فاتب بالغ بر ۲۰۰ نفر بوده و حجم جامعه نمونه ۴۴ نفر است. براساس یافته‌های پژوهش، به‌کارگیری نیروی انسانی متخصص و متعهد و آموزش‌دیده در کنار به کارگیری تجهیزات مدرن و بومی باعث پیشگیری از وقوع جرائم در فضای مجازی می‌شود و در آخر می‌توان نتیجه گرفت که آموزش کارکنان در خصوص جرائم رایانه‌ای و آشنا نمودن آنان با قوانین مربوط با این دسته از جرائم بسیار مهم بوده و با استفاده از دانش فضای مجازی می‌توان میزان خطرپذیری را در تصمیم‌گیری مدیران، به اندازه قابل توجهی کاهش داد.

کلید واژه‌ها: *آموزش، پیشگیری، جرم، فضای مجازی، فرماندهی انتظامی تهران بزرگ*

۱- مربی دانشگاه علوم انتظامی، کارشناس ارشد پدافند غیر عامل از دانشگاه فارابی - s.koochi@chmail.ir
۲- مربی دانشگاه علوم انتظامی، دانشجوی دکتری پیشگیری از جرم دانشگاه علوم انتظامی - davoodi57@chmail.ir

مقدمه

جرائم رایانه‌ای، جرائمی وارداتی هستند که با ورود رایانـه در اسـتفاده از اینترنـت بـه مقیـاس گسـترده درکشور رواج پیداکرده است. ورود اینترنت به کشور از سال ۱۳۷۰، آغاز شد و در سال ۱۳۷۲ به تکامل رسید اما در این چند سال، نبود قوانینی مدون باعث گردید که بسیاری از مجرمین رایانه ای از زیر مجـازات فـرار کرده و به جرائم خود ادامه دهند و استناد آنها نیز به اصل برائت و اصل قانونی بودن جرم و مجازات بود که استناد درستی هم به شمار می رفت. با تصویب قانون جرائم رایانه‌ای در سال ۱۳۸۸، مفاهیم و جرائم تازه‌ای درحقوق کیفری ایران خلق شد که هر یک نیازمند بررسی‌های دقیق وکارشناسانه می‌باشد. وقتی درخصوص فناوری بحث می‌شود، نمی‌توان رایانه را نادیده گرفت. رایانه، هم بزرگترین فناوری عصر حاضر است و هـم سایر فناوری‌های نوین به وسیله آن و یا بر بستر آن شکل می‌گیرند. البته فناوری‌ها در کنـار مزایـای خـود می‌توانند بسترساز سوء استفاده‌هایی نیز باشند. به خصوص اگر این فناوری، رایانه باشد، دامنه خطرهـای آن افزایش می‌یابد. حقوق کیفری نوین، امروزه با جرائم و مجرمان رایانه‌ای طرف است. ماهیت و ویژگـی ایـن دسته از جرائم به نحوی اساسی با جرائم سنتی تفاوت دارد. امروزه، مجرمان رایانه‌ای در مکان‌هایی به غیـر از نقاطی‌که آثار و نتایج اعمال آنها ظاهرمی‌شود، قرار دارند. درصورتی که کـارایی قـوانین جزایـی موجـود و متداول، منحصر به قلمرو خاصی است و به دلیل آن که اجزای عنصر مادی کـاملاً یـا بعضـاً تغییـر یافتـه و برخی عناوین مجرمانه تازه هم به وجود آمده است، نمی‌توان مجرمان را با قوانین قبلی محاکمه کرد.

با رشد و گسترش فناوری‌های اطلاعاتی و ارتباطی و دسترسی عموم جامعه به شبکه اینترنت در قالـب چت روم ها، فضای جدیدی فراروی کاربران قرارگرفته است؛ فضـایی کـه در آن محـدودیت‌هایی همچـون مرزهای جغرافیایی، ملیت، بعدمسافت، زمان و ... فاقد معنا و مفهوم اسـت. باگسـترش و توسـعه ایـن فضـا، جرائم رایانه‌ای مرتبط با امور غیر اخلاقی نیز گسترش یافته و تأثیر منفـی بـر نظـام اجتمـاعی و پایـه‌ای – مخصوصاً خانواده ها– گذاشته و بیشتر کودکان و نوجوانان را مورد هجوم قرارداده است و شرایط لازم برای ارتکاب برخی جرائم به منظور اشاعه این مفاسد را آماده ساخته است. امـروزه حفـظ امنیـت ملـی کشـور در ردیف یکم اولویت حکومت‌ها قرار داشته و هر کدام برای تأمین آن، تمامی تلاش خود را به کـار می‌گیرنـد تا این امنیت را برای عموم مردم کشور خود فراهم ساخته و به پشتوانه آن استقلال و تمامیت ارضی کشـور را حفظ کنند. با این حال گاهی اوقات از طریق تهدیدهای فضای مجازی شرایطی به کشور تحمیل می‌شود که این امنیت، از جهات مختلف با تهدید و قانون‌شکنی مواجه می‌شود که بخشی از این تهدیـد بـا رویکـرد داخلی و بخشی با رویکرد خارجی قابل تفسیر و ارزیابی است. در رویکردهای داخلـی بـه‌طور عمـده، شـکل تهدید نامشخص و تشخیص آن سخت است. شناسایی عوامـل مـؤثر در ارتقـا آمـوزش کارکنـان پلـیس در

برخورد با جرائم در این فضا باعث می‌شود تا پلیس، در پیشگیری از وقوع جرم و مقابلـه بـا جـرائم، برخـورد مؤثرتری نموده و در نتیجه به‌طور مستقیم باعث ارتقای امنیت در این فضا خواهد شد. به کارگیری فنـاوری اطلاعات در حوزه پلیسی به دلایل مختلفی از جمله به کارگیری آن توسط حریفان، اجتنـاب ناپـذیر بـوده و باید کارشناسان با موضوعات مختلف فناوری آشنایی کافی داشته باشند. برای همین منظور نیاز است که در ساختار سازمانی فاتب[1]، توجه ویژه به این امر صورت گرفته و به منظـور تربیـت کارشناسـان خبـره در ایـن حوزه، اقدامات بهینه‌سازی مؤثر صورت گیرد و آموزش و ارتقای سطح علمی کـاربران پلـیس در فرمانـدهی انتظامی تهران بزرگ مد نظر قرار گیرد.

یکی از راه‌کارهای کاهش جرائم فضای مجازی، پرداختن به آموزش‌هـای پیشـگیری از وقـوع جـرم در فضای مجازی برای کارکنان است. به‌طور حتم، از ایـن طریـق مـی‌تـوان کـارایی کارکنـان را افـزایش داد. وضعیت فضای مجازی و نوع استفاده مجرمان از این فضا در گسترش جرائم، در کنـار ضـعف آموزش‌هـای کارکنان، غافلگیری در پیشگیری و مقابله با آن‌ها را به‌دنبال خواهـد داشـت. آشـکار شـدن اهمیـت فضـای مجازی برای فرماندهان و رؤسا، باعث به کـارگیری و تهیـه تجهیـزات مـدرن و پیشـرفته در ایـن حـوزه و برنامه‌ریزی ارائه آموزش‌های نوین به کارکنان خواهد شد. برای بالابردن کارایی کارکنان در محیط مجـازی و به منظور پیشگیری از وقوع جرم می بایست جایگاه آموزش در این حوزه را مشخص کرد. حال با توجه به اهمیت این موضوع در فضای مجازی، شناسایی عواملی که باعث می‌شود عملکرد پلیس در این حوزه ارتقـا یابد، از اهمیت به‌سزایی برخوردار است. چه بسا مواردی همچون رشد روز افزون نرم افزارهای کلاه بـرداری و جاسوسی که در اختیار مجرمان قرار دارد، طمع مجرمان به منظور سوءاستفاده از ایـن فضـا بـرای اهـداف شوم خود، پایین بودن سطح علمی عموم شهروندان از تهدیدهای ایـن فضـا، و در نهایـت دانـش پلـیس در آشنایی با جرائم در فضای مجازی از مهم‌ترین موضوع‌های طرح مسئله در این مقاله است.

با عنایت به گسترش روز افزون استفاده از فضای مجازی از یک‌سو و همچنین رشد جرائم رایانـه‌ای در این فضا، ضرورت این پژوهش از جهات زیر اجتناب‌ناپذیر است:

۱- بالا بردن اثربخشی آموزش‌های پلیسی در فضای مجازی و ایجاد امنیت و آسایش عمومی؛

۲- شناسایی تهدیدها در حوزه مجازی در فرماندهی انتظامی تهران بزرگ؛

۳- مشخص‌نمودن جایگاه آموزش کارکنان در پیشگیری از وقوع جرائم رایانه‌ای در حوزه فضای مجازی؛

۴- به‌وجودآوردن پلیس مقتدر در فضای مجازی با توجه به امر آموزش؛

۵- بالابردن ضریب امنیت عمومی در فضای مجازی از طریق توسعه آموزش‌های مرتبط؛

۱- فرماندهی انتظامی تهران بزرگ

۶- شناسایی افراد بزه‌کار و کلاه‌بردار در این فضا برای پیشگیری از وقوع جرم؛

بنابراین سؤال اصلی پژوهش عبارت است از: «آیا می‌توان با آموزش کارکنان از وقوع جرم در فضای مجازی پیشگیری نمود؟»

و سئوال‌های فرعی عبارت‌اند از:

آیا با افزایش دقت کارکنان در فاتب می‌توان از وقوع جرائم در فضای مجازی پیشگیری نمود؟

آیا با افزایش سرعت کارکنان در فاتب می‌توان از وقوع جرائم در فضای مجازی پیشگیری نمود؟

آیا با ایجاد کار تمام وقت در فاتب می‌توان از وقوع جرائم در فضای مجازی پیشگیری نمود؟

آیا با ایجاد همکاری از راه دور (دور کاری) می‌توان از وقوع جرائم در فضای مجازی پیشگیری نمود؟

همچنین فرضیه پژوهش به شرح زیر صورت‌بندی شده است:

به کارگیری نیروی انسانی آموزش‌دیده، متعهد و آگاه همراه با نرم افزارهای نوین و ارائه آموزش‌های به‌روز و مؤثر، به‌عنوان مهم‌ترین عوامل در پیشگیری از وقوع جرم در فضای مجازی در فاتب هستند.

مبانی نظری

اسلام و آموزش:

درسوره طه حضرت موسی(ع) در جواب سوال فرعون که پرسید خداوند شما کیست ؟ فرمود «خداوند،هم اوست که به هر چیزخلقت شایسته آن را داد و سپس هدایتش کرد (آیه۵۰)». درآیینی که زیادخواستن علم ازخداوند توصیه شده است؛ برای مبارزه با جهل و گسترش علم در نخستین پیروزی نظامی در جنگ بدر همین بس که پیامبراکرم (ص) فرمودند: هر اسیری که بتواند تعداد ۱۰ نفر از بیسوادان را باسواد کند و از نعمت دانش و علم برخوردار سازد، آزاد است (قورچیان،۱۳۷۸:۱۱۱).

اسلام، به‌خوبی می‌دانست که تمام آموزش‌ها از انسان سرچشمه می‌گیرد؛ یادگیری از مردم و جوامع – ضمن این‌که با دشواری همراه است – دانشی است که از بطن جامعه بیرون آمده و عمیق‌ترین ریشه‌ها را دارد. آدمی تنها آفریده‌ای است که نیاز به تعلیم و تربیت دارد و آدمی فقط به‌وسیله "آدمی" یعنی به دست مردم تربیت می‌شود و محتمل است که تعلیم و تربیت روز به روز بهتر می‌شود و هر انسان به سهم خود، گام تازه‌ای در راه بهبود انسان دیگر بر می‌دارد؛ زیرا رمز بزرگ بهبود طبیعت آدمی در تعلیم و تربیت وی نهفته است.

فضای مجازی:

فضای مجازی مجموعه‌ای از شبکه‌های ارتباطی رایانه‌ای؛ شامل تجهیزاتِ ارتباطی، انتقالی، کنترلی و سامانه‌های مدیریتی با اهداف ارزشمند برای پردازش‌ها و زیر ساخت‌ها است. اینترنت بزرگ‌ترین مؤلفه فضای مجازی است.

یکی از نگرانی‌های اساسی که در مورد اینترنت و فضای مجازی وجود دارد، امنیت و حفظ حریم شخصی افراد و حفظ اسناد محرمانه سازمانی است. اطلاعات گوناگونی اعم از اطلاعات شخصی و شغلی در پایگاه‌های داده شهری و پلیس نگهداری می‌شوند. نفوذ به این سامانه‌ها امکان سوء استفاده و ایجاد خطر برای شهروندان را فراهم می‌سازد؛ بنابراین حفظ امنیت و حریم شخصی افراد یکی از دغدغه‌های اساسی امروز پلیسِ جامعه‌محور است که باید راه کارهای مناسب برای حل آن انتخاب و اجرا شود. (دزیانی، ۱۳۸۸،۲۲)

بیشتر افرادی که به فضای مجازی وابسته‌اند و از آن استفاده می‌کنند، از آن به عنوان یک ضعف امنیتی یاد می‌کنند که می‌توان از آن در جهت انجام حملات استفاده نمود. بیشتر سامانه‌های فضای مجازی به‌گونه‌ای طراحی شده‌اند که بتوانند استفاده ارزان و وسیعی از دسترسی به شبکه داشته باشند و این موضوع، توانایی سوءاستفاده مهاجمان به منظور استثمار و آسیب‌پذیر نمودن شبکه‌ها و سرویس‌های هدف را افزایش داده است (سروری،۱۱۲:۱۳۸۸).

جرائم رایانه‌ای شامل هرگونه دخل و تصرف غیرمجاز از طریق ورود یا خروج، ضبط و ذخیره، پردازش و مدیریت داده‌ها و نرم‌افزارهای رایانه‌ای و ایجاد، یا واردکرن انواع ویروس‌های رایانه‌ای و امثال آن است. (دزیانی،۱۳۸۸، جلد اول)

منظور از اطلاعات، عبارت از داده‌هایی است که در بافتی معنادار و مفید جای می‌گیرد و دراختیار دریافت‌کننده قرارداده می‌شود تا ازآن‌ها برای تصمیم‌گیری استفاده کند. اطلاعات، متضمن انتقال و دریافت آگاهی و دانش است. اطلاعات، آگاهی و هوشیاری می‌دهد، شگفتی می‌آفریند، انگیزه ایجاد می‌کند و از عدم اطمینان می‌کاهد. (متواضع، ۱۳۸۴: ۸۴)

فناوری اطلاعات:

به کاربرد علم –به ویژه برای اهداف صنعتی و تجاری– یا به دانش و روش‌های مورد استفاده برای تولید یک محصول، فناوری گفته می‌شود. (اسدی،۱۴۷) و به گردآوری، سازماندهی، ذخیره و نشر اطلاعات اعم از صوت، تصویر، متن یا عدد که با استفاده از ابزار رایانه‌ای و مخابراتی صورت پذیرد، فناوری اطلاعات اطلاق می‌شود. (گلپایگانی، ۱۳:۱۳۸۲)

اینترنت بزرگ‌ترین شبکه رایانه ای موجود در جهان است که از میلیون‌ها رایانه شخصی، مسیریاب[1] و تجهیزات مخابراتی تشکیل شده است. سابقه ایجاد اینترنت به سال ۱۹۶۸ باز می‌گردد. در این سال ارتش آمریکا برای تبادل اطلاعات نظامی، شبکه‌ای را با نام آرپانت[2] بین مراکز نظامی ایجاد نمود که این پروژه با موفقیت انجام شد. به تدریج مراکز تحقیقاتی و دانشگاه‌ها به این شبکه متصل شدند و به تدریج، سازمان‌ها و افراد دیگر در سراسر دنیا، شبکه‌های محلی خود را به این شبکه بین‌المللی متصل کردند. (متواضع،۱۳۸۴:۳۸)

امنیت ملی و امنیت اطلاعات

مفهوم امنیت ملی در علوم انسانی دارای تعریف واحدی نیست؛ لذا برخی تعاریف مربوط به فضای مجازی درج می‌شود:

- ✓ حفظ یا ایجاد وضعیتی است که در آن منافع و ارزش‌های حیاتی کشور مورد تهدید جدی نباشد؛
- ✓ حفظ قدرت (نظامی، سیاسی، اقتصادی، فرهنگی) و اعمال حکومت در امور داخلی و خارجی علیه نفوذ بیگانگان و جلوگیری از عملیات غیرقانونی دشمن که به‌منظور تضعیف یا سرنگونی حکومت و دولت باشد؛
- ✓ توان یک ملت برای حفظ ارزش‌های داخلی از تهدیدهای خارجی؛
- ✓ اینکه یک کشور هیچ گونه احساس خطر حمله نظامی، فشار سیاسی یا اقتصادی نکند و بتواند آزادانه پیشرفت و توسعه خویش را تعقیب نماید؛
- ✓ حالتی است که ملتی فارغ از تهدید، از دست دادن تمام یا بخشی از جمعیت، دارایی یا خاک خود به سر برد (روشندل، ۱۳۷۴: ۱۱۱).

در سامانه‌های رایانه ای، «اطلاعات» مهم‌ترین و پرارزش‌ترین عنصر است؛ زیرا در صورت خرابی سخت افزارها با هزینه اندکی می‌توان آن‌ها را تعویض نمود ولی تهیه مجدد اطلاعات که معمولاً حاصل تلاش چند ساله شرکت‌ها است، غیر ممکن است و یا در صورت امکان بسیار پر هزینه و وقت گیراست. معمولاً افراد، سازمان‌ها و مؤسسات بزرگ، حجم زیادی از اطلاعات را در شبکه‌های رایانه ای خود نگهداری می‌کنند که حفظ این اطلاعات و عدم دسترسی افراد غیر مجاز به آن، برای صاحبان این‌گونه افراد و مؤسسات امری حیاتی به شمار می‌آید؛ زیرا ممکن است دستاوردها و اطلاعات مهم مالی و تجاری و خانوادگی، مورد سوء استفاده قرار گیرد. در نتیجه، همه سازمان‌ها و مؤسسات و حتی شهروندان باید با فضای مجازی و جنگ مجازی آشنا شده و دستورالعمل‌هایی برای تشخیص مشکلات امنیتی و نحوه

1. Router
2. ARPANET

گزارش آن‌ها وجود داشته باشد تا در حملات مجازی به افراد و مؤسسات، ضمن آشنایی با وظایف خود، بدانند که در صورت وجود هر مشکل با چه کسی باید تماس بگیرند. (روشندل،۱۳۷۴: ۷۴)

امنیت، مبحثی کاملاً پیچیده ولی با اصولی ساده است. در بسیاری از مواقع، همین سادگیِ اصول هستند که ما را دچار گمراهی می‌کنند و دورنمای فعالیت‌های ما را از لحاظ سهولت و اطمینان در سایه‌ای از ابهام فرو می‌برند. صادقانه باید گفت که امنیت، یک پردازش چند لایه است. تعیین نوع و نحوه تلفیق لایه‌های دفاعی مورد نیاز، فقط پس از تکمیل ارزیابی قابل ارائه است. تهیه فهرستی از سیاست‌های اجرایی بر مبنای اینکه چه چیزی برای سازمان مهم‌تر و انجام آن ساده‌تر است، در اولویت قرار دارد. پس از آنکه این اولویت‌ها به تأیید رسیدند، هر یک از آن‌ها باید به سرعت در جای خود به اجراگذارده شود. ارزیابی امنیتی، یک بخش بسیار مهم‌تر از برنامه‌ریزی امنیتی است. بدون ارزیابی از مخاطرات، هیچ طرحِ اجرایی در جای خود به درستی قرار نمی‌گیرد. ارزیابی امنیتی، خطوط اصلی را برای پیاده‌سازی طرح امنیتی که به منظور حفاظت از دارایی‌ها در مقابل تهدیدها است، مشخص می‌کند. (شفیعی، ۱۳۸۵، ۴۵)

امنیت اطلاعات به «حفاظت از اطلاعات» و به «حداقل رساندن خطر افشای اطلاعات» در بخش‌های غیرمجاز اشاره دارد. امنیت اطلاعات مجموعه‌ای از ابزارها برای جلوگیری از سرقت، حمله، جنایت، جاسوسی، خرابکاری و علم مطالعه روش‌های حفاظت از داده‌ها در رایانه‌ها و نظام‌های ارتباطی در برابر دسترسی و تغییرات غیرمجاز را شامل می‌شود. به منظور جلوگیری از سوءاستفاده و یا مخدوش‌سازی اطلاعات که از لحاظ امنیتی دارای اهمیت زیادی می‌باشد، لازم است سامانه‌های موجود با استفاده از فناوریِ امنیت اطلاعات به صورت «امن» در اختیار کاربران مجاز قرار داده شود. (همان) به طور کلی مفاهیم سرویس‌های امنیتی عبارت‌اند از: (همان:۱۲۰)

الف) محرمانه ماندن اطلاعات: دلایل متعددی برای یک سازمان یا حتی فرد عادی وجود دارد که بخواهد اطلاعات خود را محرمانه نگه دارد.

ب) احراز هویت: قبل از آنکه محتوای یک پیام یا اطلاعات اهمیت داشته باشد، باید مطمئن شد که پیام از شخصی که تصور می‌شود، رسیده است و کسی قصد فریب و گمراه کردن دیگران را ندارد.

ج) سلامت داده‌ها: یعنی دست نخوردگی و عدم تغییر پیام و اطلاعات و اینکه داده‌ها با اطلاعات مخرب مثل یک ویروس رایانه‌ای آلوده نشده‌اند. (همان:۱۲۱)

د) کنترل دسترسی: یعنی بتوان دسترسی افراد غیر مجاز به شبکه را با دقت کنترل کرد و توانایی منع افراد غیرقابل اعتماد از دسترسی به شبکه، وجود داشته باشد. (انستیتو ایز ایران، ۱۳۸۷:۱۲۳)

ه) در دسترس بودن: باید تمام امکانات شبکه، بدون دردسر و زحمت در اختیار آن‌هایی که مجاز به استفاده از شبکه هستند، باشد و در ضمن، هیچ کس نتواند در دسترسی به شبکه اختلال ایجاد کند. زمانی که یکی از سرویس‌های امنیتی پنج‌گانه فوق نقض شود، بدین معناست که به سامانه حمله شده است. (همان:۱۲۴)

فناوری اطلاعات با برخورداری از ویژگی‌ها و قابلیت‌های مختلف توانسته است انعطاف‌پذیری شایان توجهی را در زمینه کارآفرینی از خود نشان دهد. همین ویژگی‌ها سبب افزایش کارایی این فناوری در امر کارآفرینی و ایجاد اشتغال شده است. در یک نگاه کلی می‌توان به برخی از این ویژگی‌ها اشاره نمود (احمدی، ۱۳۸۴، ۳۰)

- *افزایش سرعت:* محاسبه و پردازش سریع اطلاعات و انتقال فوری آن، زمان انجام کار را کاهش و در نتیجه بهره‌وری را افزایش می‌دهد. فناوری اطلاعات امکان جستجو و دستیابی سریع به اطلاعات را نیز فراهم می‌کند.
- *افزایش دقت:* در مشاغل مبتنی بر انسان، دقت انجام کار متغیر است؛ در حالی که فناوری اطلاعات دقتی بالا و ثابت را تأمین و تضمین می‌کند. در انواع فعالیت‌های پردازشی و محاسباتی دقت رایانه به مراتب بیشتر از انسان است.
- *کاهش‌دهنده فیزیکی مخازن اطلاعات:* با توسعه فناوری اطلاعات و به کارگیری آن، دیگر لزومی به حمل و نگهداری حجم زیادی از کتاب‌های مرجع تخصصی وجود ندارد. به راحتی می‌توان در هر لوح فشرده، اطلاعات چندین کتاب را ذخیره نموده و یا آنکه منابع مورد نیاز را از طریق شبکه‌های رایانه‌ای دریافت نمود.
- *رفع برخی از فسادهای اداری:* استفاده از فناوری اطلاعات، شفافیت در انجام کارها را افزایش می‌دهد و بسیاری از واسطه‌ها را حذف می‌کند. این دو مزیت کلیدی منجر به رفع برخی از فسادهای اداری به خصوص در سطوح پایین می‌شوند.
- *ایجاد امکان کار تمام وقت:* به کمک فناوری اطلاعات، بسیاری از استعلام‌ها و مراجعات افراد و غیره از طریق شبکه‌های رایانه ای و به صورت خودکار انجام می‌گیرد؛ بنابراین می‌توان به صورت بیست و چهار ساعته از آن بهره گرفت.
- *ایجاد امکان همکاری از راه دور:* مخابرات، تلفن، تله کنفرانس، ویدئو کنفرانس و همچنین سامانه‌های همکاری، تبادل الکترونیکی داده‌ها و غیره، نمونه‌هایی از کاربردهای فناوری اطلاعات در این زمینه هستند.

– *کاهش هزینه‌های سامانه یا سازمان:* با توجه به موارد فوق به ویژه افزایش سرعت که باعث انجام تعداد کار بیشتر می‌شود و انجام کار تمام وقت، بهره‌وری سامانه افزایش می‌یابد و در نتیجه باعث کاهش مقدار زیادی از هزینه‌ها می‌گرد. (احمدی،۱۳۸۴:۳۱)

پیشگیری از جرم

پیشگیری در یک معنای عام، عبارت است از تمامی اقداماتی که از وقوع بزه، جلوگیری می‌کند. به عقیده شرمن، هر رویدادی که اعمال شود و نتیجه آن نشان دهد که از نرخ بزهکاری کاسته شده، می‌تواند پیشگیرانه قلمداد شود (نجفی ابرندآبادی، ۱۳۸۷: ۱۲۲۸). بر مبنای این تعریفِ شرمن، عده‌ای پیشگیری را اعم از پیشگیری کیفری (پیشگیری از جرم از طریق اعمال مجازات‌ها) و پیشگیری غیرکیفری دانسته‌اند.

عده‌ای دیگر از جرم‌شناسان نظیر «گسن» با نقد سرکوبی و غیر پیشگیرانه دانستن آن، پیشگیری را به معنایی خاص تعریف می‌کنند: مجموعه اقدامات غیرکیفری که هدف غایی آن منحصراً یا به صورت جزئی محدود کردن دامنه ارتکاب جرم و غیرممکن، دشوار و کم‌کردن احتمال وقوع جرم باشد. در همین راستا، یک محقق کانادایی در سال ۱۹۹۸ تعریف پیشگیری را دارای سه مؤلفه زیر دانست:

هدف اصلی آن، تأثیرگذاری بر یکی از عوامل فرایند کیفری است؛

بعد جمعی دارد (پیشگیری در یک محله خاص یا ...)؛

شامل اقدام پیشگیرانه غیر قهرآمیز و غیرکیفری است (همان، ۱۲۲۹).

به این ترتیب می‌توانیم تعریف آقای کوسن را در سال ۲۰۰۲ مبنا قرار دهیم:

پیشگیری، مجموعه اقدام‌ها و تدابیر غیر قهرآمیز است که با هدف خاص مهار بزهکاری، کاهش احتمال و وخامت جرم، پیرامون علل جرائم اتخاذ می‌شود. در این تعریف اقدام پیشگیرانه، اقدام غیرقهرآمیزی است که بر عوامل جرم‌زا اعمال می‌شود. در واقع پیشگیری مستلزم آن است که ابتدا علت‌شناسی اولیه از جرم صورت بگیرد (همان).

ماده (۱) لایحه پیشگیری از جرم نیز تعریف نسبتاً جامعی از پیشگیری ارائه کرده است: «پیش‌بینی، شناسایی و ارزیابی خطر وقوع جرم و اتخاذ تدابیر و اقدامات لازم برای از بین بردن یا کاهش آن، پیشگیری از جرم است».

در مورد انواع پیشگیری، تقسیم‌بندی‌های متفاوتی از منظرهای مختلف صورت گرفته است. این تقسیم‌بندی‌ها فراتر از تقسیم‌بندی‌های صرف نظری هستند و به جنبه‌های متنوعِ مداخلات پیشگیرانه اشاره دارند. (نوروزی، بارانی و سرکشیکیان، ۱۳۹۰: ۳۰)

پیش‌بینی، مطابق معیار «زمان مداخله»، دو گونه ی کنشی (قبل از ارتکاب جرم) و واکنشی (پس از ارتکاب جرم)؛ بر اساس معیار «سطح مداخله» سه دسته نخستین (برای همه افراد)، دومین (برای افراد آسیب‌پذیر) و سومین (برای افرادی که مرتکب جرم شده‌اند)؛ مطابق معیار «قلمرو مداخله» دو دسته عمومی (با تمرکز به عوامل عمومی جرم) و اختصاصی (با تمرکز بر علل اختصاصی جرم)؛ بر اساس معیار «سازمان مداخله‌کننده» سه گونه اجتماعی (نهادهای دولتی و غیردولتی فعال در مسائل اجتماعی)، انتظامی (نهاد پلیس) و قضایی (مراجع رسیدگی‌کننده به جرم) و مطابق «نوع مداخله» دو دسته کیفری (از طریق سازوکارهای نظام عدالت کیفری) و غیرکیفری (از طریق سازوکارهای خارج از نظام عدالت کیفری) دسته‌بندی می‌شود (عباچی، ۱۳۸۸).

به طورکلی، برنامه‌های پیشگیرانه در سه سطح، قابلیت اجرا دارند. «برانتینگام» و «فست» (۱۹۷۶) از جرم‌شناسانی بودند که با الگوگرفتن از مدل های بهداشت عمومی، به سنخ‌شناسی پیشگیری از جرم در سه سطح زیر پرداختند (Crawford :2007 :870)

پیشگیری نخستین[1]؛ شامل آگاه‌ساختن محیط‌ها و اجتماعات عمومی نسبت به خطرات احتمالی بروز جرم است؛ پیش از آن‌که جرمی به‌وجود آمده باشد.

پیشگیری دومین[2]؛ شامل انجام اقداماتی برای افراد یا محیط‌هایی است که به‌دلیل دارا بودن برخی تمایلات و ویژگی‌ها، در معرض خطر بزهکاری، تشخیص داده شده‌اند.

پیشگیری سومین[3]؛ ناظر به «باز رخداد» جرم است و با کانونِ توجه قراردادنِ مجرمان، بزه‌دیدگان و یا محل‌های ارتکاب جرم، از تکرار بزه جلوگیری می‌کند.

انواع روش‌های پیشگیری از جرم

پیشگیری کیفری: پیشگیری کیفری –که بر مبنای ارائه تعریفی عام از پیشگیری می‌تواند یکی از انواع پیشگیری به‌حساب آید، از طریق وضع کیفر و ویژگی‌های ارعابی و بازدارنده آن می‌کوشد تا از یک‌سو، نسبت به مجرم امکان تکرار جرم را از بین ببرد و از سوی دیگر با تأکید بر ویژگی‌های ارعابی کیفر، انگیزه مجرمان احتمالی را برای ارتکاب جرم کاهش دهد. بازدارندگی[4] یکی از مفاهیم اساسی در پیشگیری کیفری است؛ به این معنی که مجازات‌ها باید به‌گونه‌ای وضع شوند که مانع ارتکاب مجدد جرم شوند. گذشته از

1. Primary Prevention
2. Secondary Prevention
3. Tertiary prevention
4. Deterrence

مفاهیم کلیدی مجازات و بازدارندگی، فوریت و دقت شناسایی، تعقیب و دستگیری نیز از اهمیت بسیاری در پیشگیری کیفری برخوردار است. در واقع ـ به‌مانند پیشگیری موقعیت‌مدار ـ اینجا نیز فرض اصلی، حساب‌گر بودن مجرم است. تعقیب و مجازات باید به‌گونه‌ای باشد که مجرم حساب‌گر را به این نتیجه برساند که منافع حاصل از ارتکاب جرم، به‌دلیلِ شدت، دقت و سرعت واکنش کیفری، از خطرپذیری بسیار بالایی برخوردار است. سنگینی کفه خطرپذیری، می‌تواند عاملی باشد برای چشم‌پوشی مجرم از منافع احتمالی کفه دیگرِ ترازو (نوروزی، بارانی و سرکشیکیان، ۱۳۹۰: ۳۲).

پیشگیری موقعیت‌مدار[1]**:** برنامه‌ها و اقدامات پیشگیرانه را (از منظر پیشگیری به‌معنای خاص) به‌طورکلی می‌توان به دو بخش پیشگیری موقعیت‌مدار (وضعی) و پیشگیری اجتماعی تقسیم کرد. هر دو قسم پیشگیری می‌توانند در هر سه سطح پیش‌گفته (نخستین، دومین و سومین) استقرار یابد.

«پیشگیری وضعی (موقعیت‌مدار)، به‌معنای ایجاد تغییرات در اوضاع و احوال خاصی است که انسان متعارف در آن ممکن است مرتکب جرم شود» (نجفی ابرندآبادی، ۱۳۸۷: ۱۲۴۲). منظور از انسان متعارف در تعریف فوق، آن است که انسان به‌طور معمول موجودی حساب‌گر است؛ این موجود حساب‌گر زمانی که در موقعیت مناسبِ ارتکاب جرم قرار می‌گیرد، دست به حساب‌گری زده و سود و زیان حاصل از ارتکاب جرم را در ذهن خود ارزیابی می‌کند؛ بنابراین هرگونه تغییرات ایجاد شده در موقعیت جرم‌زا که بتواند محاسبات این موجود حساب‌گر را به‌سمت عدم ارتکاب جرم پیش ببرد، پیشگیری وضعی به‌حساب می‌آید (نوروزی، بارانی و سرکشیکیان، ۱۳۹۰: ۳۳).

پیشگیری موقعیت‌مدار با تسلط بر محیط و شرایط پیرامون جرم (وضعیت مشرف بر جرم) درصدد آن است تا از طریق کاهش جذابیت آماج و جاذبه‌زدایی از آن، و نیز افزودن خطر شناسایی و احتمال دستگیری بزهکار (و به‌طور کلی نامناسب جلوه دادن وضعیت پیش‌جنایی)، آمار جرائم را مهار کند (نجفی ابرندآبادی، ۱۳۸۰، ۱۴۰).

کاهش موقعیت از منظر پیشگیری موقعیت مدار می‌تواند به یکی از سه شکل زیر باشد (Crawford, 2007, 873):

۱- گسترش و افزایش اقدامات لازم برای ارتکاب جرم با دشوار ساختن آماج جرم؛ به‌گونه‌ای که مجرمین برای ارتکاب جرم مجبور باشند هزینه و دشواری بیشتری متحمل شوند؛

۲- افزایش خطر قابل درک برای مجرم در مورد احتمال زیاد دستگیری و مجازات؛

۳- کاهش منافع قابل پیش‌بینی جرم.

1. Situational Prevention

پیشگیری اجتماعی[1]: پیشگیری اجتماعی برخلاف پیشگیری وضعی که بر موقعیت جرم‌زا تمرکز دارد، به مجرم احتمالی و محیط پیرامونی او می‌پردازد. پیشگیری اجتماعی خود به دو بخشِ رشد مدار و جمعی تقسیم می‌شود. در پیشگیری اجتماعی، تقویت سازوکارهای خودکنترلی (یا موانع اخلاقی) از یک‌سو، و آموختن مهارت‌های اجتماعی برای تعامل با دیگران از سوی دیگر، به نوجوانان آموزش داده می‌شود (نجفی ابرندآبادی، ۱۳۸۷، ۱۲۳۸).

این نوع پیشگیری با هدف قراردادن اصلاح فرد و جامعه، منجر به جلوگیری از جرم به‌صورت پایدار و همیشگی می‌شود. این نوع از پیشگیری، برخلاف پیشگیری وضعی (که بزه‌دیده‌مدار و سیبل‌مدار است)، مجرم‌مدار و فردمدار است (همان، ۱۲۶۱).

فرد در ارتباط با محیط‌های پیرامونی خود ـ متشکل از خانواده، مدرسه، گروه‌های همسالان، ساختارهای محلی و... ـ فرآیند جامعه‌پذیری را طی می‌کند. در صورتی‌که هر یک از این محیط‌ها، کارکرد خود را به‌درستی انجام ندهد و یا نقش سازنده آن، به نقشی مخرب و منحرفانه تبدیل شود، مداخله ی پیشگیرانه اجتماعی می‌تواند نقش‌آفرینی کرده و سازوکارهای مخرب را ترمیم سازد. بدین‌ترتیب، انحراف زودهنگام و قابل ترمیم دوران کودکی به جرمِ استقرار یافته و –در بعضی مواقع– درونی‌شده دوران بزرگسالی تبدیل نمی‌شود (نوروزی، بارانی و سرکشیکیان، ۱۳۹۰: ۳۴).

پیشگیری رشدمدار[2]: برنامه‌های رشدمدار درصدد شناسایی عوامل خطر۳ بزهکاری هستند تا با شناسایی آن‌ها مانع شوند تا این عوامل در کودکان و نوجوانان رشد کنند و آنان را مرتکب انحراف و سپس جرم نمایند. پیشگیری رشدمدار بیش از آنکه در پی ارائه آموزش‌های کلی و عمومی در مورد پیشگیری از جرم به مردم باشد، بر گروه‌هایی از جوانان که عوامل خطر بزهکاری در آن‌ها شناسایی شده و در معرض خطر ارتکاب جرم هستند، تمرکز دارد (پیشگیری دومین به‌جای پیشگیری نخستین). پیشگیری رشدمدار درصدد شناسایی موارد زیر است:

۱– عوامل خطری که می‌تواند نشانه روی‌آوردن به بزهکاری در آینده باشد؛

۲– عوامل حمایتی که می‌تواند احتمال ارتکاب جرم را کاهش دهد؛

۳– عوامل قطع‌کننده که می‌تواند نوجوانان یا جوانان را از استمرار فعالیت منحرفانه و یا مجرمانه منصرف سازد (ترک تکرار جرم) (Crawford, 2007, 883).

1. Social Prevention
2. Developmental Prevention
3. Risk Factors

در نظام‌های توسعه‌یافته، مهار جرم در یک فرایند زمانی دراز مدتِ مطالعاتی تحت عنوان دوره‌های جنایی[1] بر روی نوجوانان منحرف یا جوانان بزهکار صورت می‌گیرد که در آن‌ها شیوه زندگی این افراد، طی سال‌های پس از ارتکاب بزه یا انحراف مورد مطالعه قرار می‌گیرد. به این ترتیب، پس از گذشت ۱۵ یا ۲۰ سال و زمانی که این افراد به سنین میان سالی می‌رسند، مشخص می‌شود که:

- آیا انحراف دوران جوانی، آن‌ها را به ارتکاب جرم در میان سالی کشانیده یا خیر؟
- چند درصد این افراد از ارتکاب جرم دست کشیده‌اند؟
- چند درصد به‌طور اتفاقی و چند درصد به‌طور حرفه‌ای به ارتکاب جرم پرداخته‌اند؟

پاسخ به این سؤالات با شناسایی دو دسته از عوامل همراه است: عوامل خطر (چه عواملی منجر به تکرار جرم و استمرار رویه مجرمانه شد) و عوامل حمایتی (چه عواملی منجر به قطع ارتکاب جرم شد).

به‌عنوان مثال، مطالعه دوره‌های جنایی نشان خواهد داد که عواملی نظیر ازدواج، اشتغال، استفاده یا عدم استفاده از مواد مخدر و یا مواد الکلی و ... چه تأثیری بر استمرار یا قطع[2] جرم داشته است؟

شناسایی عوامل خطر و حمایتی در دوره‌های جنایی، امکان مداخله زودهنگام نسبت به کودکان و نوجوانانِ منحرف –یا در معرض خطر انحراف– را فراهم می‌کند تا برای جلوگیری از ارتکاب جرم آنان، از الگوهای پیشگیری اجتماعی استفاده شود. (نوروزی، بارانی و سرکشیکیان، ۱۳۹۰: ۳۵).

پیشگیری جامعه‌مدار[3]: مرز میان این نوع، با پیشگیری رشدمدار کاملاً محسوس و مشخص نیست. از نظر برخی (نجفی ابرندآبادی، ۱۳۸۷: ۱۲۳۶)، پیشگیری رشدمدار همان پیشگیری جامعه‌مدار است که ناظر به قشر خاصی (اطفال) است. این در حالی است که پیشگیری اجتماعی تمام افراد را مدنظر قرار می‌دهد.

پیشگیری انتظامی از جرم[4]: پلیس یکی از اجزای نظام عدالت کیفری است که در پیشگیری از جرم، امکان مداخله کیفری و غیرکیفری را دارد. در مداخله کیفری، پلیس با سرعت و دقت در فرایند تعقیب و دستگیری ـ که خود یکی از عوامل بازدارنده نسبت به ارتکاب مجدد بزه است ـ فعالیت پیشگیرانه خود را انجام می‌دهد. جنبه بازدارنده و ارعابی مداخله کیفری پلیس از سویی بزهکاران را بلافاصله پس از ارتکاب جرم با نظام نیرومند تعقیب و دستگیری مواجه می‌سازد – که بنابراین یکی از ابعاد بازدارندگی برای تکرار جرم را فراهم می‌کند – و از سوی دیگر، با بالابردن احتمال دستگیری و افزایش خطرپذیری ارتکاب جرم، قصد و تمایل مجرمان احتمالی را برای ارتکاب آن بزه، کاهش می‌دهد. (نوروزی، بارانی و سرکشیکیان، ۱۳۹۰: ۳۸).

1. Criminal Careers
2. Desistence
3. Community Prevention
4. Police Crime Prevention

در پیشگیری غیرکیفری نیز پلیس از طریق مداخله و طراحی برنامه‌های پیشگیرانه از طریق نظارت بر مجرمان سابقه‌دار، گشت‌های خیابانی، نظارت بر مناطق جرم‌زا، نصب دوربین‌های مداربسته در معابر عمومی و جرم‌خیز و بسیاری دیگر از برنامه‌های پیشگیرانه، پیش از ارتکاب جرم، آن را به واپایش خود در می‌آورد (همان).

به‌طورکلی، نقطه تمرکز مداخله‌های پیشگیرانه را می‌توان یکی از سه منظر موقعیت جرم‌زا، بزه‌دیده و بزهکار قرار داد. هریک از این سه مورد می‌تواند نقطه اجرای برنامه‌های پیشگیرانه در یکی از سه سطح زیر باشد: پیشگیری مرحله اول (پیشگیری عمومی و آگاهی بخشی جامعه نسبت به جرم)، پیشگیری مرحله دوم (تمرکز بر افراد در معرض بزه)، پیشگیری مرحله سوم (پیشگیری از تکرار بزه). (فرجی‌ها، ۱۳۸۹)

تجربه کشورهای توسعه‌یافته نشان می‌دهد که پلیس امکان مداخله در تمام سطوح فوق را دارد؛ اما متناسب با سطح و نقطه تمرکز انتخابی حضور پلیس نسبت به سایر نهادهای مدنی یا رسمی، کمرنگ یا پررنگ‌تر می‌شود. به‌عنوان مثال در پیشگیری مرحله اول، نقش «آموزش» پررنگ‌تر است و پلیس به‌عنوان یک بازوی اجرایی، در کنار نهادهای آموزشی، نقشی مکمل ایفا می‌کند؛ حال آن‌که در برنامه‌های پیشگیری مرحله سوم (نظارت بر مجرمان سابقه‌دار)، پلیس عهده‌دار نقش اصلی است و سایر نهادها، نقش مکمل دارند. به‌طورکلی می‌توان ادعا کرد که هرچه از مرحله اول به‌سمت مرحله سوم می‌رویم، نقش پلیس و برنامه‌های پیشگیرانه پلیسی، به‌تدریج پررنگ‌تر می‌شود (نوروزی، بارانی و سرکشیکیان، ۱۳۹۰: ۳۹).

راهبردهای اصلی پیشگیری از جرائم فضای مجازی

۱- نهادینه سازی فرامین و تدابیر فرمانده ناجا در راستای پیشگیری از وقوع جرائم در فضای مجازی؛

۲- ساماندهی، انسجام بخشی و هدایت راهبردی مجموعه‌های علمی، پژوهشی آموزشی و صنعتی مرتبط با حوزه تخصصی فاتب در راستای تولید و توسعه دانش و فناوری‌های بومی و ملی مورد نیاز فاتب در راستای کاهش و پیشگیری از وقوع جرائم در فضای مجازی.

۳- توسعه امنیت، ایمنی و پایداری در شبکه‌های ارتباطی و الکترونیکی موجود با تأکید بر فناوری‌های بومی.

۴- نهادینه کردن اصول و ملاحظات پیشگیری از وقوع جرم در طرح‌های توسعه شبکه‌های ارتباطی و الکترونیکی فاتب.

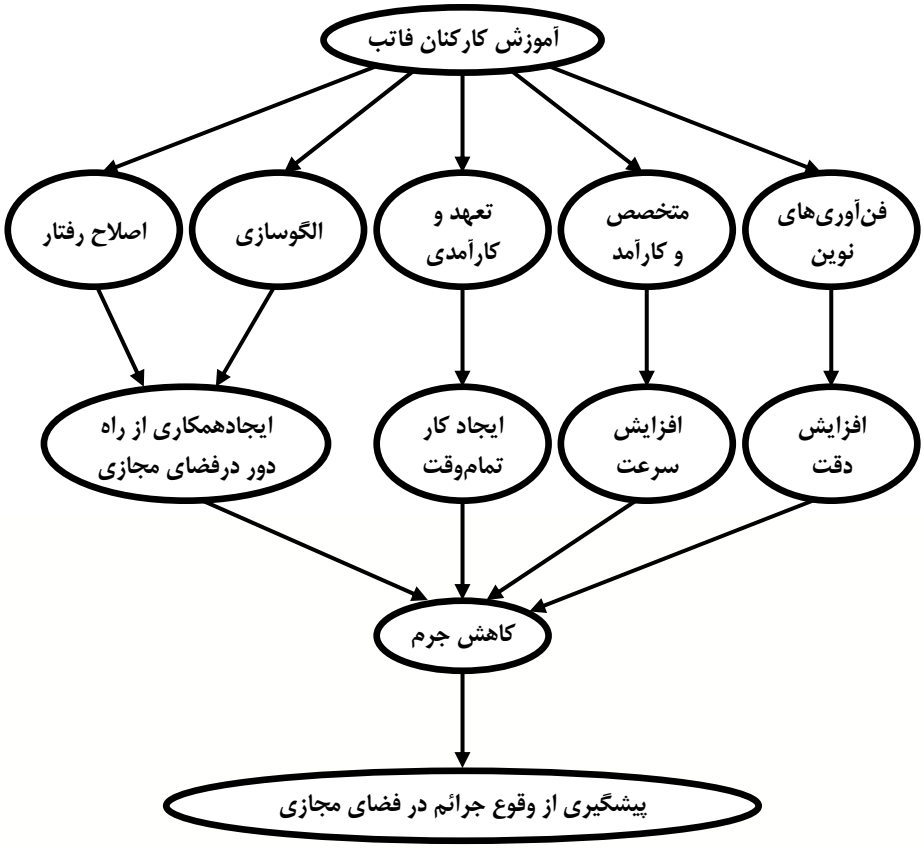
۵- توسعه فرهنگ و ارتقای دانش و شناخت مسئولین و کارشناسان حوزه ارتباطات و الکترونیک از مقوله پیشگیری از جرم

۶- خود اتکایی از دستگاه‌های پشتیبان و آسیب پذیری و خودکفایی از منابع خارجی فناوری‌ها.

۷- حمایت از برنامه ایجاد شبکه ملی اینترنت مبتنی بر مؤلفه‌های امنیت، ایمنی، پایداری و متکی بر فناوری‌های بومی.

۸- توسعه توان مهار و مدیریت بحران و برنامه‌های حراست، حفاظت اطلاعات و ضد جاسوسی.

مدل مفهومی تحقیق:



شکل ۱- مدل مفهمومی

یافته‌های تحقیق:

این تحقیق، از منظر روش توصیفی و از نوع کاربردی است. با استفاده از آمار توصیفی و استنباطی، داده‌ها تجزیه و فرضیه‌های پژوهش مورد بررسی و تحلیل قرار گرفته است. جامعهٔ آماری این تحقیق، رؤسا و فرماندهان فاتب، مدیران رده‌های میانی فاتب، کارشناسان فنی و کارکنان مرتبط بالغ بر ۲۰۰ نفر هستند. حجم جامعه نمونه ۴۴ نفر است.

همچنین اطلاعات به‌صورت کتابخانه‌ای و با استفاده از پرسشنامه جمع‌آوری شده است. با توجه به اینکه جامعه انتخابی دارای طبقه‌های مشخص، تعریف‌پذیر و داده‌های داخل طبقه تا جایی که امکان دارد همگون هستند و همه کارکنان و فرماندهان در فرماندهی انتظامی تهران بزرگ را در بر می‌گیرد، از روش تصادفی طبقه‌ای استفاده شده است.

$$n = \frac{N(Z_a/2)^2 \times \sigma^2}{D^2(N-1) + (Z_a/2)^2 \times \sigma^2} = \frac{200(1.96)^2 \times 3.7}{0.25(200-1) + (1.96)^2 3.7} = \frac{2842.784}{64.61} = 44$$

جدول ۱- جامعه آماری مورد مطالعه

عنوان	رؤسا و فرماندهان فاتب	مدیران رده‌های میانی فاتب	کارشناسان	کارکنان مرتبط	جمع
تعداد	۱۰	۳۰	۵۰	۱۱۰	N=۲۰۰

جدول ۲- جامعه آماری و تعداد نمونه

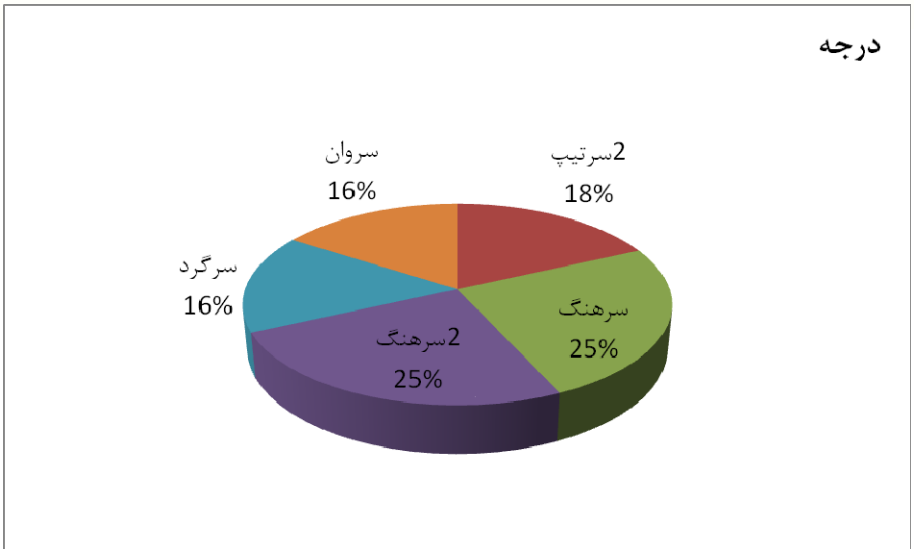
	رؤسا و فرماندهان فاتب	مدیران رده‌های میانی فاتب	کارشناسان	کارکنان مرتبط	جمع
جامعه آماری	۱۰	۳۰	۵۰	۱۱۰	N=۲۰۰
تعداد نمونه	۲	۷	۱۱	۲۴	n=44

میزان سابقه خدمتی جامعه آماری به شرح زیر است:

سابقه خدمتی	۱۰-۱۵ سال	۱۵ تا ۲۰ سال	۲۰ تا ۳۰ سال	بالای ۳۰ سال	جمع
فراوانی	۷	۶	۳۰	۱	۴۴
درصد	۱۶	۱۴	۶۸	۲	۱۰۰

درجات جامعه آماری به شرح زیر است:

درجه	سرتیپ دومی	سرهنگی	سرهنگ دومی	سرگردی	سروانی	جمع
فراوانی	۸	۱۱	۱۱	۷	۷	۴۴
درصد	۱۸	۲۵	۲۵	۱۶	۱۶	۱۰۰



شرح جدول و نمودار:

۱۸٪ از جامعه آماری دارای درجه سرتیپ دومی، ۲۵٪ دارای درجه سرهنگی، ۲۵٪ دارای درجه سرهنگ دومی، ۱۶٪ دارای درجه سرگردی و ۱۶٪ دارای درجه سروانی هستند.

آزمون استنباطی داده‌ها:

مرحله اول – تبدیل فرضیه پژوهشی به فرضیه آماری:

H_1=ادعا

به کارگیری نیروی انسانی متخصص، متعهد، علاقمند، آگاه و دانا و نیز استفاده از نرم افزارهای نوین با مدیریت کارآفرینی برای افزایش کارایی فرماندهی انتظامی تهران بزرگ در محیط مجازی برای پیشگیری از وقوع جرم مناسب است.

نقیض ادعا =H_0

به کارگیری نیروی انسانی آموزش دیده و متخصص، متعهد، علاقمند، آگاه و دانا و نیز استفاده نرم افزارهای نوین و ارائه آموزش‌های به روز و مؤثر به عنوان مهم‌ترین عوامل در پیشگیری از وقوع جرم در محیط مجازی در فاتب مناسب نیست.

مرحله دوم – تعیین آماره آزمون فرضیه:

طیف	خیلی زیاد	نسبتاً زیاد	زیاد	کم	خیلی کم	جمع
فراوانی	۳۴۳	۲۳۱	۴۴	۵۳	۳۳	۷۰۴
درصد	۴۸.۷۲	۳۲.۸۱	۶.۲۵	۷.۵۳	۴.۶۹	۱۰۰
$\overline{P}$	۸۱.۵۳					

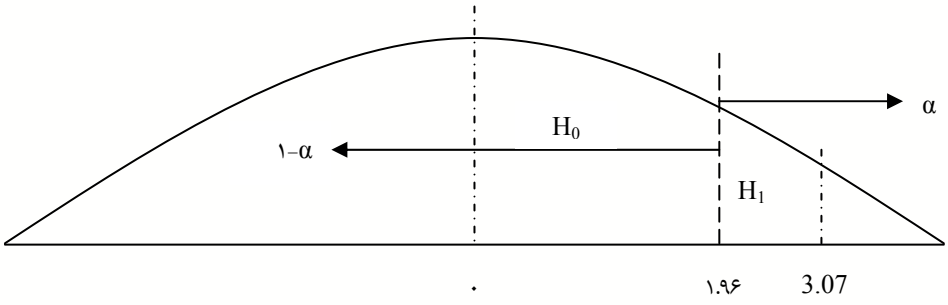
$$Z = \frac{\overline{P} - P_0}{\sqrt{P_0 \frac{1-P_0}{n}}} = \frac{\%81.53 - \%60}{\sqrt{\%60 \frac{1-\%60}{44}}} = \frac{\%21.53}{\sqrt{.005}} = \frac{0.2153}{.07} = +3.07$$

$$P_0 = \%60 \text{ و } \overline{P} = \%81.53$$

مرحله سوم– تعیین سطح زیر منحنی و نقطه بحرانی:

$\alpha = ٪۲$ ۱ – α=٪۹۸

$Z_{\alpha} = ۲.۰۵$ $Z_{\text{آزمون}}$=3.07



مرحله چهارم– تحلیل:

چون مقدار آمار آزمون (3.07) از Z_{α} (مقدار بحرانی ۲.۰۵) بزرگ‌تر است و در ناحیه H_1 قرار گرفته، فرضیه H1 پذیرفته می‌شود و فرضیه مقابل آن یعنی H0 رد می‌گردد؛ به‌عبارتی دیگر با اطمینان ۹۸٪ می‌توان گفت به کارگیری نیروی انسانی آموزش دیده و متخصص، متعهد، علاقمند، آگاه و دانا با مدیریت کارآفرینی برای پیشگیری از وقوع جرم در فضای مجازی مناسب است.

نتایج حاصل از تجزیه و تحلیل اطلاعات:

طیف	خیلی زیاد	نسبتاً زیاد	زیاد	کم	خیلی کم	جمع
فراوانی	۳۴۳	۲۳۱	۴۴	۵۳	۳۳	۷۰۴
درصد	۴۸.۷۲	۳۲.۸۱	۶.۲۵	۷.۵۳	۴.۶۹	۱۰۰

۴۸.۷۲٪ از جامعه نمونه معتقدند به کارگیری نیروی انسانی متخصص در کارایی فرماندهی انتظامی تهران بزرگ در محیط مجازی برای پیشگیری از وقوع جرم به نسبت خیلی زیاد، ۳۲.۸۱٪ نسبتاً زیاد، ۶.۲۵٪ نسبتاً زیاد، ۷.۵۳٪ کم و ۴.۶۹۱٪ دیگر به نسبت خیلی کم مناسب است.

نتیجه‌گیری

از مجموع ادبیات نظری پژوهش و تجزیه و تحلیل اطلاعات می‌توان نتیجه گرفت که مهم‌ترین رسالت و مزیت شبکه‌های رایانه‌ای، اشتراک منابع سخت‌افزاری و نرم‌افزاری و دستیابی سریع و آسان به اطلاعات به‌صورت هدفمند است که این خود زمینه ای برای ایجاد جرائم رایانه‌ای است؛ بنابراین ارتقای آموزش‌های فضای مجازی برای استفاده از فناوری اطلاعات منجر به تصمیم‌گیری مطمئن و امن برای فرماندهان می‌شود؛ همچنین با توجه به دسترسی سارقان اطلاعاتی به بانک‌های اطلاعاتی ناامن، گشت‌های امنیتی می‌توانند سارقان اطلاعاتی را شناسایی و از جرائم آنان پیشگیری کنند.

جمع‌آوری داده‌ها، پردازش داده‌های برتر برای تولید دانش و توزیع دانش برای یگان‌های عملیاتی به‌عنوان سه حوزه مشخص‌فناوری‌های برتر اطلاعات هستند که در این راستا نقش اطلاعات در ارتقای فناوری‌ها و دغدغه‌های اطلاعاتی باعث می‌شود تا تلاش‌هایی برای ارتقای فناوری اطلاعات صورت گیرد؛ بنابراین داشتن اطلاعات و اشراف اطلاعاتی از اهمیت بسزایی در پیشگیری از وقوع جرم برخوردار است.

با توجه به رشد روزافزون سامانه‌ها و نرم‌افزارها در فضای مجازی، دیگر نمی‌توان به‌راحتی، صحبت از یک سامانه کاملاً ایمن به میان آورد، به‌علاوه اینکه در کنار ناامنی‌های سخت‌افزاری و نرم‌افزاری فراوان موجود، در حال حاضر، مهم‌ترین شیوه رایج و تأثیرگذار در فضای مجازی، عملیات روانی دشمن است که اعتقادات و فکر و ذهن حریف را در اختیار می‌گیرد و امروزه کاربرد ویژه‌ای در فضای مجازی دارد.

پیشنهادها

ارتقای سامانه‌های مانیتورنیگ توسط معاونت‌های فاوا و فتای ناجا و با هماهنگی ستاد کل نیروهای مسلح، منجر به توسعه دفاع مجازی به منظور صیانت از داده‌پردازی مطمئن خواهد شد؛ همچنین جذب نیروهای متخصص و کارشناسان مجرب و آشنا با اصول امنیت در فضای مجازی و استمرار و تداوم آموزش‌های مرتبط، کاهش زمینه آسیب‌های فضای مجازی را به‌دنبال خواهد داشت.

لزوم آموزش کارکنان در خصوص شیوه‌های مقابله با عملیات روانی دشمن و افزایش مقاومت و پایدارای آنان در مقابل جنگ نرم و توجه به حیله‌ها و نیرنگ‌های دشمن می‌تواند آنان را در مقابل مخاطرات، ایمن نماید؛ همچنین آموزش کارکنان درخصوص جرائم رایانه‌ای و آشنا نمودن کارکنان با قوانین مربوط با این دسته از جرائم، در کاهش نرخ جرائم فضای مجازی بسیار مؤثر است.

مدیریت اطلاعات، امروزه به مفهومی پیچیده تبدیل شده است؛ زیرا اطلاعات موجود، حجمی نا باورانه به خود گرفته است و روز به روز بر این حجم افزوده می‌شود و در این راستا نیاز مبرم به کارکنان کار آزموده و متخصص در حوزه مجازی وجود دارد و در این راستا، ایجاد مراکز آموزش تخصصی باید مد نظر باشد.

تدوین دوره‌های تخصصی در حوزه فضای مجازی، تأسیس دانشکده فتا در مقاطع تحصیلی کاردانی، کارشناسی و کارشناسی ارشد مرتبط با مأموریت‌های فتا، برگزاری رزمایش های پیشگیری از جرم در فضای مجازی، تولید، ارائه و رشد فناوری اطلاعات بر اساس هوشمندسازی، توسعه دانش فضای مجازی به‌منظور کاهش میزان خطرپذیری تصمیم مدیران، گشت‌های اینترنتی، کاوش در داده‌ها از طریق سامانه‌های مختلف، پشتیبان تصمیم‌گیری و سامانه‌های هوش مصنوعی و استفاده از شبکه‌های پردازش مرکزی می‌توانند به عنوان اصلی‌ترین سیاست‌ها و راهبردهای این حوزه مدنظر قرار گرفته و در اسرع وقت اجرایی و کاربردی شوند.

کتابنامه

انستیتو ایز ایران (۱۳۸۷)، ***جنگ سایبر***

سروری، اسدا... (۱۳۸۸)، ***اصول و مبانی پدافند غیر عامل***، دانشگاه علوم انتظامی

دزیانی، محمدحسن، ***جرائم رایانه ای***، سازمان مدیریت و برنامه ریزی، جلد اول

متواضع، مرتضی (۱۳۸۴)، ***علوم رایانه ای***، دیبا گران.

روشندل، جلیل (۱۳۷۴)، ***امنیت ملی و نظام بین المللی***، سمت

اسدی، مریم، فصلنامه علوم اطلاع‌رسانی، ***شهر الکترونیک***، همدان (http://hamedan.ir.com/post)

سایت اینترنتی پلیس کشور www.cybrpolice.ir

شفیعی، عبدالحسین، (۱۳۸۵)، ***سیاست اطلاع‌رسانی و تکنولوژی اطلاعاتی: اطلاعات و ارتباطات***، تهران، سازمان چاپ و انتشارات علوم انسانی.

قورچیان، نادرقلی، ***دانش مدیریت***، نشرسمت، شماره ۴۵، سال ۱۳۷۸.

نجفی ابرندآبادی، علی‌حسین (۱۳۸۷) ***مباحثی در علوم جنایی (تقریرات)***، ویراست پنجم، به کوشش شهرام ابراهیمی.

فرجی‌ها، محمد (۱۳۸۹)، ***طرح تدوین برنامه ملی پیشگیری از جرم***، مرکز تحقیقات کاربردی پلیس پیشگیری ناجا.

نوروزی، بهرام و بارانی، محمد و سرکشیکیان، سیدمحمدحسین (۱۳۹۰) ***پیشگیری از جرم از نظریه تا عمل***، مرکز تحقیقات کاربردی پلیس پیشگیری ناجا.

عباچی، مریم (۱۳۸۸)، ***پیشگیری از بزه‌دیدگی مکرر کودکان با تأکید بر نقش پلیس، پیشگیری از تکرار جرم و تکرار بزه‌دیدگی***، مجموعه مقالات ارائه شده در نخستین همایش ملی پیشگیری از جرم، تهران: معاونت آموزش ناجا.

نجفی ابرندآبادی، علی‌حسین (۱۳۸۰)، ***پیشگیری از بزهکاری و پلیس محلی***، مجله امنیت، سال پنجم، شماره ۲۱ و ۲۲.

Crawford, A. (2007), Crime Prevention and Community Safety, the Oxford Handbook of Criminology, 4th Edition, New York, Oxford University Press.