

## پیشگیری انتظامی از جرم سرقت رایانه‌ای<sup>۱</sup>

ساسان رضایی‌فرد<sup>۲</sup>، جواد نیک افشار<sup>۳</sup>

تاریخ دریافت: ۱۴۰۰/۰۸/۰۴ تاریخ پذیرش: ۱۴۰۰/۰۹/۳۰

### چکیده

**زمینه و هدف:** باتوجه به گسترش روزافزون شبکه‌های رایانه‌ای و ارتباطی که برجسته‌ترین آن اینترنت است و سهولت و سرعت بیشتر این شبکه‌ها و ابزارها، مردم گرایش بیشتری برای استفاده از این ابزارها برای انجام امور خود از قبیل کارهای روزمره و اعمال تجاری دارند که زمینه سوء استفاده سارقان اینترنتی و افراد سودجو به‌منظور سرقت موجودی حساب کارت‌های بانکی را فراهم می‌کند. بنابراین پژوهش حاضر باهدف بررسی راهکارهای پیشگیری انتظامی از سرقت رایانه‌ای در فضای مجازی انجام شد.

**روش:** پژوهش حاضر از نظر هدف کاربردی و از نظر نوع تحقیق، توصیفی - تحلیلی است. جامعه آماری پژوهش کارکنان پلیس فتای استان کرمانشاه بودند که ۲۵ نفر از آنها به روش تصادفی انتخاب شدند. ابزار گردآوری داده پرسشنامه محقق‌ساخته بود که داده‌های آن با روش‌های توصیفی و استنباطی تحلیل شد. **یافته‌ها و نتایج:** یافته‌های پژوهش نشان می‌دهد که هشدارهای پلیس به مردم در ارتباط با شیوه و شگردهای مجرمان در فضای مجازی، اطلاع‌رسانی کامل و جامع به‌صورت مصدق از طریق وسایل ارتباط جمعی، آموزش مناسب و تخصصی پلیس و ضابطان قضایی درخصوص نحوه مقابله با جرم سرقت رایانه‌ای، میزان استفاده از ویروس‌کش‌های به‌روز و درگاه‌های پرداخت معتبر در خریدهای اینترنتی نقش موثری در پیشگیری انتظامی از سرقت رایانه‌ای در فضای مجازی دارد.

**کلیدواژه‌ها:** پیشگیری انتظامی، پلیس، سرقت رایانه‌ای، شبکه‌های ارتباطی، جرائم رایانه‌ای.

۱. این مقاله برگرفته از پایان‌نامه کارشناسی ارشد رشته حقوق جزا و جرم‌شناسی دانشگاه آزاد واحد تهران مرکز با همین عنوان است.

۲. استادیار گروه حقوق جزا و جرم‌شناسی، دانشگاه آزاد اسلامی واحد کرمانشاه، کرمانشاه، ایران. (نویسنده مسئول). رایانامه: rezaiefard.s@yahoo.com

۳. کارشناسی ارشد حقوق جزا و جرم‌شناسی، دانشگاه آزاد واحد تهران مرکز، تهران، ایران. رایانامه: jnikafshar@gmail.com

## مقدمه

فضای سایبری در کنار کارکردهای مهم و حیاتی، محل فعالیت انسان‌های فرصت‌طلب نیز هست. یکی از جرائمی که در فضای سایبری توسط این افراد رخ می‌دهد، سرقت داده‌ها و اطلاعات متعلق به دیگران است که برای جلوگیری و هرچه کمتر کردن ارتکاب این جرم، به‌خصوص توسط افرادی که سابقه‌دار نبوده و ویژگی‌های فضای مجازی آنها را به ارتکاب جرم ترغیب می‌کند، استفاده از راهکارهای پیشگیری از جرم است. این راهکارها شامل دو روش پیشگیری وضعی و پیشگیری اجتماعی می‌شوند، از جمله شیوه‌های تأثیرگذار در کاهش وقوع جرم سرقت رایانه‌ای هستند که هرچند در اصل برگرفته از شیوه‌های پیشگیری از سرقت‌های سنتی هستند ولی با تطبیق آنها با شرایط فضای سایبری می‌توانند موجب کاهش جرم سرقت رایانه‌ای شوند. روش‌های متعددی برای معرفی برنامه‌های پیشگیری از جرم توسط پلیس به مردم وجود دارد. به‌طور مثال ممکن است این اقدامات در برنامه‌ها و وب‌گاه‌های خبری به اطلاع مردم برسد یا روزنامه‌ها و جراید جزئیاتی از اقدامات پلیس را منعکس کنند. اقدامات پیشگیرانه پلیس باید دارای ویژگی‌های زیر باشد:

- ۱- از یک تلاش برنامه‌ریزی شده برخوردار باشد؛
- ۲- توسط نهاد اجرایی پلیس انجام شود؛
- ۳- هدف آن گسترش برنامه‌های پیشگیرانه پلیس میان مخاطبان و آموزش بزه‌دیدگان یا بازداشتن بزهکاران از ارتکاب جرم باشد.

در رویکردهای پیشگیرانه، نقش اجتماع و فرهنگ بی‌بدیل است. آموزش و فرهنگ به‌عنوان بستر حرکت جوامع و الگوهایی که انعکاس‌دهنده ارزش‌ها، سنت‌ها و هنجارهای پایدار جامعه‌اند در مباحث پیشگیری از جرم در فضای سایبری لازم است مدنظر قرار گیرد. برای این منظور می‌توان فرهنگ‌سازی سایبری را وارد نظام آموزشی مدارس، دانشگاه‌ها و مراکز علمی کرد زیرا مدرسه و محیط آموزشی بخش اعظمی از زندگی یک فرد را به خود

اختصاص می‌دهد؛ بنابراین نقش مهمی در تکوین شخصیت فرد و نهادینه شدن بسیاری از هنجارهای درون فرد دارد اما برای نهاد اجرایی مانند پلیس کم‌ترین نقش در این حوزه دیده شده و میزان مشارکت نهادهای فرهنگی و آموزشی با این نهاد اقداماتی نمادین و محدود است. تبلیغات عمومی یا آگهی‌های پیشگیری از جرم یکی از ابزارهای پلیس برای تقویت تدابیر پیشگیرانه انتظامی است و در کشورهای مختلف به صورت‌های متفاوتی از آن استفاده می‌شود. از طرفی فعالیت‌های جاری نهادهای عمومی و خصوصی، حسب مورد، می‌تواند نقش مستقیم یا غیرمستقیم در کاهش یا افزایش عوامل ایجادکننده جرم و ناهنجاری داشته باشد. بنابراین سیاست پیشگیری از جرم زمانی می‌تواند مؤثر واقع شود که بتواند سیاست‌ها و فعالیت‌های جاری نهادهای تأثیرگذار در عوامل ایجادکننده جرم را با آموزه‌های پیشگیری از جرم هم‌سو کند. یکی از روش‌های هم‌سوسازی اقدام‌های جاری نهادهای دولتی و خصوصی با آموزه‌های پیشگیری از جرم، رویکرد نوینی باعنوان پیشگیری چندنهادی است. این رویکرد، تدابیر پیشگیرانه نهاد پلیس را وارد مرحله‌ای جدید کرده، که در آن پلیس علاوه بر بهره‌گیری از ابزارهای ترسیم‌شده در نظام عدالت کیفری، تلاش می‌کند که از همکاری و مشارکت نهادهای دولتی و اجتماعی و شهروندان، در راستای پیشگیری از جرم استفاده کند. در سنوات اخیر پلیس برای کارآیی، اثربخشی و بهره‌وری خود در جامعه و توسعه آن در عرصه‌های مختلف گام‌های مؤثری را برداشته است.

اقدام‌های مداخله‌ای پلیس در زمینه پیشگیری از جرم مبتنی بر رویکردهای خاص موجود در هر سازمان پلیس است و یکی از مهم‌ترین رویکردهای عملی پلیسی رایج در زمینه پیشگیری از جرم، رویکرد جامعه‌محوری است. در این رویکرد پلیس خود را به‌عنوان بخشی از جامعه دانسته و تلاش دارد با جلب همکاری سایر اقشار اجتماعی به پیشگیری از جرم بپردازد. پیشگیری انتظامی جامعه‌محور از جرم نیز رویکردی است که در آن پلیس علاوه بر بهره‌گیری از ابزارهای تعریف‌شده در نظام عدالت کیفری، از همکاری و مشارکت نهادهای اجتماعی و دولتی برای کنترل عوامل ایجادکننده جرم استفاده و در تلاش است تا

از رهگذر تغییر در ساختارهای سازمانی و روش‌های اجرایی، خود را در قبال شهروندان مسئول کند تا در ادامه بتواند از مشارکت حداکثری اجتماع در کنترل عوامل ایجادکننده جرم بهره‌بردارد. پیشگیری از وقوع جرم تدابیری است که با کمک آن وسعت و شدت ارتکاب جرم، چه با کاهش فرصت‌ها و موقعیت‌های ارتکاب جرم و چه با تحت تأثیر قراردادن مجرمان بالقوه و کل جامعه به حداقل می‌رسد. پیشگیری از جرم عبارت است از پیش‌بینی، شناسایی و ارزیابی خطر وقوع جرم و به‌کارگیری تدابیر و اقدام‌های لازم برای از بین بردن یا کاهش آن.

سرقت به‌عنوان یکی از جرائم علیه اموال در قانون مجازات اسلامی به ربودن مال متعلق به غیر تعریف شده که پیشرفت روزافزون فناوری باعث شده شیوه و ابزار ارتکاب این جرم نیز تغییر پیدا کند. قانون‌گذار تحول سرقت از طریق رایانه را به‌عنوان سرقت رایانه‌ای جرم‌انگاری کرده است. در سرقت رایانه‌ای رفتار مجرمانه ربودن است اما این ربودن به دو روش ممکن است انجام شود. در یکی از این روش‌ها پس از سرقت اطلاعات و محتوای متعلق به دیگری دارنده آنها از این اطلاعات و محتوا محروم می‌شود و دیگر نسخه‌ای از آنها در اختیارش باقی نمی‌ماند. در روش دیگر پس از سرقت اطلاعات همچنان یک نسخه از آن در اختیار صاحب آن باقی می‌ماند که این روش با کپی کردن اتفاق می‌افتد مانند آنکه کسی رایانه خود را برای تعمیر نزد شخصی بگذارد و او بدون اجازه از فایل‌های دیگران کپی بگیرد. نکته دیگری که باید مدنظر قرار گیرد آن است که در سرقت رایانه‌ای با ربودن داده و اطلاعاتی روبرو هستیم که در سامانه‌های رایانه‌ای و مخابراتی مانند لپ‌تاپ، تلفن همراه و یا ابزارهای حامل داده مانند اطلاعات موجود درون فلش و مانند آن وجود داشته است. در سرقت سنتی موضوع جرم مال است و باید آنچه که ربوده می‌شود، دارای ارزش اقتصادی باشد اما در سرقت رایانه‌ای چون قانون‌گذار بر این موضوع تأکید نکرده است، موضوع سرقت رایانه‌ای می‌تواند داده، محتوا و اطلاعات دارای ارزش مالی یا غیرمالی باشد. قانون‌گذار در ماده ۷۴۰ قانون تعزیرات، سرقت رایانه‌ای را تعریف کرده است. طبق این

ماده قانونی، هرکس به طور غیرمجاز داده‌های متعلق به دیگری را برباید چنانچه عین داده‌ها در اختیار صاحب آن باشد، به جزای نقدی از یک میلیون ریال تا بیست میلیون ریال و در غیر این صورت به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد.

پژوهش‌های متعدد نشان می‌دهند که صرف انجام تدابیر پیشگیرانه انتظامی توسط پلیس، اثر محدودی در زمینه پیشگیری از جرم دارد اما در صورتی که پلیس در کنار این اقدامات پیشگیرانه، تبلیغات عمومی را در دستور کار خود قرار داده و به جامعه منتقل کند، اثرات پیشگیرانه اقدامات پلیس تشدید شده و طیف وسیع‌تری از مردم را پوشش خواهد داد. برای اینکه تبلیغات پیشگیرانه اثربخشی لازم را داشته باشد، ضروری است که مخاطبان آن به خوبی تعریف شوند؛ همچنین در هنگام طراحی آن، زمان و مکان مشاهده تبلیغات توسط مخاطبان مدنظر قرار گیرد.

جامعه و سایر نهادهای عمومی و دولتی، انجام تبلیغات عمومی و پیشگیرانه، آموزش روش‌های پیشگیری از جرم از طریق تلویزیون و رسانه‌های مکتوب، ارائه دوره‌های آموزشی پیشگیری از جرم برای پلیس که هدف نهایی این تدابیر ترغیب جامعه به قبول مسئولیت بیشتر در مورد امنیت شخصی است، در واقع بدون همکاری بدنه اجتماع، توفیق پلیس در پیشگیری انتظامی از جرم ناممکن به نظر می‌رسد اما همکاری جامعه مستلزم آگاهی مردم از مسئله جرم و شیوه‌های پیشگیری از آن است. بنابراین پرسش اصلی پژوهش حاضر این است که مؤلفه‌های اساسی پیشگیری انتظامی از جرم سرقت رایانه‌ای کدامند؟ همچنین پرسش‌های فرعی پژوهش عبارت‌اند از: ۱- افزایش آگاهی مردم در پیشگیری از جرم سرقت رایانه‌ای تا چه اندازه مؤثر است؟؛ ۲- تأثیرات ایمنی و تقویت سیستم‌ها و ابزارهای رایانه‌ای در پیشگیری از جرم سرقت رایانه‌ای تا چه اندازه است؟؛ ۳- تأثیر پیشگیری انتظامی در کاهش توانایی مرتکبان جرم سرقت رایانه‌ای تا چه اندازه است؟؛ ۴- پیشگیری انتظامی در جرم سرقت رایانه‌ای در کاهش منافع قابل پیش‌بینی از

ارتکاب جرم مؤثر تا چه اندازه است؟ و ۵- اثرات پیشگیری انتظامی در کاهش عوامل محرک ارتکاب جرم سرقت رایانه‌ای تا چه اندازه است؟

**پیشینه:** باتوجه به بررسی‌های انجام‌شده، بیشتر پژوهش‌های داخلی موجود، بارویکردی حقوقی به جرائم و تخلفات رایانه‌ای پرداخته‌اند. خرم‌آبادی (۱۳۸۴) در رساله دکتری خود با عنوان جرائم فناوری اطلاعات و طارمی (۱۳۸۷) در مقاله‌ای با عنوان طبقه‌بندی و آسیب‌شناسی جرائم رایانه‌ای، با رویکردی حقوقی به انواع جرائم رایانه‌ای، خصوصیات و نیز چالش‌های مربوط به این جرائم می‌پردازند و راهکارهایی را برای مقابله با این آسیب ارائه داده و به لوایح قانونی موجود در این زمینه و کاستی‌های آن تأکید کرده‌اند. رضوی (۱۳۸۷) در مقاله‌ای با عنوان پیشگیری انتظامی از جرائم سایبری و جلالی فراهانی (۱۳۸۳) در مقاله‌ای با عنوان پیشگیری از جرائم رایانه‌ای، روش‌های پیشگیری از جرائم رایانه‌ای را بررسی کرده‌اند. صادقی فسائی و محمدی (۱۳۸۴) در مقاله‌ای با عنوان نگاهی جرم‌شناسانه بر جرائم، امنیت و کنترل در اینترنت و آسیب‌های اجتماعی، راودراد (۱۳۸۴) در مقاله خود با عنوان مسائل اجتماعی زنان در اینترنت، عبدالهیان (۱۳۸۴) در مقاله‌ای با عنوان نوع‌شناسی و بازتعریف آسیب‌های اینترنتی و تغییرات هویتی در ایران و رازقی (۱۳۸۹) در پژوهشی با عنوان شناخت آسیب‌ها و جرائم اجتماعی در فضای مجازی از منظر جامعه‌شناختی به بررسی جرائم رایانه‌ای و پیامدهای آن و راهکارهای پیشگیری و مبارزه با این جرائم پرداخته‌اند.

بررسی‌ها نشانگر آن است که پژوهش‌های انجام‌شده در حیطه جامعه‌شناسی محدود بوده و بیشتر توصیفی است. در میان این تحقیقات، میزان جرائم رایانه‌ای و علل ارتکاب به آنها کمتر بررسی شده است. پژوهش‌های انجام‌شده بیشتر به‌روش اسنادی و کتابخانه‌ای انجام شده و فاقد چارچوب نظری بودند و به‌نظر می‌رسد تاکنون تخلفات رایانه‌ای در ایران، به‌طور کافی از منظر جامعه‌شناختی و از دیدگاه یادگیری اجتماعی به‌طور کلی بررسی نشده است. همچنین در پژوهش‌های انجام‌شده تفکیکی میان جرائم و تخلفات رایانه‌ای دیده نشده

و همه رفتارهای انحرافی مرتبط با رایانه با عنوان جرائم رایانه‌ای بررسی شده‌اند. در زمینه جرائم رایانه‌ای، پژوهش‌های غیرفارسی زیادی صورت گرفته و مباحث و موضوعات متعددی از قبیل بررسی مجرمان و قربانیان جرائم رایانه‌ای، گرایش به جرائم رایانه‌ای، میزان و انواع جرائم رایانه‌ای بررسی شده است. همچنین تنوع دیدگاه‌های روان‌شناختی، حقوقی و جامعه‌شناختی نیز در این زمینه به چشم می‌خورد. هلینگر (۱۹۹۲) در پژوهش خود با عنوان جرم رایانه‌ای، ارتباط سرقت نرم‌افزاری و دسترسی غیرمجاز به رمز عبور دیگران، از منظر نظریه یادگیری اجتماعی به بررسی مجرمان رایانه‌ای پرداخته است. اسکینر و فریام (۱۹۹۷) در مقاله‌ای با عنوان تحلیل نظریه یادگیری اجتماعی از جرائم رایانه‌ای در میان دانشجویان دانشگاه به بررسی پنج رفتار غیرقانونی رایانه‌ای شامل استفاده عمدی از نرم‌افزار کپی شده یا کپی کردن نرم‌افزار بدون اجازه، حدس زدن رمز عبور دیگران برای نفوذ به رایانه آنها یا دسترسی به فایل‌هایشان، دسترسی به رمز ورود رایانه دیگران بدون اجازه یا اطلاع آنها برای نگاه کردن به فایل‌ها یا اطلاعاتشان، اضافه کردن، حذف کردن، تغییر یا پخش هر اطلاعاتی از رایانه دیگران بدون اجازه یا اطلاع آنها و نوشتن برنامه ویروس یا استفاده از برنامه‌ای که به اطلاعات دیگران صدمه بزند پرداخته است. نتایج پژوهش یادشده، نشانگر رابطه معنادار بین میزان پیوند افتراقی، تقویت و تنبیه افتراقی، تعاریف و منابع تقلید با جرم رایانه‌ای بوده است. به عبارت دیگر براساس یافته‌های پژوهش یادشده، هرچه فرد با دوستانی که مرتکب جرائم رایانه‌ای می‌شوند بیشتر در ارتباط باشد و هرچه بیشتر از محیط اطراف از قبیل مدرسه و خانواده این جرائم را یاد بگیرد و نیز هرچه این قبیل رفتارها بیشتر تأیید شوند، فرد بیشتر مرتکب این جرائم می‌شود.

### مبانی نظری

نکته بسیار مهم در برخورد و مبارزه با جرائم رایانه‌ای استانداردهای فنی و اخلاق حرفه‌ای افراد است. مسلماً زمانی می‌توان از افراد انتظار عملکرد صحیح داشت که به‌راستی به وی

تفهم شود که چه تدابیر امنیتی باید به کار گیرد و چه اخلاق شغلی را رعایت کند. بنابراین مشخص است که چه در زمینه اخلاق حرفه‌ای و چه در زمینه اتخاذ تدابیر امنیتی، دولت‌ها، شرکت‌ها و حتی اشخاص لازم است درباره آموزش، شناسایی، فراگرفتن، استفاده از رایانه و فناوری‌های نوین ارتباطی موجود در شبکه‌های بین‌المللی اهتمام ورزند (باستانی، ۱۳۹۰، ص ۱۲۸).

طیف وسیعی از مجرمان و بزه‌دیدگان جرائم رایانه‌ای را افراد کم سن و سال تشکیل می‌دهند. بنابراین از جمله تدابیر بسیار موثر در پیشگیری از جرائم رایانه‌ای از جمله سرقت رایانه‌ای، ارائه آموزش کافی و اطلاع‌رسانی به‌هنگام است. آگاه ساختن افراد و ارائه آموزش‌های لازم از سنین کودکی می‌تواند تاثیر شایان توجهی در مقابله با جرم رایانه‌ای به‌ویژه سرقت رایانه‌ای داشته باشد.

**پیشگیری رشدمدار از سرقت رایانه‌ای:** پیشگیری رشدمدار به‌دنبال بهبود پایدار توانایی‌های اجتماعی اطفالی است که خطر گرایش آنها به دنیای بزهکاری زیاد است. این نوع از پیشگیری بر این اندیشه مبتنی است که رفتار و آداب اکتسابی دوران رشد یعنی از تولد تا سن بزرگسالی زمینه‌ساز ارتکاب اعمال مجرمانه می‌شود. هدف پیشگیری رشدمدار بهبود پایدار صلاحیت اجتماعی اطفالی است که مستعد ورود به دنیای بزهکاری هستند. این تدابیر به‌دنبال احیای شرایطی است که اجازه دهد قابلیت‌های فکری، اخلاقی و اجتماعی طفل رشد کنند. در دو مرحله اعمال می‌شود: در ابتدا و قبل از هر چیز، این مداخلات به‌منظور دستیابی به بیشترین اثربخشی باید زودهنگام باشد و نسبت به اطفال اعمال شود. پس از این مرحله، اقدامات باید در بستر خانواده و مدرسه اعمال و دنبال شود. درواقع هدف اساسی در این جا این است که اختلالات رفتاری ریشه‌دار نشود و خلاءهای شناختی برطرف و جبران شود (ابراهیمی، ۱۳۹۰، ص ۷۳-۷۴). اولین محیطی که توجه متصدیان پیشگیری رشدمدار را به خود جلب می‌کند خانواده و به‌دنبال آن والدین است. چنانچه بتوان در ابتدا توصیه‌ها و آموزش‌های لازم را به والدین منتقل کرد آنها را با خطرها و در عین



حال مزایا و مطلوبیت‌های فضای سایبر که در آن سرقت رایانه‌ای رخ می‌دهد آشنا کرد، می‌توان امیدوار بود که تا حدود زیادی اهداف این تدابیر به ثمر بنشینند. در کنار خانواده نقش دوستان، مریبان و دیگر مسئولان آموزشی و تربیتی نیز در شکل‌گیری شخصیت کودکان در استفاده از فضای سایبر حائز اهمیت است. بیشتر نظریه‌های جرم‌شناسی به ارتباط میان مجرم و عوامل مختلف زیست‌شناسانه، روان‌شناسانه یا اجتماعی توجه می‌کنند و می‌پندارند که صرف نظر از سن مجرمان، این عوامل تاثیر یکسانی دارند. برعکس، نظریه پردازان رشدنگر بر این پندارند که عوامل مختلف ممکن است بر مجرمان در سنین مختلف تاثیرهای متفاوت داشته باشد (ولد، برنارد و اسنیپس، ۱۳۹۴، ص ۳۷۷ و ۴۰۱).

**پیشگیری اجتماعی جامعه‌مدار سایبری در جرم سرقت رایانه‌ای: هدف از تدابیر پیشگیری اجتماعی جامعه‌مدار، جلوگیری از شکل‌گیری یا بروز انگیزه مجرمانه در عموم جامعه به‌وسیله دو اقدام اصلی است:**

۱- ترغیب و تسهیل بروز انگیزش‌های مشروع و سودمند؛

۲- برحذر داشتن از ناهنجارهای سایبری.

چنانچه کاربران ملاحظه کنند که با ورود به شبکه اینترنت می‌توانند امور خود را به‌طور بهینه به پیش برند و این تحول مثبت را در زندگی خودشان احساس کنند، اولویت کاربری‌شان را در فضای سایبر به امور بیهوده اختصاص نخواهند داد. هنوز بسیاری از افراد با کارکرد اصلی این فناوری آشنا نیستند و ابزارهای الکترونیکی و ارتباطی را یک وسیله سرگرمی تلقی و در همین حد از آن بهره‌برداری می‌کنند، برای تغییر این نگرش باید از رسانه‌های ارتباط جمعی مثل تلویزیون و مانند آن استفاده کرد. راهکار دیگر تدوین کدهای رفتاری برای مشاغل گوناگون و الزام به آگاهی از مفاد آنی است. یک کد رفتاری می‌تواند توسط هر سازمانی برای الزام اعضای سازمان و تعیین مبنای انضباطی برقرار شود. جرائم رایانه‌ای از جمله سرقت رایانه‌ای می‌تواند از طریق بالابردن تدابیر آموزشی برای گروه‌های حمایتی مصرف‌کنندگان و بسط تدابیر امنیتی خصوصی کاهش یابد.

اغلب دولت‌ها قادر به حمایت مستقیم از شهروندان خود در زمینه جرائم ارتكابی در فضای سایبری نیستند اما می‌توانند ابزارهای کافی به‌کار گیرند تا به‌واسطه آن شهروندان بتوانند خودشان از خود در فضای سایبر حمایت کنند (زیبر، ۱۳۸۱، ص ۴۶).

یکی از مهمترین ویژگی‌های فضای سایبر فعالیت‌های رایانه‌ای در خلوت است، کاربر بدون آنکه کسی متعرض حریم وی شود می‌تواند تمایلات نفسانی خود را که چه بسا در عمل آنها را بروز نمی‌دهد از طریق فعالیت‌های منفی در فضای سایبر ابراز کند. امکان ارتكاب جرم در حریم امن باعث شده است که برخی افراد در فضای سایبر شخصیتی متفاوت از چهره واقعی خود در دنیای واقعی بروز دهند. بنابراین نباید تنها به تدابیر پیشگیرانه اجتماعی بسنده کرد، بلکه باید کوشید حداقل کودکان نتوانند در خلوت به فضای سایبر ارتباط برقرار کنند. از این رو لازم است سیستم‌های رایانه‌ای در اماکن عمومی منزل قرار گیرند. معضل دیگری که فضای سایبر به‌طور خاص برای تدابیر پیشگیرانه اجتماعی به‌وجود آورده، ایجاد یک دنیای دیگر با شرایط مخصوص به خود است. پدیدآورندگان فضای سایبر از همان ابتدا معتقد بودند که این فضا ماهیت مجازی (جلالی فراهانی و باقری اصل، ۱۳۸۶، ص ۱۵۰) دارد و در واقع آن‌را در برابر دنیای واقعی قرار می‌دهند. این امر باعث شده که کاربران با تلقی مجازی بودن فضای سایبر سعی در اجرای رویای خود در این فضا داشته باشند و مرتکب جرم رایانه‌ای همچون سرقت اطلاعات و نسخه‌پردازی از داده‌ها شوند. درحالی‌که یکی از قابلیت‌های این فضا مجازی‌سازی است و نباید آن را با مجازی بودن اشتباه گرفت. بیشتر کاربران شبکه‌ای از فضای سایبر این تصور را در ذهن دارند که فقط یک‌سری تصاویر و اعداد و ارقام در صفحه نمایشگر قابل رؤیت هستند. غافل از اینکه تمام افعال سایبری در زندگی فیزیکی آنان اثر و بازتاب مستقیم و واقعی دارد. البته این معضل تا حدود زیادی قابل حل است حتی شاید بتوان امیدوار بود حل آن تا حدودی بتواند معضل قبلی را برطرف کند زیرا اگر افراد بدانند حتی در حریم‌شان نیز چشمان بیدار بسیاری مراقبشان هستند و سوابق فعالیت‌شان در موقعیت‌های متعددی به ثبت می‌رسد، و از همه

مهمتر اعمال بر زندگی‌شان در دنیای فیزیکی آثار مستقیم و غیرمستقیم بسیاری برجای می‌گذارد با احتیاط بیشتری عمل خواهند کرد (جلالی فراهانی، ۱۳۸۶، ص ۱۵۱).

معضل دیگر فضای سایبر برای تدابیر پیشگیرانه اجتماعی به ماهیت بین‌المللی و یا به بیان بهتر فرامرزی این فضا مربوط می‌شود. گفتیم که تدابیر پیشگیرانه اجتماعی که براساس هنجارها و ارزش‌های پذیرفته شده وضع می‌شوند که افراد حاضر در یک اجتماع مشخص آنها را می‌شناسند و به آنها باور دارند اما با حضور فضای سایبر به تدریج باورهای اجتماعی مردم نیز دچار تحول شده است. از این رو ضروری است با به‌کارگیری تدابیر پیشگیرانه اجتماعی به‌ویژه از نوع رشدمدار و بالابردن آگاهی کاربران جوان نسبت به این مسائل میزان لطمات را به حداقل رساند.

**محدودیت‌های ناشی از شکاف نسلی در پیشگیری اجتماعی از جرم سرقت رایانه‌ای:**

امروزه استفاده از سیستم‌های رایانه‌ای همانند گذشته در انتصاب قشر خاصی نیست و به‌دلیل فراگیری آن و امکانات بی‌شماری که فضای سایبر برای کاربری هرچه آسان‌تر آن فراهم آورده، گروه‌های جوان و نوجوان بیشتر از دیگران جلب شده‌اند. این در حالی است که تدوین‌کنندگان تدابیر پیشگیرانه اجتماعی با فضای سایبر رابطه عمیقی ندارند یا نمی‌توانند به اندازه جوانان و نوجوانان به فعالیت‌های شبکه‌ای بپردازند. این شکاف دیجیتال میان متولیان پیشگیری و بزه‌کاران و بزه‌دیدگان باید برطرف شود زیرا در این صورت نمی‌توان به تاثیرگذار بودن آنها امیدوار بود.

**پیشگیری وضعی از جرم سرقت رایانه‌ای:** به‌دنبال موفقیت ناقص پیشگیری اجتماعی در کاهش و مهار جرم، توسل به پیشگیری وضعی برای کنترل بزهکاری مدنظر قرار می‌گیرد. پیشگیری وضعی شامل مجموعه اقدام‌ها و تدابیری است که به‌سمت تسلط بر محیط و شرایط پیرامون جرم و مهار آن متمایل است. در پیشگیری وضعی با استفاده از شیوه‌ها و روش‌هایی چون تقویت آماج‌ها و سیبل‌های جرم، استفاده از فناوری‌های مراقبتی و کنترلی و مدیریت و طراحی محیطی به‌دنبال کاهش فرصت‌ها و موقعیت‌های ارتکاب جرم و تسلط

بر شرایط و اوضاع و احوال پیرامونی جرم و در نتیجه جلوگیری از وقوع جرم است (احمدی، ۱۳۸۸، ص ۱۱۶).

این نوع پیشگیری برخلاف پیشگیری اجتماعی به جای تکیه بر فرد بر محیط توجه دارد. تدابیر امنیتی زیادی درباره پیشگیری سایبری وجود دارد که هرگونه وقوع جرم یا دیگر ناهنجاری را به اطلاع مراجع ذیربط می‌رساند. یکی از این تدابیر، حفاظت از سیستم رایانه‌ای است. روش‌های حفاظت از سیستم عبارت‌اند از: حفاظت فیزیکی، حفاظت کارکنان، حفاظت ارتباطات و حفاظت عملیات که هدف همه آنها سخت‌تر ساختن دسترسی مجرمان به سیستم‌های رایانه‌ای است. سیستم امنیتی نامطلوب در بیشتر مواقع علت وقوع جرم سرقت رایانه‌ای است. تدابیر امنیتی نامطلوب در بیشتر مواقع حاصل بی‌اطلاعی از مشکلات موجود در زمینه امنیت داده‌ها است.

**نظریات یادگیری سرقت رایانه‌ای:** براساس نظریات یادگیری اجتماعی، رفتار انحرافی آموختنی است و در فرایند روابط با دیگران، به خصوص در گروه‌های کوچک آموخته می‌شود. فرآیند مدل‌سازی در کانون توجه نظریه یادگیری اجتماعی قرار دارد که در آن شخص رفتار اجتماعی دیگران را به وسیله مشاهده و تقویت یاد می‌گیرد و آموختنی‌ها را از طریق پاداش و تنبیه تقویت می‌شود. در این قسمت به سه نظریه از مشهورترین نظریه‌های یادگیری که قادر به تبیین سرقت‌های مقرون به تهدید و آزار هستند اشاره می‌شود:

**نظریه همنشینی افتراقی:** ساترلند بر این باور بود که رفتار انحرافی موروثی و ذاتی نیست و به همان روشی آموخته می‌شود که هر رفتار دیگری آموخته می‌شود. برای مثال دزدی‌های حرفه‌ای ممکن است نسبت به تجاوز به عنف، آدم‌کشی و اعتیاد به مواد مخدر به همان اندازه مردم درستکار نفرت داشته باشند (احمدی، ۱۳۸۸، ص ۹۶). او معتقد بود در فرآیند

هم‌نشینی با افراد کج‌رو، فراگیری رفتار مجرمانه در ابعاد زیر اتفاق می‌افتد:

- فنون ارتکاب جرم؛
- انگیزه‌ها و رهیافت‌ها و توجیه‌هایی که با جرم همراه است؛

• تعریف مجموعه‌ای از قوانین به‌عنوان امری مطلوب یا نامطلوب (برای نمونه نامطلوب دانست قوانین مربوط به سرقت خودرو با این استدلال که به هر حال مردم امکان استفاده از تسهیلات بیمه خودرو را دارند) (وایت و هینز، ۱۳۹۲، ص ۵۸).

می‌توان دریافت که نظریه ساترلند از نظر به‌رسمیت شناختن قدرت نیروهای اجتماعی در تعریف جرم، نظریه‌ای جامعه‌شناختی و از منظر توجه به فرد، نظریه‌ای روان‌شناختی است.

نظریه قانون تقلید تارد در جرم سرقت رایانه‌ای: گابریل تارد از نخستین جرم‌شناسانی است که این نظریه را مطرح کرد. نخستین قانون تارد این بود که مردم به تناسب میزان برخورد نزدیکی که با هم دارند، از یکدیگر تقلید می‌کنند از این رو تقلید در شهرها شایع‌تر است و با سرعت بیشتری تغییر می‌یابد. دومین قانون تارد این است که به‌طور معمول فرودستان از فرادستان تقلید را یاد می‌گیرند. سومین قانون تارد این بود که مدل‌های نوین‌تر جایگزین مدل‌های قدیمی‌تر می‌شوند. برای نمونه، وی استدلال می‌کند قتل عمدی ناشی از چاقو زدن کاهش یافته و قتل عمدی ناشی از تیراندازی افزایش یافته است (ولد و همکاران، ۱۳۹۴، ص ۲۵۸).

نظریات یادگیری کنشی ابزاری: اصول بنیادین این نظریه را اسکینر مطرح کرده است؛ به‌عقیده وی رفتارهای مجرمانه به‌دلیل تقویت‌هایی که همراه خود دارد آموخته و تحکیم می‌شوند. از منظر این نظریه، رفتارهای آدمی محصول جامعه و محیط است. به‌گونه‌ای که یادگیری رفتارهای مجرمانه به‌صورت تام از راه تقویت و تنبیه‌ها در جامعه صورت می‌گیرد. سه اصل مهم در نظریه اسکینر به این ترتیب است:

الف. تقویت همیشه ملموس و قابل مشاهده نیست و با الگوبرداری از رفتارها با پاره‌ای از تقویت‌های روانی نیز روبرو هستیم؛

ب- رفتارهای مجرمانه برای اولین بار آموخته می‌شود اما در استمرار و تکرار متکی به تقویت‌ها هستند.

ج- جوامع در مهندسی رفتار سعی می‌کنند که افراد به هنگام اطاعت از قانون از تقویت‌ها

بهره ببرند و نه به هنگام سرپیچی از مقررات (اسکینر و فریم<sup>۱</sup>، ۱۹۹۷، ص ۴۹۶).

**نظریات فشار:** دومین دسته از نظریاتی که به نظر می‌رسد با بحث سرقت‌های مقرون به تهدید و آزار مرتبط است، نظریات فشار است. نظریه فشار به جای پرداختن به دو بُعد روان‌شناسی فردی یا خصیصه‌های زیست، مدعی است که موجبات شکل‌گیری جرم را باید در درون جامعه جست. بدین ترتیب در نگاه این نظریه، یک مجرم محصول نوعی نظم خاص اجتماعی است (وایت و هینز، ۱۳۹۲، ۱۴۲).

## روش

پژوهش حاضر از نظر هدف کاربردی و از نظر نوع تحقیق، توصیفی - تحلیلی است. جامعه آماری پژوهش کارکنان پلیس فتای استان کرمانشاه بودند که ۲۵ نفر از آنها به روش تصادفی انتخاب شدند. ابزار گردآوری داده پرسشنامه محقق‌ساخته بود که داده‌های آن با روش‌های توصیفی و استنباطی تحلیل شد.

۱۳۰

## یافته‌ها

به‌منظور بررسی اهداف پایان‌نامه درباره جرم سرقت رایانه‌ای و سنجش دقیق آن در سطح جامعه، از کارکنان پلیس فتا نظرسنجی شد. ۲۲ نفر از کارکنان پلیس فتا که همگی مرد بودند در این پژوهش همکاری کردند. ۸۶/۳۶ درصد آنها متاهل و ۱۳/۶۳ درصد آنها مجرد بودند. میزان تحصیلات ۴/۵۴ درصد پاسخگویان کاردانی، کارشناسی ۵۴/۵۴ درصد، کارشناسی ارشد ۳۶/۳۶ درصد و دکتری ۴/۵۴ درصد بود. سنوات خدمت ۲۷/۲۷ درصد افراد زیر پنج سال، ۵۰ درصد افراد پنج تا ده سال، ۹ درصد افراد ده تا پانزده سال، ۹ درصد افراد پانزده تا بیست سال خدمت و ۴/۵۴ درصد افراد بیست و پنج تا سی سال، سابقه خدمت داشتند.

پرسشنامه پژوهش: پرسش‌های ارائه شده به جامعه آماری که برای پاسخ به هر سوال پنج گزینه به صورت زیر در نظر گرفته شده بود، در ادامه آمده است:

۱- اطلاع‌رسانی در خصوص روش‌های سارقان و خطرات احتمالی به مردم در پیشگیری از سرقت رایانه‌ای موثر است؛

۲- هشدارهای پلیس در ارتباط با شیوه و شگردهای مجرمان در فضای مجازی در پیشگیری از سرقت رایانه‌ای موثر است؛

۳- اطلاع‌رسانی کامل و جامع به صورت مصداقی از طریق وسایل ارتباط جمعی در پیشگیری از سرقت رایانه‌ای تاثیرگذار است؛

۴- آشناکردن کاربران با روش و فنون پیشگیری از سرقت از کارت‌های اعتباری در فضای مجازی در پیشگیری از سرقت رایانه‌ای موثر است؛

۵- آموزش مناسب و تخصصی پلیس جنایی و ضابطان قضایی در خصوص نحوه مقابله با جرائم فضای مجازی در پیشگیری از جرم سرقت رایانه‌ای موثر است؛

۶- میزان استفاده از ویروس‌کش‌های به‌روز در پیشگیری از جرم سرقت رایانه‌ای موثر است؛

۷- میزان استفاده از درگاه‌های پرداخت معتبر در خریدهای اینترنتی در پیشگیری از جرم سرقت رایانه‌ای موثر است؛

۸- تغییر مداوم رمز دوم کارت‌های اعتباری در پیشگیری از جرم سرقت رایانه‌ای موثر است؛

۹- تقویت سیستم‌ها و به‌روزرکردن آنها در مقابل بدافزارهای موجود در پیشگیری از جرم سرقت رایانه‌ای موثر است؛

۱۰- افزایش حضور پلیس فتا در فضای مجازی و معرفی نرم‌افزارهای جدید مقابله‌ای با سارقان اینترنتی در پیشگیری از جرم سرقت رایانه‌ای موثر است؛

- ۱۱- وجود سیستم‌های کنترلی مناسب و کنترل مداوم فضای مجازی به‌منظور هشدار به کاربران توسط پلیس فتا برای کاهش جرم سرقت رایانه‌ای موثر است؛
- ۱۲- شناسایی و برخورد با سارقان اینترنتی توسط دستگاه‌های نظارتی در پیشگیری از جرم سرقت رایانه‌ای موثر است؛
- ۱۳- استفاده از وسایل پیشرفته اطلاعاتی و امنیتی برای شناسایی مجرمان اینترنتی در پیشگیری از جرم سرقت رایانه‌ای موثر است؛
- ۱۴- شناسایی و کنترل سایت‌ها و کاربران مشکوک به اعمال مجرمانه، در پیشگیری از جرم سرقت رایانه‌ای موثر است؛
- ۱۵- تشدید برخورد با سارقان اینترنتی با اجرای طرح‌های ضربتی در پیشگیری از سرقت رایانه‌ای موثر است؛
- ۱۶- استفاده از تجهیزات پیشرفته علمی توسط پلیس در کشف سرقت‌های اینترنتی در پیشگیری از جرم سرقت رایانه‌ای موثر است؛
- ۱۷- شناسایی شرکت‌های هرمی در پوشش‌های مختلف در فضای مجازی در پیشگیری از جرم سرقت رایانه‌ای موثر است؛
- ۱۸- بالابردن سواد اینترنتی در بین کاربران برای پیشگیری از جرم سرقت رایانه‌ای موثر است؛
- ۱۹- افزایش اطلاع‌رسانی درخصوص برخورد قضایی و انتظامی با مرتکبان جرم سرقت در فضای مجازی، در پیشگیری از سرقت رایانه‌ای موثر است؛
- ۲۰- محرومیت مدنی سارقان به‌ویژه سارقان فضای مجازی در پیشگیری از جرم سرقت رایانه‌ای موثر است؛
- ۲۱- تشکیل کمیته‌های مبنی بر شناخت منافع ارتکاب جرم سرقت در فضای مجازی در پیشگیری از جرم سرقت رایانه‌ای موثر است؛



- ۲۲- شناسایی و انهدام باندهای سرقت‌های رایانه‌ای در پیشگیری از جرم سرقت رایانه‌ای موثر است؛
- ۲۳- اجرایی کردن مجازات‌های تعیین‌شده برای مرتکبان سرقت رایانه‌ای در پیشگیری از جرم سرقت رایانه‌ای موثر است؛
- ۲۴- آشنایی افراد از قوانین مرتبط با سرقت اینترنتی در پیشگیری از جرم سرقت رایانه‌ای موثر است؛
- ۲۵- کنترل افراد سابقه‌دار و سارقان اینترنتی در پیشگیری از جرم سرقت رایانه‌ای موثر است؛
- ۲۶- هشدارهای پلیس و دقت بیشتر در امر شناخت محرک‌هایی که باعث گرایش مرتکبان سرقت رایانه‌ای می‌شود، در کاهش این جرم موثر است؛
- ۲۷- بالابردن سواد اینترنتی کاربران در کاهش تحریک سارقان و پیشگیری از جرم سرقت رایانه‌ای موثر است؛
- ۲۸- تلاش برای بستن کامل راه‌های ارتکاب جرم سرقت اینترنتی و کاهش تحریک مجرمان بالقوه در کاهش این جرم موثر است؛
- ۲۹- ملزم کردن سایت‌های تبلیغ و فروش کالاهای مختلف در فضای مجازی در رعایت نکات قانونی و کنترل لازم بر آنان در کاهش سرقت‌های اینترنتی موثر است.

## یافته‌های توصیفی

جدول ۱. آمار توصیفی داده‌های پرسشنامه

شماره پرسش	حداقل نمره	حداکثر نمره	میانگین	خطای استاندارد	انحراف معیار
۱	۰	۱۴	۴/۴	۲/۶۳	۳۴/۸
۲	۰	۱۱	۴/۴	۲/۱۵	۲۳/۳
۳	۰	۱۲	۴/۴	۲/۲۹	۲۶/۳
۴	۰	۱۰	۴/۴	۱/۸۶	۱۷/۳
۵	۰	۱۰	۴/۴	۱/۹۳	۱۸/۸
۶	۱	۹	۴/۴	۱/۴۳	۱۰/۳
۷	۰	۱۰	۴/۴	۱/۷۲	۱۴/۸
۸	۰	۹	۴/۴	۱/۹۳	۱۸/۸
۹	۰	۱۱	۴/۴	۲/۱۵	۲۳/۳
۱۰	۰	۱۱	۴/۴	۲/۱۵	۲۳/۳
۱۱	۰	۹	۴/۴	۱/۷۲	۱۴/۸
۱۲	۰	۱۱	۴/۴	۲/۳۱	۲۶/۸
۱۳	۰	۹	۴/۴	۱/۷۲	۱۴/۸
۱۴	۰	۹	۴/۴	۱/۸۰	۱۶/۳
۱۵	۰	۱۱	۴/۴	۲/۰۳	۲۰/۸
۱۶	۰	۱۵	۴/۴	۲/۹۷	۴۴/۳
۱۷	۰	۱۰	۴/۴	۱/۸۰	۱۶/۳
۱۸	۰	۱۲	۴/۴	۲/۴	۲۸/۸
۱۹	۰	۱۱	۴/۴	۲/۱۵	۲۳/۳
۲۰	۰	۱۲	۴/۴	۲/۱۵	۲۳/۳
۲۱	۰	۸	۴/۴	۱/۶۳	۱۳/۳
۲۲	۰	۹	۴/۴	۱/۷۴	۱۵/۳
۲۳	۰	۱۰	۴/۴	۲/۲۹	۲۶/۳

شماره پرسش	حداقل نمره	حداکثر نمره	میانگین	خطای استاندارد	انحراف معیار
۲۴	۰	۹	۴/۴	۱/۹۳	۱۸/۸
۲۵	۰	۸	۴/۴	۱/۶۳	۱۳/۳
۲۶	۰	۱۱	۴/۴	۲/۱۱	۲۲/۳
۲۷	۰	۱۶	۴/۴	۲/۹۷	۴۴/۳
۲۸	۰	۹	۴/۴	۲/۰۱	۲۰/۳
۲۹	۰	۱۳	۴/۴	۲/۵	۳۱/۳

### یافته‌های استنباطی

توزیع نرمال، یکی از مهمترین توزیع‌ها در نظریه احتمال است و کاربردهای بسیاری در علم فیزیک و مهندسی دارد. این توزیع توسط کارل فریدریش گاوس در رابطه با کاربرد روش کمترین مربعات در آمارگیری کشف شد. فرمول آن برحسب دو پارامتر امید ریاضی و واریانس بیان می‌شود. همچنین تابع توزیع نرمال یا گاوس از مهمترین توابعی است که در مباحث آمار و احتمالات مورد بررسی قرار می‌گیرد زیرا به تجربه ثابت شده است که در دنیای اطراف ما توزیع بسیاری از متغیرهای طبیعی از همین تابع پیروی می‌کنند. با استفاده از آزمون کولموگروف - اسمیرنوف می‌توان پیروی یک‌سری زمانی را نسبت به یک توزیع آماری بررسی کرد، نه تنها توزیع نرمال بلکه برای بررسی پیروی داده‌ها از سایر توزیع‌ها هم می‌توان از این آزمون استفاده کرد. آزمون کولموگروف - اسمیرنوف که به افتخار دو آماردان روسی به نام‌های ان. کولموگروف و ن.و. اسمیرنوف به این نام خوانده می‌شود، روش ناپارامتری ساده‌ای برای تعیین همگونی اطلاعات تجربی با توزیع‌های آماری منتخب است. آزمون شاپیرو ویلک از آزمون‌های برازش توزیع نرمال محسوب می‌شود. به کمک این آزمون و آماره آن می‌توانید مشخص کنید که آیا داده‌ها از توزیع نرمال پیروی می‌کنند یا خیر. باتوجه به این موضوع می‌توان این آزمون را جز گروه روش‌های آمار ناپارامتری در نظر گرفت.

در آزمون شاپیرو ویلک فرض صفر به صورتی است که نمایانگر توزیع نرمال برای داده‌ها است. این روش آزمون براساس پژوهش‌های دو دانشمند «ساموئل شاپیرو» آمارشناس آمریکایی و «مارتین ویلک» آمارشناس کانادایی توسعه و به کار گرفته شد.

جدول ۲. نتایج آزمون‌های کولموگروف - اسمیرنوف و شاپیرو - ویلک

	نتایج آزمون کولموگروف - اسمیرنوف			نتایج آزمون شاپیرو ویلک		
	مقدار آماره	درجه آزادی	سطح معناداری	مقدار آماره سطح معناداری	درجه آزادی	سطح معناداری
پرسش فرعی اول	۰/۲۳۷	۵	۰/۲۰۰	۰/۸۶۲	۵	۰/۲۳۵
پرسش فرعی دوم	۰/۱۹۱	۵	۰/۲۰۰	۰/۹۳۱	۵	۰/۶۰۵
پرسش فرعی سوم	۰/۳۸۳	۵	۰/۰۱۶	۰/۷۲۸	۵	۰/۰۱۸
پرسش فرعی چهارم	۰/۲۴۶	۵	۰/۲۰۰	۰/۸۱۹	۵	۰/۱۱۴
پرسش فرعی پنجم	۰/۲۴۵	۵	۰/۲۰۰	۰/۸۷۳	۵	۰/۲۷۹

براساس پارامتر سطح معناداری در جدول‌های خروجی باید دریافت که داده‌ها از توزیع نرمال پیروی می‌کنند یا خیر؟ اگر پارامتر مذکور از  $0/5$  کمتر باشد داده‌ها از توزیع نرمال پیروی نکرده و اگر از  $0/5$  بیشتر باشد داده‌ها نرمال هستند. بر همین اساس و باتوجه به نتایج ارائه شده می‌توان دریافت که هیچ‌یک از داده‌ها نرمال نیستند.

### بحث و نتیجه گیری

باتوجه به گسترش روزافزون شبکه‌های رایانه‌ای و ارتباطی از دهه ۱۹۶۰ به بعد که برجسته‌ترین آن اینترنت است و سهولت و سرعت بیشتر این شبکه‌ها و ابزارها مردم

گرایش بیشتری برای استفاده از این ابزارها در انجام امور خود از قبیل کارهای روزمره و فعالیت‌های تجاری و سایر مواردی که نیاز به بستر اینترنت دارد به جهت صرفه‌جویی در زمان و کاهش هزینه‌های تردد خود به این سمت سوق پیدا کرده‌اند. از طرفی این موضوع زمینه بسیار مناسبی برای سارقان اینترنتی و افراد سودجو به‌منظور سرقت موجودی حساب کارت‌های بانکی به طرق مختلف را فراهم می‌کند. همین امر کارکنان پلیس فتا را واداشت که با استفاده از تجهیزات رایانه‌ای جدید و آشنایی با شگردهای مختلف سارقان اینترنتی و استفاده از نرم‌افزارهای به‌روز برای کشف جرائم فضای سایبر اقدامات لازم را معمول دارند. پس از انجام پژوهش فوق نتایج حاصل از بررسی و تحلیل آماری جرم سرقت رایانه‌ای در شهر کرمانشاه به شرح ذیل می‌شود:

باتوجه به نقش اطلاع‌رسانی در خصوص روش‌های سارقان، این اقدام در پیشگیری از جرم سرقت رایانه‌ای به‌شکل قابل ملاحظه‌ای موثر است.

درخصوص هشدارهای پلیس به مردم در ارتباط با شیوه و شگردهای مجرمان در فضای مجازی می‌توان گفت که امری بسیار تاثیرگذار درباره جرم یادشده است.

اطلاع‌رسانی کامل و جامع به‌صورت مصداقی برای عموم مردم از طریق وسایل ارتباط جمعی، در پیشگیری از سرقت رایانه‌ای بسیار تاثیر گذار است.

یکی از روش‌های موثر در پیشگیری از جرم سرقت رایانه‌ای آشناکردن کاربران فضای مجازی با روش و فنون سرقت از کارت‌های اعتباری در فضای مجازی است که این موضوع نیز از عوامل مهم در این خصوص تلقی می‌شود.

آموزش مناسب و تخصصی پلیس و ضابطان قضایی درخصوص نحوه مقابله با این جرم از عوامل مهم و موثر در جرم سرقت رایانه‌ای است.

استفاده از ویروس‌کش‌های به‌روز در پیشگیری از این جرم تا حدودی موثر و همچنین میزان استفاده از درگاه‌های پرداخت معتبر در خریدهای اینترنتی نیز بسیار موثر است.

یکی دیگر از روش‌های پیشگیری، تغییر مداوم رمز دوم کارت‌های اعتباری است که

می‌تواند مانعی برای جلوگیری از دستبرد سارقان در جرم یادشده باشد. همچنین تقویت سیستم‌ها و به‌روز کردن آنان در مقابل بدافزارهای موجود بسیار مهم است. افزایش حضور پلیس فتا در فضای مجازی و معرفی نرم‌افزارهای جدید مقابله‌ای با سارقان اینترنتی و وجود سیستم‌های کنترلی مناسب و کنترل مداوم فضای مجازی در دادن هشدارهای لازم به کاربران توسط آنان در کاهش جرم سرقت رایانه‌ای موثر است. شناسایی و برخورد با سارقان اینترنتی توسط دستگاه‌های نظارتی و استفاده از وسایل پیشرفته اطلاعاتی و امنیتی برای شناسایی مجرمان اینترنتی در پیشگیری از جرم یادشده موثر است.

شناسایی و کنترل سایت‌ها و کاربران مشکوک به اعمال مجرمانه و تشدید برخورد با سارقان اینترنتی با اجرای طرح‌های ضربتی در فضای مجازی از عوامل بسیار تاثیرگذار و حیاتی در پیشگیری از جرم یادشده است.

استفاده از تجهیزات پیشرفته علمی توسط پلیس در کشف سرقت‌های اینترنتی و شناسایی شرکت‌های هرمی در پوشش‌های مختلف در فضای مجازی در پیشگیری نیز یکی دیگر از موضوع‌های بسیار مهم در پیشگیری از سرقت رایانه‌ای است.

بالا بردن سواد اینترنتی در بین کاربران و افزایش اطلاع‌رسانی در خصوص برخورد قضایی و انتظامی با مرتکبان جرم سرقت در فضای مجازی در پیشگیری انتظامی از جرم یادشده نقش بسیار مهمی را ایفا می‌کند. ارتقاء سطح آگاهی کاربران از حقوق اجتماعی سارقان به‌ویژه سارقان در فضای مجازی و همچنین تشکیل کمیته‌های مبتنی بر شناخت منافع ارتکاب جرم سرقت در فضای مجازی در پیشگیری از این جرم موثر است.

شناسایی و انهدام باندهای سرقت‌های رایانه‌ای و اجرا کردن مجازات‌های تعیین‌شده برای مرتکبان، یکی از موضوع‌های بسیار مهمی است که نقش تعیین‌کننده‌ای در این زمینه دارد. هشدارهای پلیس و دقت بیشتر در امر شناخت محرک‌هایی که باعث گرایش مرتکبان به

جرم سرقت رایانه‌ای می‌شوند و همچنین کنترل افراد سابقه‌دار و سارقان اینترنتی و آشنایی این قبیل افراد با قوانین مرتبط با جرم یادشده در کاهش این جرم بسیار موثر است.

ملزم کردن سایت‌های تبلیغ و فروش کالاهای مختلف در فضای مجازی در رعایت نکات قانونی و کنترل لازم بر آنان و تلاش برای بستن کامل راه‌های ارتکاب جرم سرقت اینترنتی و کاهش تحریک مجرمان بالقوه در کاهش این جرم بسیار موثر است.

در مجموع براساس یافته‌های پژوهش حاضر، به‌طور خلاصه می‌توان گفت: افزایش و تعمیق سطح آگاهی‌های مردم و همچنین اثرات پیشگیری انتظامی در کاهش عوامل محرک و توانایی مرتکبان جرم سرقت رایانه‌ای و تأثیرات ایمنی و تقویت سیستم‌ها و ابزارهای رایانه‌ای و همچنین افزایش سطح آموزش مناسب و تخصصی پلیس و برخورد با سارقان اینترنتی درخصوص نحوه مقابله با جرم یادشده، تاثیر بسیار زیادی در پیشگیری انتظامی از جرم سرقت رایانه‌ای دارد.

## منابع

- ابراهیمی، شهرام. (۱۳۹۰). جرم‌شناسی پیشگیری. جلد اول. چاپ نخست. تهران: میزان.
- احمدی، حبیب. (۱۳۸۸). جامعه‌شناسی انحرافات. چاپ سوم. تهران: انتشارات سمت.
- باستانی، برومند. (۱۳۹۰). جرائم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهکاری. چاپ سوم. تهران: پیام.
- جلالی فراهانی، امیرحسین و باقری اصل، رضا. (۱۳۸۶). نهادسازی برای پیشگیری از جرائم رایانه‌ای (با نگاهی به قانون جرائم رایانه‌ای). رویکرد چندنهادی به پیشگیری از وقوع جرم (مجموعه مقالات نخستین همایش ملی پیشگیری از جرم). تهران: معاونت آموزش نیروی انتظامی.
- جلالی فراهانی، امیرحسین. (۱۳۸۳). پیشگیری از جرایم رایانه‌ای، مجله حقوقی دادگستری، ۶۸(۴۷)، صص ۸۷-۱۱۹. قابل بازیابی از: [http://www.jlj.ir/article\\_44548.html](http://www.jlj.ir/article_44548.html)

خرم‌آبادی، عبدالصمد. (۱۳۸۴). جرایم فناوری اطلاعات. پایان‌نامه مقطع دکتری. دانشکده حقوق و علوم سیاسی دانشگاه تهران.

رازقی، نادر. (۱۳۸۹). شناخت آسیب‌ها و جرایم اجتماعی در فضای مجازی. مجموعه مقالات همایش بررسی آسیب‌های اجتماعی. بابل‌سر: انتشارات دانشگاه مازندران.

راودراد، اعظم. (۱۳۸۴). مسائل اجتماعی زنان در اینترنت. فصلنامه مطالعات فرهنگی و ارتباطات. ۱(۲-۳). صص ۹۲-۷۳. قابل بازیابی از: <https://www.sid.ir/fa/journal/ViewPaper.aspx?id=54311>

رضوی، محمد. (۱۳۸۷). پیشگیری انتظامی از جرایم سایبری. مجموعه مقالات نخستین همایش ملی پیشگیری از جرم. تهران: مرکز تحقیقات کاربردی پلیس پیشگیری نیروی انتظامی.

رضوی، محمد. (۱۳۸۷). پیشگیری انتظامی از جرائم سایبری. زیرنظر محمد فرجی‌هاو غلامرضا محمدنسل. در: پیشگیری انتظامی از جرم (مجموعه مقالات نخستین همایش ملی پیشگیری از جرم). تهران: مرکز تحقیقات کاربردی پلیس پیشگیری نیروی انتظامی.

زیبر، اولریش. (۱۳۸۱). حرکت به سوی هزاره جدید مسئولیت در اینترنت. محمدحسن دزیانی، مترجم. خبرنامه انفورماتیک، شماره ۱۲۳.

صادقی فسائی، سهیلا و شهریار محمدی. (۱۳۸۷). نگاهی جرم‌شناسانه بر جرائم، امنیت و کنترل در اینترنت، در اینترنت و آسیب‌های اجتماعی. مسعود کوثری، ویراستار. تهران: نشر سلمان.

طارمی، محمدحسین. (۱۳۸۷). طبقه‌بندی و آسیب‌شناسی جرایم رایانه‌ای. مجله پگاه حوزه. شماره ۲۳۳، صص ۱۴-۲۴. قابل بازیابی از: <https://hawzah.net/fa/Magazine/View/3814/6256/68067>

عبداللهیان، حمید. (۱۳۸۴). نوع‌شناسی و بازتعریف آسیب‌های اینترنتی و تغییرات هویتی در ایران. ۱(۲-۳). صص ۱۵۴-۱۳۵. قابل بازیابی از: <https://www.sid.ir/fa/journal/ViewPaper.aspx?id=54318>

قانون مجازات اسلامی جمهوری اسلامی ایران. (۱۳۹۲).

وایت، راب و هینز، فیونا. (۱۳۹۲). جرم و جرم‌شناسی. سلیمی، ع، مترجم. تهران: پژوهشگاه حوزه و دانشگاه.

ولد، جورج برایان؛ برنارد، توماس و اسنیپس، جفری. (۱۳۹۴). جرم‌شناسی نظری. علی شجاعی، مترجم. چاپ دوم. تهران: انتشارات دادگستر.

Hollinger, Richard, C. (1992). Crime by Computer: Correlates of Software Piracy and Unauthorized Account Access. *Security Journal*, 2(1), pp 2-12.

Skinner F. William & Fream M. Anne. (1997). Social Learning Theory analysis of Computer Crime among College Students. *Journal of Research in Crime and Delinquency*, 34(4), pp 495-518. Retrieved from: <https://journals.sagepub.com/doi/10.1177/0022427897034004005>