فصلنامه رهیافت پیشگیری/ دورهٔ اول، شمارهٔ دوم، تابستان ۱۳۹۷
Prevention Approach Quarterly
Vol. 1, No.2, (Summer 2018)

تاریخ دریافت: ۱۳۹۷/۰۳/۱۹
تاریخ پذیرش: ۱۳۹۷/۰۴/۱۸

رابطه تعامل برون‌سازمانی با مدیریت پیشگیری از کلاهبرداری در فضای مجازی

ابراهیم داودی‌دهاقانی[۱] و علیرضا خمسه[۲]

چکیده

زمینه و هدف: استفاده روزافزون از رسانه‌های ارتباط‌جمعی مانند اینترنت در دنیای امروز باوجود پیامدهای مثبت و تأثیرگذار فراوان، دستاوردهای منفی بسیاری دارد. از جمله پیامدهای منفی، جرایم نوظهور رایانه‌ای و اینترنتی است که مقابله مؤثر با آن نیازمند تعامل برون‌سازمانی است. بنابراین هدف از پژوهش حاضر، تبیین رابطه تعامل برون‌سازمانی با مدیریت پیشگیری از کلاهبرداری در فضای مجازی است .

روش: پژوهش حاضر از نظر هدف کاربردی و از نظر روش جمع‌آوری داده‌ها از نوع پژوهش‌های توصیفی – تحلیلی است که به‌روش پیمایشی انجام شد. جامعه آماری پژوهش شامل فرماندهان ارشد انتظامی، روسای پلیس‌های تخصصی، کارکنان پلیس فتا، قضات و صاحب‌نظران قوه قضائیه و کارشناسان و صاحب‌نظران شرکت مخابرات، به تعداد ۵۰ نفر بود که باتوجه به محدودبودن جامعه آماری، از شیوه تمام‌شمار استفاده شد. داده‌های پژوهش با استفاده از پرسشنامه محقق‌ساخته، جمع‌آوری شد. روایی پرسشنامه به‌روش صوری تایید شد و پایایی کل آن نیز طریق محاسبه ضریب آلفای کرونباخ، ۷۹/. به دست آمد.

یافته‌ها: بین تعامل برون‌سازمانی رسمی با مدیریت پیشگیری از کلاهبرداری رایانه‌ای رابطه در حد متوسط رو به بالا وجود دارد؛ در این بخش، «تعامل با شرکت مخابرات برای نظارت رسمی بر فعالیت‌های کافی‌نت‌ها و مراکز تبادل اطلاعات»، در رتبه اول قرار دارد. همچنین بین تعامل برون‌سازمانی غیررسمی با مدیریت پیشگیری از کلاهبرداری رایانه‌ای رابطه در حد متوسط رو به بالا وجود دارد که در این بخش نیز «منع شیوع ابزارهای هک و تسهیل‌کننده شگردهای مجرمانه از طریق تعامل با اتحادیه فروشندگان محصولات فناوری اطلاعات» در رتبه اول قرار دارد.

نتایج: تعامل برون‌سازمانی غیررسمی اولویت بیشتری نسبت به تعامل برون‌سازمانی رسمی در پیشگیری از کلاهبرداری رایانه‌ای دارد، در تعامل برون‌سازمانی غیررسمی نیز تعامل با مخابرات در اولویت اول و تعامل با اتحادیه فروشندگان محصولات فناوری اطلاعات در اولویت بعدی قرار دارد.

کلیدواژه‌ها: تعامل برون‌سازمانی، تعامل برون‌سازمانی رسمی و غیررسمی، کلاهبرداری رایانه‌ای، فضای مجازی، مدیریت پیشگیری از جرم

❑ **استناد:** داودی دهاقانی، ابراهیم؛ خمسه، علیرضا (تابستان، ۱۳۹۷). رابطه تعامل برون‌سازمانی با مدیریت پیشگیری از کلاهبرداری در فضای مجازی. *فصلنامه رهیافت پیشگیری، ۱(۲)*، ۴۱-۶۰.

۱. استادیار مدیریت پیشگیری از جرم دانشگاه علوم انتظامی امین. (نویسنده مسئول). رایانامه:.davoodi57@chmail.ir
۲. کارشناسی ارشد فرماندهی و مدیریت انتظامی. . رایانامه:alikhamseh0304@gmail.com

مقدمه

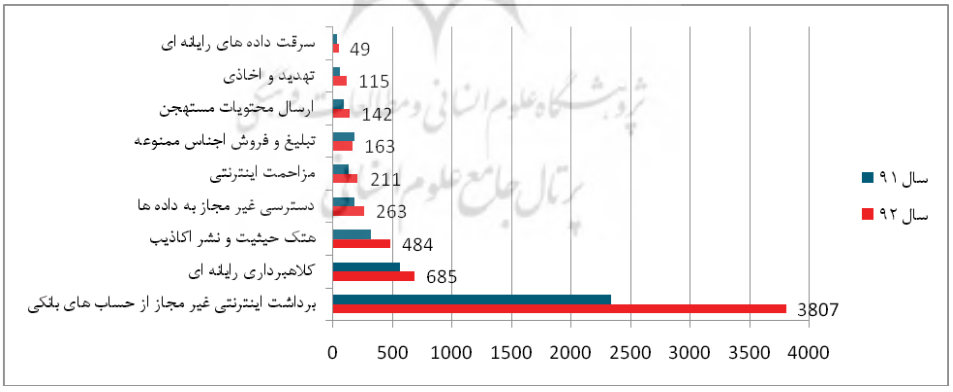
ظهور اینترنت، نمونه‌ای از تحولات فناوری ارتباطی و اطلاعاتی است که تغییرات عمیقی را در عرصه اقتصادی، فرهنگی و اجتماعی ایجاد کرده است. تا آنجا که حتی منشا تولید نظریات و مفاهیم جدید در حوزه‌های مختلف جامعه شناسی، روان‌شناسی، ارتباطات، اقتصاد و به‌طور کلی علوم انسانی شده است. اینترنت با تسهیل برقراری ارتباط میان دوردست‌ترین نقاط جهان، کره خاکی را تبدیل به دهکده‌ای کوچک کرده است؛ دهکده‌ای که ناخودآگاه نام مارشال مک لوهان را در ذهن تداعی می‌کند که سال‌ها پیش، از روزی سخن گفته بود که جهان به واسطه پیشرفت‌های فناوری ارتباطات، به دهکده‌ای کوچک تبدیل خواهد شد و مردم نه در کشورهای دوردست و با فاصله، که گویی در یک دهکده زندگی می‌کنند. وقتی صحبت از فضای مجازی به میان می‌آید مردم بیشتر به رایانه‌ای فکر می‌کنند که به اینترنت متصل است در حالی که این فقط بخش بسیار کوچکی از فضای مجازی را تشکیل می‌دهد. از نگاه دیوید بل[1] (۲۰۰۱) فضای مجازی فقط مجموعه‌ای از سخت‌افزار نیست بلکه مجموعه‌ای از تعاریف نمادین است که شبکه‌ای از عقاید و باورها را در قالب داد و ستد رد و بدل می‌کنند. فضای مجازی در واقع نامی است که تعداد زیادی از کاربردهای امروز فناوری‌های جدید ارتباطی را دربر می‌گیرد. این نام نخستین بار به‌وسیله ویلیام گیبسون در رمان نورومانسر ابداع شد. گیبسون، فضای مجازی را؛ مکان تجسم‌های همراه با رضامندی معرفی می‌کند که در آن هر دو بعد فیزیکی و ذهنی خود، دچار تحول و دگرگونی می‌شوند. در واقع، جسم فیزیکی در واقعیت مجازی و فضای سایبر، فاقد ارزش است و طراحی خود، در دنیای مجازی به تقلیل پیش بینی پذیری و اعمال کنترل بر هویت می‌انجامد. در فضای مجازی، متون تایپ شده بر صفحه رایانه، همچون ماسک عمل می‌کنند و این تغییر قیافه متنی، می‌تواند عامل لذت و هیجان و روشی برای کسب تجربه باشد (عباسی قادی و خلیلی کاشانی، ۱۳۹۰، ص ۵۸).

استفاده روزافزون از فناوری‌های اطلاعات مانند رایانامه و اینترنت شرایط لازم را برای انواع جرایم سازمان‌یافته و غیرسازمان‌یافته اینترنتی فراهم کرده است. روزانه هزاران نفر در جهان قربانی جرایم سایبری هستند و آگاهی چندانی نیز از انواع جرایم و نحوه وقوع آن‌ها ندارند (کاستلز[2]، ۲۰۱۱ و

1. Bell
2. Castells

داگلاس[1]، ۲۰۰۲). اولین پژوهشات پیرامون جرایم رایانه‌ای در آمریکا انجام شد که در این پژوهش‌ها به قضیه کلاهبرداری از طریق سوء استفاده از ۵۶ هزار مورد بیمه به ارزش حدوداً ۳۰ میلیون دلار اشاره شد. در دهۀ ۱۹۹۰ که شبکه جهانی اینترنت فراگیر شد جرایم رایانه‌ای از جنبه اقتصادی وسیع‌تر شده و ابعاد جدیدتری به خود گرفت. پژوهش‌های انجام شده نشان می‌دهد که بین سال‌های ۲۰۱۳ تا ۲۰۱۵، تقریباً ۴/۲ میلیون کاربر رایانه در آمریکا به‌وسیله فیشینگ زیان‌دیده شده‌اند (مندی[2]، ۲۰۰۱).

در سال‌های اخیر با پدیده‌ای به نام کلاهبرداری اینترنتی روبه‌رو هستیم که ضرورت تلاش برای حفظ امنیت داده‌ها و اطلاعات در این فضا را بیش از پیش نمایان می‌کند؛ ازطرفی شناسایی و دستگیری مجرمان فضای مجازی با توجه به گمنامی استفاده‌کنندگان این فضا بسیار مشکل و پیچیده است. در سه سال گذشته براساس آمارهای موجود ۵۰۰ فقره کلاهبرداری رایانه‌ای با مبالغ بالای ۳۰ میلیون تومان علیه تجار ایرانی رخ داده است و مجموع مبلغ کلاهبرداری شده در سال ۱۳۹۵ بالغ بر شصت میلیارد تومان بود و باعث شد بسیاری از تجار به‌همین دلیل ورشکست شوند و آسیب زیادی به حوزه اقتصادی کشور وارد شود (علایی، ۱۳۹۵). براساس آمار جرایم در سال‌های ۹۱ و ۹۲ از میان ۵۴ عنوان کد جرم، جرایم «برداشت اینترنتی غیرمجاز از حساب‌های بانکی» و «کلاهبرداری رایانه‌ای» بالاترین میزان وقوع جرم را دارا بوده‌اند.



نمودار ۱. وضعیت جرایم مالی و کلاهبرداری مجازی در کشور در مقایسه با جرایم شایع دیگر

1. Douglas
2. Mandy

بنابراین پیشگیری از وقوع جرم در این فضا امری اجتناب‌ناپذیر است و از راهبردهای مهم در برقراری نظم و امنیت پایدار در این حوزه است. در حال حاضر آمار این‌گونه از جرایم به‌شدت رو به افزایش است؛ در یک وضعیت مطلوب کلیه دستگاه‌های فرهنگی و انتظامی باید با مدیریت صحیح، از وقوع این جرایم پیشگیری کنند اما آیا می‌توان با روش‌های سنتی پیشین از جرایم نوین پیشگیری کرد؟ مسلماً جواب منفی است. جرایم نوین روش‌های پیشگیرانه نوین را طلب می‌کنند اما در موضوع جرایم فضای مجازی که از ویژگی‌های عمده مرتکبان جرایم در این فضا گمنامی و ناشناخته بودن مجرم است چه شیوه‌ای باید برای مقابله برگزید؟ چگونه باید اقدامات پیشگیرانه انجام داد؟ اینجاست که باید از ظرفیت تمام سازمان‌های دولتی و غیردولتی در امر پیشگیری از جرایم فضای مجازی استفاده کرد. به این منظور، مدیریت نحوه تعامل و ایجاد اجماع میان سازمان‌های کنشگر از راه گفتگو با تمام سازمان‌های رسمی و به‌ویژه غیررسمی، می‌تواند به ایجاد تفاهم و تعامل سازمانی مناسب برای اجرای طرح‌ها و مداخله‌های پیشگیرانه کمک کند (جلالی فراهانی، ۱۳۹۳، ص ۴). با توجه به اینکه پیشگیری از جرم در فضای مجازی نیازمند تعامل‌های بسیار گسترده‌ای با سازمان‌ها است در قانون برخی از سازمان‌ها و نهادها موظف به همکاری با نهادهای انتظامی و قضایی هستند، باشند بنابراین تعاملات براساس رسمی (با سازمان‌ها و نهادهایی که در قانون ارتباط دو سویه برای آنان تعریف شده) و غیررسمی (با سازمان‌ها و نهادهایی که در قانون ارتباط دوسویه برای آنان تعریف نشده) تقسیم شده است. براین اساس، تبیین رابطه تعامل برون‌سازمانی اعم از رسمی و غیر رسمی با مدیریت پیشگیری از جرایم کلاهبرداری رایانه‌ای و اولویت‌بندی آن، دغدغه اصلی پژوهش حاضر است. بنابراین پرسش اصلی پژوهش حاضر این است که تعامل برون‌سازمانی با مدیریت پیشگیری از جرایم کلاهبرداری رایانه‌ای چه رابطه‌ای دارد؟

تعامل: برای ارتباط و فراهم آوردن امکان آموزش، گفتگو و متقاعدسازی با نهادهای گوناگون، اساسی‌ترین عامل و ضروری‌ترین عنصر ارتباط است. بدیهی است تعامل مبتنی بر ارتباط دوسویه، اعتماد و احترام متقابل است (هیوز، ۱۳۸۰، ص ۱۱۷). تعامل بستر لازم برای ارتباط، اعتماد و همکاری برای پیش‌بردن برنامه‌های کاهش جرم و آسیب‌های اجتماعی است. در حقیقت مفهوم تعامل اجتماعی به‌دلیل قرابت تحلیلی و مفهومی با مفاهیم کنش، مبادله کنش متقابل ارتباط

و تحت تأثیر مفاهیم مشارکت اجتماعی، اعتماد اجتماعی و سرمایه اجتماعی در لحظه اول دو پهلو و مبهم به‌نظر می‌رسد و شاید همین موضوع موجب شکل‌گیری نظریه‌ها و الگوهای گوناگون تعامل‌های اجتماعی در حوزه جامعه‌شناسی و روان‌شناسی شده است (رجبی‌پور، ۱۳۸۷، ص ۱۴۹). در فرهنگ نامه دهخدا تعامل به معنی «با یکدیگر داد و ستد کردن» آمده است؛ در دایره المعارف علوم اجتماعی، تعامل یعنی «عمل متقابل دو یا چند موجود زنده با یکدیگر» (ساروخانی، ۱۳۹۰، ص ۳۶۴). تعامل دارای انواع مختلفی است که عبارت‌اند از:

۱- تعامل مودت‌آمیز: زمانی است که دو موجود (فرد یا گروه) درجهتی یگانه و با هدفی مشترک عمل کنند، نظیر تعاون؛

۲- تعامل دوری: بدین معنی که پدیده اول بر پدیده دوم اثر می‌گذارد، ولی خود نیز از آن تأثیر می‌گیرد. به‌عنوان مثال، هنگامی که فقر بر بی‌سوادی اثر می‌نهد یعنی میزان آن را افزایش می‌دهد، خود نیز از آن اثر می‌پذیرد، زیرا خود بی‌سوادی نیز فقر را تشدید می‌کند و از این طریق دوری بسته پدید می‌آید؛

۳- تعامل تفرقه‌آمیز: زمانی است که دو موجود در دو جهت جداگانه عمل کنند و کار آنان مکمل یکدیگر نباشد، مانند خصومت یا تقابل؛

۴- تعامل محیط‌شناختی: تعامل و همکاری آمیخته با رقابت و حتی همکاری آمیخته با خصومت بین افراد یا گروه‌هایی است که در یک محیط جغرافیایی با هم زندگی می‌کنند و در برابر فرصت‌ها، مواهب و مسائل مشخص قرار دارند؛

۵- تعامل کانونی: کنش و یا واکنش دو یا چند نفر به منظور پیگیری هدفی خاص؛

۶- تعامل چندگانه: کنش متقابل بین دو یا چند نفر در زمینه‌های گوناگون؛

۷- تعامل تأثیرگذار: کنش و واکنشی که در جریان آن نخست هر دو طرف (فرد یا گروه) تأثیرپذیرند و دوم تأثیر حاصل متضمن دگرگونی نسبی عمیق شود (ساروخانی، ۱۳۹۰، ص ۳۶۶).

۸- تعامل حسابگرانه: به معنای آن است که در آغاز افراد واکنش طرف مقابل خود را درنظر بگیرند و آن‌گاه دست به عمل بزنند. در برابر تعامل غیرحسابگرانه.

۹- تعامل نمادی: فرایند تعامل بین انسان‌ها با استفاده از نمادها (مانند زبان) است.

۱۰-تعامل غیرکانونی: افرادی جمع شده‌اند، ولی هدف معین جمعی ندارند و حتی در مواردی یکدیگر را نمی‌شناسند. به‌گفته گافمن در این شرایط نیز نحوه عمل خود به جهت وجود جمع تغییر می‌کند و این دگرگونی بصورت زنجیره‌ای به عمل دیگران نیز مؤثر می‌افتد و تعامل صورت می‌گیرد (دعاگویان، ۱۳۸۴، ص ۱۴).

پیشگیری از جرم: جرم تهدیدی علیه امنیت و اعتماد اجتماعی است (نیازی، کارکنان نصرآبادی و عشایری، ۱۳۹۵). علل بروز نابهنجاری اجتماعی در جامعه، انزوای مشارکت مردمی و کناره‌گیری سازوکارهای سنتی پیشگیری از جرم است (عشایری، عباسی، نطقی‌کاشانی و پیرحیاتی، ۱۳۹۴). به‌طورکلی جامعه به دو صورت پیشگیری و سرکوبی از خود در برابر بزهکاری واکنش نشان می‌دهد. لزوم اجرایی‌کردن بند ۵ اصل ۱۵۶ قانون اساسی، افزایش نرخ جرم، کاهش روزانهٔ فضای زندان‌ها و مجازات‌محور بودن محاکم کیفری، از جمله مواردی است که هزینهٔ جرم را تا اندازه‌ای با تورم روبرو کرده و صِرف مجازات، راهکار مناسبی برای مقابله با جرم نیست و به همین دلیل بیشتر صاحب‌نظران پیشگیری از جرم را پیشنهاد می کنند. ناکارآمدی روش‌های سرکوبگرانه در کنترل و مهار جرم و بی‌نظمی موجب اتخاذ تدابیر پیشگیرانه به جای روش‌های سرکوبگرانه شده است (ابراهیم‌زاده، ۱۳۹۵، ص ۲۱). پیشگیری از جرم، یعنی پیش‌بینی، شناسایی و ارزیابی خطر وقوع جرم و اتخاذ تدابیر و اقدام‌های لازم برای از میان بردن یا کاهش جرم است (شایگان، ۱۳۸۹، ص ۱۰۰). گاهی هدف پیشگیری را کاهش فرصت جرم (بیابانی، ۱۳۹۲) و گاهی کاهش انگیزه ارتکاب جرم و استفاده از عدالت کیفری می‌دانند (اسمعیلی و کسمایی پور، ۱۳۹۰، ص ۱۱۱). راهبرد اصلی پیشگیری از جرم، نظام برنامه‌ریزی است (اشنایدر و کیچین، ۱۳۸۷، ص ۷۳). در نهایت اصول پیشگیری ۱- شناسایی مسئله جرم و قانون‌گذاری، ۲- آسیب‌شناسی علل جرم و ۳- انتخاب اقدامات ویژه و ارائه راحل‌های عملیاتی و کاربردی است (بیابانی، ۱۳۹۲، ص ۱۳). پیشگیری به پیشگیری اولیه، ثانویه و ثالث دسته‌بندی می‌شوند (جزینی، ۱۳۹۱، ص ۱۸۴). هدف اصلی پیشگیری، کاهش احتمال وقوع بزهکاری و انحراف است (محمدنسل، ۱۳۸۷، ص ۳۶). هدف اصلی پیشگیری اولیه، آگاه ساختن محیط و اجتماعات عمومی نسبت به جرم، هدف پیشگیری ثانویه، اقدام برای افراد در معرض خطر بزهکاری و هدف پیشگیری ثانویه، تمرکز بر رخداد جرم، باز اصلاح بزه‌دیده و مجرمان است (براری، ۱۳۹۳، ص ۴۸).

مدیریت پیشگیری از جرم: منظور از مدیریت در علوم اداری و اقتصاد، فرآیند به کارگیری مؤثر و کارآمد منابع مادی و انسانی توأم با برنامه‌ریزی، سازماندهی، بسیج امکانات، هدایت و کنترل است که برای دستیابی به هدف‌های سازمانی صورت می‌گیرد. از این منظر، اصول مدیریت به این شرح است: ۱- برنامه‌ریزی، ۲- سازماندهی، ۳- بسیج امکانات و منابع، ۴- هدایت و سرپرستی و ۵- نظارت و کنترل. الوانی (۱۳۸۵) در مورد مدیریت می‌نویسد: شاید یکی از مهم‌ترین فعالیت‌ها در زندگی اجتماعی بشر امروز را بتوان مدیریت دانست. در عصر حاضر به مدد این فعالیت است که مأموریت‌ها و اهداف سازمان‌ها تحقق می‌یابند، از منابع و امکانات موجود بهره‌برداری می‌شود و توانایی و استعداد انسان‌ها از قوه به فعل در می‌آید. مدیریت فرایند به کارگیری مؤثر و کارآمد منابع مادی و انسانی در برنامه‌ریزی، سازماندهی، بسیج منابع و امکانات، هدایت و کنترل است که برای دستیابی به اهداف سازمانی و بر اساس نظام ارزشی مورد قبول صورت می‌گیرد. تاریخ پیشگیری جمعی از بزهکاری تا مدت‌های زیاد، فقط با تدابیر و اقدام‌های خاص، متفرقه و فاقد هرگونه هماهنگی همراه بود. لیکن از حدود چند دهه قبل، ضرورت تأسیس یک سازمان مرکزی در سطح ملی جهت ایجاد هماهنگی، تعریف و تدوین سیاست ملی پیشگیری از بزهکاری و نیز ارتقای کیفیت اقدام‌های پیشگیرانه به طور جدی احساس می‌شد. در پاسخ به این ضرورت، سازمان‌های رسمی پیشگیری از بزهکاری از طرف دولت‌ها و در جهت ایجاد هماهنگی و برنامه ریزی در این قلمرو به تدریج تأسیس و آغاز به کار نمودند. در واقع این گذر از سطح برنامه‌های محدود و متفرقه به سمت پیشگیری برنامه‌محور و در سطح ملی که در پاسخ به ضرورت مبارزه مؤثرتر با بزهکاری در حال گسترش صورت می‌گرفت، منجر به پیدایش مدیریت پیشگیری از جرم شد. این تغییر و تحول، با تغییر ایدئولوژی دولت‌ها سرعت بیشتری به خود گرفته است (نجفی‌ابرندآبادی، ۱۳۷۶).

کلاهبرداری در فضای مجازی: جرایم رایانه‌ای[1] یکی از پیش‌رونده‌ترین جرائمی است که با سرعت زیاد در حال پیشرفت است. این در حالی است که همگام با پیشرفت‌های علمی بویژه در زمینه رایانه و اینترنت، عده‌ای برخلاف خدمتگزاران بشریت که به فکر استفاده‌های مثبت از فناوری‌ها

1. CyberCrime

هستند به فکر سوء استفاده‌اند. فضای مجازی با ویژگی‌های خاص آن از جمله ارتباط سریع و آسان بین افراد و دسترسی به‌عنوان منبع اطلاعات باعث پیشرفت‌های بزرگ در روابط اقتصادی، اجتماعی، سیاسی و فرهنگی حاکم بر افراد شده است. همانند دنیای فیزیکی و مادی، در این فضا نیز افرادی یافت می‌شوند که بنا به نیات و انگیزه‌ها و اهداف خاص سعی در بر هم زدن نظم این اجتماع مجازی دارند. فضای مجازی به‌دلیل امنیت ناکافی و طبیعت مجازی بودن فرصت مناسبی را در اختیار افراد مجرم قرار می‌دهد. جرائم در این فضا نیز گاهی متفاوت و خاص فضای مجازی هستند. در فضای مجازی کشف جرم و پیگیری مجرم، پیچیده‌تر از جرائم فضای فیزیکی است. مثلاً سرقت از بانک جرمی کاملاً مشهود و علائم فیزیکی مانند اثر انگشت، شهود و اسناد به دست آمده امکان تعقیب و بررسی را به‌وجود می‌آورند اما سارقی که یک کپی دیجیتال کامل از نرم‌افزاری تولید می‌کند و نرم‌افزار اصلی همان‌طور که بوده دقیقا باقی می‌ماند به راحتی قابل تشخیص و پیگیری نیست (خداقلی، ۱۳۸۶).

جرم کلاهبرداری را می‌توان اینگونه تعریف کرد: «کلاهبرداری عبارتست از بردن مال غیر، از طریق توسل توأم با سوءنیت به وسایل یا عملیات متقلبانه» (پریشان، ۱۳۹۱). کلاهبرداری اینترنتی جرمی است که با توسعه اینترنت و ارتباطات اینترنتی گسترش یافته است و منظور از کلاهبرداری اینترنتی هرگونه کلاهبرداری است که به وسیله برنامه‌های رایانه‌ای یا ارتباطات شبکه اینترنتی صورت می‌گیرد، از طریق سایت‌های وب، رایانامه یا اتاق‌های گفتگو[1]. در واقع کلاهبرداری اینترنتی به هر نوع طرح متقلبانه‌ای گفته می‌شود که یک یا چند بخش از اینترنت را به‌کار می‌گیرد تا درخواست‌های متقلبانه‌ای را به منظور انجام معاملات جعلی و بردن اموال، با قربانیان احتمالی مطرح می‌سازد. تحصیل مال غیر با استفاده متقلبانه از رایانه، کلاهبرداری رایانه‌ای، کلاهبرداری اینترنتی یا کلاهبرداری آن‌لاین گویند که اصطلاحات رایجی است و به حکم قانون می‌تواند از جرائم در حکم کلاهبرداری تلقی شود (بوربور، ۱۳۹۳، ص ۸۸).

کلاهبرداری مجازی انواع و شیوه‌های گوناگونی دارد. کلاهبرداری کارت اعتباری یا بانکی، کلاهبرداری املاک و مستغلات، قاچاق مواد مخدر، سرقت هویت، بازاریابی تقلبی، پولشویی و مانند

1. chat rooms

اینها، از جمله جرایم کلاهبرداری مجازی هستند. کلاهبرداران مجازی با رخنه و دستکاری به سهام بورس نشان داده‌اند که توانمند شده و انگیزه مجرمانه آنها پیچیده‌تر شده است. برخی دیگر از مجرمان در تلاش برای نقدکردن حساب‌هایی هستند که قبلاً مشخصات حساب بانکی آنها سرقت شده است. ابزارهای اسب تروا، فیشینگ، فارمینگ در حال تکامل خود هستند و به شیوه‌های جدیدی ارتقا یافته‌اند. جرایم کلاهبرداری مجازی با به دست گرفتن علم و تخصص و تشکیل سازمان‌های زیرزمینی تهدید جهانی برای شرکت‌های بزرگ محسوب می‌شوند (رابسون[1]، ۲۰۱۲).

علایی (۱۳۹۵) در پژوهش خود باعنوان «عوامل مؤثر در پیشگیری از کلاهبرداری اینترنتی» که جامعه آماری آن کارکنان و کارشناسان حوزه پیشگیری از کلاهبرداری اینترنتی نیروی انتظامی به تعداد ۴۵ نفر بود به این نتایج رسید که از نظر کاربران فضای مجازی به‌ترتیب استفاده از پروسه‌های احراز هویت بیشترین تأثیر و افزایش سطح آگاهی و آموزش کاربران در اولویت دوم و استفاده از ابزارهای امنیتی در رتبه سوم عوامل پیشگیرانه در جرایم کلاهبرداری اینترنتی را دارند و از نظر نخبگان و صاحب‌نظران این حوزه بیشترین تأثیر را آموزش و افزایش سطح آگاهی کاربران داشته و استفاده از ابزارهای امنیتی در اولویت دوم و همچنین استفاده از پروسه‌های احراز هویت در رتبه سوم اهمیت قرار دارد. رنجبر (۱۳۹۲) در پژوهشی باعنوان «نقش سازمان‌های مردم‌نهاد در مدیریت پیشگیری از وقوع جرم» که جامعه آماری آن شامل کلیه کارکنان و کارشناسان حوزه مدیریت پیشگیری از جرم به تعداد ۱۳۸ نفر بود به این نتایج رسید که هم عوامل درون‌سازمانی و هم عوامل برون‌سازمانی بر مشارکت سازمان‌های مردم‌نهاد تأثیرگذار است. در این راستا به‌ترتیب، متغیرهای اعتماد اجتماعی، کیفیت اقدامات پلیس، مقوله جامعه‌محوری پلیس، امکانات نوین پلیس، نوع اطلاعات و آگاهی از سمن‌ها باعث مشارکت بیشتر سمن‌ها با پلیس می‌شود. میشل[2] (۲۰۰۹) در پژوهشی باعنوان «کلاهبرداری اینترنتی از زنان» به این نتایج دست یافت که درصورت کنترل و نظارت ناکافی از سوی دستگاه‌های بازدارنده، فضای مجازی بستر مستعدی برای کلاهبرداری از زنان خواهد بود. این پژوهش نشان داد آموزش‌های همگانی و تعامل پلیس

1. Robson
2. Michelle

با شهروندان تأثیر بسزایی در مقابله با کلاهبرداری اینترنتی خواهد داشت. لارسن[1](۲۰۱۲) در پژوهش خود باعنوان «پیشگیری اجتماعی از جرایم فضای سایبر» به این نتیجه دست یافت که مقابله مؤثر با جرایم فضای مجازی باید به‌صورت اجتماعی باشد و لازمه این امر هم ارتقاء سرمایه اجتماعی است؛ نتیجه مهم این پژوهش، تأکید بر امر اعتماد بین نیروهای اجرایی دولت و شهروندان است که درصورت ارتقاء این مهم، پیشگیری اجتماعی به‌نحو مؤثری امکان‌پذیر خواهد بود. هافمن و دیگران[2] (۲۰۱۴) در پژوهش خود باعنوان «کلاهبرداری اینترنتی: بحران غرب» به‌این نتایج دست یافت که جوامع غرب در عبور از مدرنیته به پست مدرن، برخی جرایم بیش از جرایم دیگر به‌وقوع می‌پیوندد؛ نتایج این پژوهش نشان داد کلاهبرداری اینترنتی در بین بقیه جرایم مطرح شده در صدر فهرست قرار دارد، در پیشنهادهای این پژوهش آمده برای مقابله با این جرم باید یک تعامل همه‌جانبه فراملی صورت پذیرد تا بتوان با وضع قوانین و مقررات جهانی و تعیین الزامات بین‌المللی با این جرم مقابله کرد.

روش‌شناسی

پژوهش حاضر از نظر هدف کاربردی و از نظر روش جمع‌آوری داده‌ها از نوع پژوهش‌های توصیفی – تحلیلی است که به‌روش پیمایشی انجام شد. جامعه آماری پژوهش شامل فرماندهان ارشد انتظامی، روسای پلیس‌های تخصصی، کارکنان پلیس فتا، قضات و صاحب‌نظران قوه قضائیه و کارشناسان و صاحب‌نظران شرکت مخابرات، به تعداد ۵۰ نفر بود که باتوجه به محدود بودن جامعه آماری، از شیوه تمام‌شمار استفاده شد. داده‌های پژوهش با استفاده از پرسشنامه محقق‌ساخته، جمع‌آوری شد. روایی پرسشنامه به‌روش صوری تایید شد و پایایی کل آن نیز طریق محاسبه ضریب آلفای کرونباخ، ۷۹/. به دست آمد. جدول ضرایب آلفای کرونباخ مؤلفه‌ها به‌شرح جدول ۱ است.

1. Larsen
2. Hoffman and others

جدول ۱. نتایج محاسبه پایایی پرسشنامه

ردیف	عنوان مؤلفه	ضریب آلفای کرونباخ	نتیجه
۱	تعامل برون‌سازمانی رسمی	/۷۷	پایایی در حد مطلوب
۲	تعامل برون‌سازمانی غیررسمی	/۸۱	پایایی در حد مطلوب
۳	آلفای کل	/۷۹	پایایی در حد مطلوب

یافته‌ها

یافته‌های توصیفی: ویژگی‌های جمعیت‌شناختی جامعه مورد مطالعه به‌شرح جدول ۲ است.

جدول ۲. توصیف جمعیت نمونه

ردیف	متغیر	طبقه	فراوانی	درصد	درصد فراوانی تجمعی
۱	سن	کمتر از۲۵ سال	۱۶	۱۴/۵	۱۴/۵
		۲۶ تا ۳۵ سال	۳۷	۳۳/۶	۴۸/۲
		۳۶ تا ۴۵ سال	۴۱	۳۷/۳	۸۵/۵
		۴۶ تا ۵۵ سال	۱۲	۱۰/۹	۹۶/۴
		۵۶ سال و بالاتر	۴	۳/۶	۱۰۰
۲	وضعیت تاهل	مجرد	۱۴	۱۲/۷	۱۲/۷
		متاهل	۹۶	۸۷/۳	۱۰۰
۳	تحصیلات	فوق دیپلم	۱۰	۹/۱	۹/۱
		کارشناسی	۶۷	۶۰/۹	۷۰
		کارشناسی ارشد	۲۷	۲۴/۵	۹۴/۵
		دکتری	۶	۵/۵	۱۰۰
۵	سابقه	کمتر از ۵ سال	۵	۴/۵	۴/۵
		۶ تا ۱۰ سال	۲۳	۲۰/۹	۲۵/۵
		۱۱ تا ۱۵ سال	۵۳	۴۸/۲	۷۳/۶
		۱۶ سال و بالاتر	۲۹	۲۶/۴	۱۰۰
۶	محل خدمت	ستادی	۴۴	۴۰	۴۰
		اجرایی	۶۶	۶۰	۱۰۰

نتایج توصیفی نشان می‌دهد، ۱۴/۵ درصد پاسخ دهندگان دارای سن کمتر از ۲۵ سال، ۳۳/۶ درصد دارای سن ۲۶ تا ۳۵ سال، ۳۷/۳ درصد دارای سن ۳۶ تا ۴۵ سال و ۱۰/۹ درصد نیز دارای سن ۵۶ سال و بالاتر هستند. در بررسی وضعیت تاهل مشخص می‌شود ۸۷/۳ درصد متاهل

و ۱۲/۷ درصد نیز مجرد هستند. ۹/۱ درصد دارای تحصیلات فوق دیپلم، ۶۰/۹ درصد دارای تحصیلات کارشناسی، ۲۴/۵ درصد دارای تحصیلات کارشناسی ارشد و ۵/۵ درصد نیز دارای تحصیلات دکتری هستند. ۴/۵ درصد دارای سابقه کمتر از ۵ سال، ۲۰/۹ درصد دارای سابقه ۶ تا ۱۰ سال، ۴۸/۲ درصد دارای سابقه ۱۱ تا ۱۵ سال و ۲۶/۴ درصد نیز دارای سابقه ۱۶ سال و بالاتر هستند. ۶۰ درصد در امور اجرایی و ۴۰ درصد نیز در امور ستادی به‌کارگیری می‌شوند.

یافته‌های استنباطی

بررسی نرمال بودن و تصادفی بودن توزیع داده‌ها: برای بررسی نرمال بودن توزیع داده‌ها از آزمون کولوموگروف اسمیرنوف استفاده شد که با توجه به مقدار آمار کولوموگروف که ۲/۲۳ و ۹/۵۲ بود و سطح معناداری که ۰/۵۵۱ و ۰/۶۳۶ است می‌توان با اطمینان ۹۵ درصد بیان کرد توزیع داده‌ها نرمال است.

جدول ۳. بررسی نرمال بودن و تصادفی بودن توزیع داده‌ها

ردیف	عنوان شاخص	نرمال بودن		تصادفی بودن		نتیجه
		مقدار آماره کلوموگروف	سطح معناداری	مقدار آزمون ران تست	سطح معناداری	
۱	تعامل برون‌سازمانی رسمی	۲/۲۳	/۵۵۱	۱۱/۰۳	/۰۰۱	نرمال و تصادفی
۲	تعامل برون‌سازمانی غیررسمی	۹/۵۲	/۶۳۶	۹/۷۴	/۰۰۵	نرمال و تصادفی

در بخش تصادفی بودن توزیع داده‌ها با عنایت به‌اینکه مقدار آماره ران تست، ۱۱/۰۳ و ۹/۷۴ بوده و سطح معناداری که ۰/۰۰۱ و ۰/۰۰۵ است. می‌توان با اطمینان ۹۵ درصد بیان کرد توزیع داده‌ها تصادفی است.

بررسی پرسش اصلی پژوهش: رابطه تعامل برون‌سازمانی پلیس با مدیریت پیشگیری از کلاهبرداری رایانه‌ای چگونه است؟

جدول ۴. بررسی پرسش اصلی پژوهش

ردیف	عنوان شاخص	مقدار آزمون تی	درجه آزادی	نمره مبنا	سطح معناداری
۱	تعامل برون‌سازمانی پلیس	۳۱/۶۶	۰/۰۰۰	۳/۲۵ از ۵	۰/۰۰۰

با توجه به مقدار آزمون تی استیودنت که ۳۱/۶۶ و سطح معناداری که ۰/۰۰۰ است، می‌توان با اطمینان ۹۵ درصد بیان کرد بین تعامل برون‌سازمانی با مدیریت پیشگیری از کلاهبرداری رایانه‌ای رابطه در حد متوسط رو به بالا وجود دارد و این بدان معناست که تعامل برون‌سازمانی سبب پیشگیری مطلوب‌تر از کلاهبرداری رایانه‌ای خواهد شد.

بررسی پرسش فرعی اول: رابطه تعامل برون‌سازمانی رسمی پلیس با مدیریت پیشگیری از کلاهبرداری رایانه‌ای چگونه است؟ با توجه به مقدار آزمون تی استیودنت که ۳۱/۸۰ و سطح معناداری که ۰/۰۰۰ است می‌توان با اطمینان ۹۵ درصد بیان کرد بین تعامل برون‌سازمانی رسمی با مدیریت پیشگیری از کلاهبرداری رایانه‌ای رابطه در حد متوسط رو به بالا وجود دارد و این بدان معناست که تعامل برون‌سازمانی رسمی سبب پیشگیری مطلوب‌تر از کلاهبرداری رایانه‌ای خواهد شد.

جدول ۵. بررسی پرسش فرعی اول

ردیف	عنوان شاخص	مقدار آزمون تی	درجه آزادی	نمره مبنا	سطح معناداری
۱	تعامل برون‌سازمانی رسمی	۳۱/۸۰	۰/۰۰۰	۳/۲۵	۰/۰۰۰

رتبه‌بندی شاخص‌های تعامل برون‌سازمانی رسمی: در بررسی توصیفی شاخص‌های مربوط به تعامل برون‌سازمانی رسمی مشخص شد شاخص «تعامل با شرکت مخابرات برای نظارت رسمی بر فعالیت‌های کافی نت‌ها و مراکز تبادل اطلاعات» با میانگین ۳/۸۰ در رتبه اول، شاخص «ایجاد محدودیت در خرید و فروش تجهیزات سخت‌افزاری تسهیل‌کننده ارتکاب جرم مانند رایانه‌های با توان پردازش بالا، دستگاه‌های اسکیمینگ، شنود اطلاعات مخابراتی و اینترنتی بی‌سیم و باسیم، ثبت‌کننده کلید سخت‌افزاری از طریق تعامل با اتحادیه عرضه و فروش محصولات دیجیتال» با میانگین ۳/۶۷ در رتبه دوم و شاخص «جلوگیری از دسترسی غیرمجاز افراد به منابع اطلاعاتی است با مشارکت مخابرات» با میانگین ۳/۶۶ در رتبه سوم قرار دارد و شاخص‌های «الزام مؤسسه‌های مالی به استفاده از معیارهای امنیتی روز دنیا در سامانه‌های پرداخت اینترنتی از طریق تعامل با بانک مرکزی» و «راه‌اندازی سامانه هوشمند ردزنی حساب بانکی به منظور ردگیری سارقان حساب درصورت استفاده از حساب بانکی آنلاین» در رتبه‌های آخر قرار دارند.

بررسی پرسش فرعی دوم: رابطه تعامل برون‌سازمانی غیررسمی پلیس با مدیریت پیشگیری

از کلاهبرداری رایانه‌ای چگونه است؟ با توجه به مقدار آزمون تی استیودنت که ۲۱/۷۸ و سطح معناداری که ۰/۰۰۰ است می‌توان با اطمینان ۹۵ درصد بیان کرد بین تعامل برون‌سازمانی غیررسمی پلیس با مدیریت پیشگیری از کلاهبرداری رایانه‌ای رابطه در حد متوسط رو به بالا وجود دارد و این بدان معناست که تعامل برون‌سازمانی غیررسمی سبب پیشگیری مطلوب‌تر از کلاهبرداری رایانه‌ای خواهد شد.

جدول ۶. بررسی پرسش فرعی دوم

ردیف	عنوان شاخص	مقدارآزمون t	درجه آزادی	نمره مبنا	سطح معناداری
۱	تعامل برون‌سازمانی غیررسمی	۲۱/۷۸	۰/۰۰۰	۳	۰/۰۰۰

رتبه‌بندی شاخص‌های مربوط به مؤلفه تعامل برون‌سازمانی غیررسمی: در بررسی توصیفی شاخص‌های مربوط به تعامل برون‌سازمانی غیررسمی مشخص می‌شود شاخص «منع شیوع ابزارهای هک و تسهیل‌کننده شگردهای مجرمانه از طریق تعامل با اتحادیه فروشندگان محصولات فناوری اطلاعات» با میانگین ۴/۶۲ در رتبه اول، شاخص «ساماندهی وب‌گاه‌های داخلی به‌ویژه فروشگاه‌های اینترنتی و اعطای نماد اعتماد به وب‌گاه‌های دارای مجوز از طریق به‌کارگیری ظرفیت‌های وزارت صنعت معدن و تجارت و وزرات فرهنگ و ارشاد» با میانگین ۴/۰۵ در رتبه دوم و شاخص «تعامل با سازمان‌های مردم نهاد در خصوص برگزاری همایش‌ها و جلسات آگاه‌سازی برای شهروندان و فعالیت در فضای مجازی» با میانگین ۳/۸۷ در رتبه سوم قرار دارد و شاخص‌های «تعامل با شهرداری درخصوص نصب بیلبوردهای آگاه‌سازی درخصوص جرایم یادشده در فضای شهری» و «تحریک وجدان و آگاهی شهروندان درخصوص مقابله با کلاهبرداری در فضای مجازی از طریق آگاه‌سازی توسط رسانه ملی» و «استفاده از ظرفیت‌های مطبوعات و نشریات درخصوص آگاه‌سازی درخصوص شگردها و شیوه‌های مجرمان حوزه کلاهبرداری در فضای مجازی» در رتبه‌های آخر قرار دارند.

بررسی پرسش سوم: کدام تعامل از اهمیت و اولویت بیشتری برخوردار است؟ در بررسی اولویت بندی نوع تعامل از آزمون فریدمن استفاده شده است که با توجه به مقدار آزمون کای دو که ۳۰/۹۴ و سطح معناداری که ۰/۰۰۰ است می‌توان با اطمینان ۹۵ درصد بیان کرد اولویت بندی نوع تعامل

معتبر بوده و می‌توان به ضرایب فریدمن مراجعه نمود که نتایج نشان می‌دهد تعامل برون‌سازمانی غیررسمی با ضریب ۱/۷۶ در رتبه اول و تعامل برون‌سازمانی رسمی با ضریب ۱/۲۴ در رتبه دوم قرار دارد.

جدول ۷. بررسی پرسش فرعی سوم

ردیف	عنوان شاخص	ضریب فرید من	اولویت	مقدار آزمون کای دو	درجه آزادی
۱	تعامل برون‌سازمانی غیررسمی	۱/۷۶	۱	۳۰/۹۴	./۰۰۰
۲	تعامل برون‌سازمانی رسمی	۱/۲۴	۲		

بحث و نتیجه‌گیری

در بررسی پرسش اصلی مشخص شد، بین تعامل برون‌سازمانی پلیس با مدیریت پیشگیری از کلاهبرداری رایانه‌ای رابطه در حد متوسط رو به بالا وجود دارد و این بدان معناست که تعامل برون‌سازمانی سبب پیشگیری مطلوب‌تر از کلاهبرداری رایانه‌ای خواهد شد. در بررسی توصیفی گویه‌های مربوط به تعامل برون‌سازمانی رسمی مشخص شد که شاخص «تعامل با شرکت مخابرات برای نظارت رسمی بر فعالیت‌های کافی‌نت‌ها و مراکز تبادل اطلاعات» در رتبه اول، شاخص «ایجاد محدودیت در خرید و فروش تجهیزات سخت‌افزاری تسهیل‌کننده ارتکاب جرم مانند رایانه‌های با توان پردازش بالا، دستگاه‌های اسکیمینگ، شنود اطلاعات مخابراتی و اینترنت بی‌سیم و باسیم، ثبت‌کننده کلید سخت‌افزاری از طریق تعامل با اتحادیه عرضه و فروش محصولات دیجیتال»، در رتبه دوم و شاخص «جلوگیری از دسترسی غیرمجاز افراد به منابع اطلاعاتی با مشارکت مخابرات» در رتبه سوم قرار دارد. در بررسی توصیفی شاخص‌های مربوط به تعامل برون‌سازمانی غیررسمی مشخص شد که شاخص «منع شیوع ابزارهای هک و تسهیل‌کننده شگردهای مجرمانه از طریق تعامل با اتحادیه فروشندگان محصولات فناوری اطلاعات» در رتبه اول، شاخص «ساماندهی وب‌گاه‌های داخلی به‌ویژه فروشگاه‌های اینترنتی و اعطای نماد اعتماد به وب‌گاه‌های دارای مجوز از طریق به‌کارگیری ظرفیت‌های وزارت صنعت معدن و تجارت و وزرات فرهنگ و ارشاد» در رتبه دوم و شاخص «تعامل با سازمان‌های مردم‌نهاد درخصوص برگزاری همایش‌ها و جلسات آگاه‌سازی برای شهروندان و فعالیت در فضای مجازی» در رتبه سوم قرار دارد.

نتایج به دست آمده در این بخش هم سو با نتایج علایی (۱۳۹۵) است. نتایج حاصل از این پژوهش نشان می‌دهد از نظر کاربران فضای مجازی به ترتیب استفاده از پروسه‌های احراز هویت بیشترین تأثر و افزایش سطح آگاهی و آموزش کاربران در اولویت دوم و استفاده از ابزارهای امنیتی در رتبه سوم عوامل پیشگیرانه در جرایم کلاهبرداری اینترنتی را دارند و از نظر نخبگان و صاحب نظران این حوزه بیشترین تأثیر را از بین عوامل آموزش و افزایش سطح آگاهی کاربران داشته و استفاده از ابزارهای امنیتی در اولویت دوم و همچنین استفاده از پروسه‌های احراز هویت در رتبه سوم اهمیت قرار دارد. میشل (۲۰۰۹) نشان داد ارائه آموزش‌های همگانی و تعامل پلیس با شهروندان تأثیر بسزایی در مقابله با کلاهبرداری اینترنتی خواهد داشت. هافمن و دیگران (۲۰۱۴) دریافتند کلاهبرداری اینترنتی در بین بقیه جرایم مطرح شده در صدر فهرست قرار دارد در پیشنهادات این پژوهش آمده برای مقابله با این جرم باید یک تعامل همه‌جانبه فراملی صورت پذیرد تا بتوان با وضع قوانین و مقررات جهانی و تعیین الزامات بین‌المللی با این جرم مقابله کرد. جمع‌بندی مقایسه این بخش را می‌توان در دو مؤلفه مهم نظارت و آموزش خلاصه کرد. در بخش نظارت وظایف بسیاری بر عهده مخابرات بوده از جمله نظارت بر عملکرد کافی‌نت‌ها و آی‌پی‌های خانگی. در بخش نظارت بر کافی‌نت‌ها، مهمترین اصل، احراز هویت کاربران است که در نتایج پژوهشی که علایی (۱۳۹۵) انجام داده است نیز به آن اشاره شده است. در بخش نظارت نیز می‌توان گفت نظارت بر عملکرد مختص کافی‌نت نیست، در قدم دوم پیشگیری از خرید و فروش لوازم سخت‌افزاری تسهیل‌کننده ارتکاب جرم مانند رایانه‌های با توان پردازش بالا، دستگاه‌های اسکیمینگ، شنود اطلاعات مخابراتی و اینترنتی بی‌سیم و باسیم، ثبت‌کننده کلید سخت‌افزاری از طریق تعامل با اتحادیه عرضه و فروش محصولات دیجیتال، اقدامی ضروری است، در این بین وضع قوانین بازدارنده می‌تواند بسیار مهم و حیاتی باشد که هافمن (۲۰۱۴) نیز به آن اشاره کرده است. در نتیجه یافته‌های پژوهش حاضر در زمینه‌های دو مؤلفه نظارت و آموزش هم‌سو با نتایج پژوهش‌های علایی (۱۳۹۵)، میشل (۲۰۰۹) و هافمن (۲۰۱۴) است. در قسمت نظارت بحث اصلی مربوط به احراز هویت است که می‌تواند گام مهمی در پیشگیری در این حوزه محسوب شود. در قسمت آموزش مباحثی چون آگاه‌سازی و آموزش‌های همگانی می‌تواند بسیار تأثیرگذار باشد.

نتایج به دست آمده درخصوص تعامل برون‌سازمانی غیررسمی با نتایج به دست آمده از پژوهش گودرزی (۱۳۹۵) هم‌سو است؛ نتایج این پژوهش نشان داد بین اعتماد اجتماعی، مشارکت اجتماعی، انسجام اجتماعی و پیشگیری انتظامی از وقوع جرایم فضای مجازی رابطه معناداری وجود دارد که با یافته‌های پژوهش حاضر نیز هم‌سو است. رضایی (۱۳۹۴) در پژوهش خود دریافت جلب مشارکت مردمی، در کنار تعامل مستمر نیروی انتظامی در شاخص‌های یادشده پژوهش مورد اشاره می‌توان از ظرفیت سازمان‌های مردم‌نهاد در پیشگیری از آسیب‌های اجتماعی استفاده کرد و به امنیت مطلوب دست یافت، همچنین پاک‌شریفی (۱۳۸۹) نشان داد که تعامل پلیس با مدارس با اعتماد بین مسئولان مدارس برای پیشگیری از جرم ارتباط معنادار داشته و هم‌چنین متغیرهای آموزش مسئولان، استفاده از توانمندی مدارس توسط پلیس، اقدامات فرهنگی پلیس و استفاده از تجهیزات نوین ارتباطی بر مدیریت پیشگیری از جرم تأثیر مثبت دارد که این یافته‌ها با یافته‌های پژوهش حاضر هم‌سو است.

پیشنهادها:

- امن‌سازی مراکز پردازش و ذخیره اطلاعات مالی با شیوه‌های معیار از طریق ایجاد تعامل سازنده و مستمر با بانک‌ها و مؤسسه‌های مالی و اعتباری می‌تواند سبب پیشگیری مناسب از بروز جرایم فضای مجازی شود.
- یکی از سازمان‌هایی که می‌تواند نقش اساسی در امن‌سازی فضای مجازی ایفا کند، شرکت مخابرات است بنابراین تعامل برون‌سازمانی رسمی با مخابرات برای امن‌سازی زیرساخت‌های مخابراتی و اینترنتی از قبیل نقاط انتقال، سوئیچ‌ها، سرورها، شبکه‌های توزیع سیگنال می‌تواند سبب پیشگیری مناسب در این زمینه را فراهم سازد.
- استفاده از ظرفیت‌های علمی و تعاملی دانشگاه‌ها، پژوهشگاه‌ها و مراکز مطالعات راهبردی برای برگزاری جلسات هیئت اندیشه‌ورزی می‌تواند برای به‌روز رسانی‌های امنیتی مؤثر باشد.
- تعامل با رسانه ملی و سایر رسانه‌های جمعی درخصوص اطلاع‌رسانی به کاربران برای به‌کارگیری ابزارهای ضد فیشینگ بر روی مرورگرهای اینترنتی منجر به پیشگیری مناسب در زمینه کلاهبرداری در فضای مجازی خواهد شد.

- تعامل پلیس فتا با مخابرات و اتحادیه‌ها درخصوص ایجاد روش‌های شناسایی و کشف وب‌گاه‌های زیرزمینی و نظارت بر مراکز توزیع انبوه پیامک‌های تلفنی و اینترنتی و هماهنگی برای ایجاد محدودیت دسترسی به پهنای باند اینترنتی بالا و سرویس‌های اینترنتی حرفه‌ای به افراد ناشناس منجر به کاهش آسیب‌پذیری‌های فنی در این حوزه برای کاربران خواهد شد.
- تعامل با سایر سازمان‌ها نظیر وزارت اطلاعات و سپاه درخصوص نظارت بر مجرمان سابقه‌دار با ایجاد محدودیت در اتصال به فضای مجازی و انجام عملیات‌های نقل و انتقال مالی، پیشنهاد می‌شود.
- استفاده از تجارب علمی و عملی مراکز دانش بنیان درخصوص به‌کارگیری ربات‌های هوشمند در جمع‌آوری اخبار و تحلیل آنها، در پیشگیری از کلاهبرداری در فضای مجازی بسیار مؤثر است.

فهرست منابع

ابراهیم‌زاده، علی. (۱۳۹۵). تبیین برنامه‌ریزی مؤثر در مدیریت پیشگیری از جرم. *فصلنامه دانش انتظامی ایلام، ۵(۱۷)، صص ۲۷-۳۹.*

اسمعیلی، حبیبه و کسمایی‌پور، وحیده. (۱۳۹۰). بررسی عوامل امنیتی جرم و نقش آن‌ها در پیشگیری از جرم. *فصلنامه دانش انتظامی آذربایجان شرقی. ۱(۱)، صص ۱۰۳-۱۲۵.*

اشنایدر، ریچارد و کیچین، تد (۱۳۸۷). *برنامه‌ریزی شهری برای پیشگیری از جرم.* (فرزان سجودی، مترجم). تهران: نشر میزان.

براری، شهروز. (۱۳۹۳). نقش هدایت و کنترل در مدیریت پیشگیری انتظامی از جرایم (مورد مطالعه کوپ استان گیلان در سال ۱۳۹۱). *فصلنامه دانش انتظامی گیلان. ۳(۱۰)، صص ۳۱-۵۴.*

بوربور، مسعود. (۱۳۹۳)، *تبیین شیوه‌های مبتنی بر فناوری اطلاعات برای پیشگیری از کلاهبرداری‌های مالی موجود در فضای مجازی*، پایان نامه کارشناسی ارشد، دانشگاه علوم انتظامی امین.

بیابانی، غلامحسین. (۱۳۹۲). نقش رسانه در پیشگیری از جرم. *فصلنامه رسانه. ۲۴(۳)، صص ۳۳-۴۲.*

پریشان، جابر. (۱۳۹۱). *بررسی جرم کلاهبرداری رایانه‌ای.* سایت نشریه تخصصی حقوق ارتباطات دانشگاه علامه طباطبایی.

جزینی، علیرضا. (۱۳۹۱). *مدیریت ستادی پیشگیری از جرم.* تهران: انتشارات معاونت تربیت و آموزش نیروی انتظامی.

جلالی فراهانی، امیرحسین. (۱۳۹۳). پیشگیری از جرایم رایانه‌ای. *مجله حقوقی دادگستری. شماره ۴۷.*

خداقلی،زهرا. (۱۳۸۶). *جرائم رایانه‌ای.* چاپ اول. تهران: انتشارات آریان.

دعاگویان، داود. (۱۳۸۴). جنگ نرم شبکه‌های تلویزیونی ماهواره‌ای در عرصه ارتباطات بین‌الملل. *مطالعات عملیات روانی. شماره ۳۹.*

رجبی‌پور، محمود. (۱۳۸۳). درآمدی بر پیشگیری مقتدرانه پلیس از جرم. *فصلنامه دانش انتظامی، ۶(۲).*

ساروخانی، باقر. (۱۳۹۰). *روش‌های پژوهش در علوم اجتماعی*. تهران: انتشارات سروش.
شایگان، فریبا. (۱۳۸۹). رسانه و آموزش جرم (مطالعه موردی صفحه حوادث روزنامه جام جم سال ۱۳۸۸). *فصلنامه مطالعات امنیت اجتماعی، ۱(۲۴)*، صص ۹۱-۱۱۶.
عباسی قادی، مجتبی و خلیلی‌کاشانی، مرتضی. (۱۳۹۰). *تأثیر اینترنت بر هویت ملی*. تهران: پژوهشکده مطالعات راهبردی.
عشایری، طاها؛ عباسی، الهام؛ نطقی کاشانی، علیرضا و پیرحیاتی، نرگس. (۱۳۹۴). بررسی عوامل اجتماعی- فرهنگی مؤثر بر قانون‌گریزی شهروندان استان اردبیل. *فصلنامه پژوهش‌های دانش انتظامی. ۱۷(۶۹)*، صص ۱۷۱-۱۹۴.
علایی، محمدعلی. (۱۳۹۵). راهکارهای مقابله با جرم کلاهبرداری رایانه‌ای در حقوق کیفری ایران. *دیدگاه‌های حقوق قضایی. شماره ۴۲ و ۴۳*.
کمالی رنجبر، جلال. (۱۳۹۲). نقش سازمان‌های مردم‌نهاد در مدیریت پیشگیری از وقوع جرم. *فصلنامه دانش انتظامی هرمزگان. ۴(۷)*، صص ۳۹-۶۶.
محمدنسل. غلامرضا. (۱۳۸۷). *پلیس و سیاست پیشگیری از جرم* (مجموعه مقالات). تهران: مرکز تحقیقات کاربردی پلیس پیشگیری نیروی انتظامی.
نجفی‌ابرندآبادی، علی‌حسین. (۱۳۷۶). روابط میان پیشگیری وضعی و کنترل بزهکاری. *تحقیقات حقوقی، ۱۲(۱۹)*.
نیازی، محسن؛ کارکنان‌نصرآبادی، محمد و عشایری، طاها. (۱۳۹۵). *آسیب‌شناسی اجتماعی*. تهران: نشر سخنوران.
الوانی، مهدی. (۱۳۸۵). *مدیریت عمومی*. تهران: انتشارات نی.
هیوز، گوردون. (۱۳۸۰). *پیشگیری از جرم* (کنترل اجتماعی، ریسک و مدرنیته اخیر)، (علیرضا کلدی و محمدتقی جغتایی، مترجمان). تهران: انتشارات سازمان بهزیستی کشور.

Bell, D.; Kennedy, B. (2000). *The Cybercultures Reader*. London: Rutledge.
Castells. M. (2011). *Seeking after the truth in computer evidence any proof of ATM fraud*. oxford-journals.org.
Douglas, T. (2002). *Hacker Culture*. University of Minnesota Press.
Mandy, A. (2001). *CIW Security Professional*. Hungry Minds. p 638.
Robson، B. (2012). *Study on Cybercrime*, Steven Malby, United Nations.