ISSN: 2538-3787
http://www.Joce.ir

مجله علمی پژوهش در فقه و حقوق (سال دوم)
شماره ۴ / تابستان ۱۳۹۶ / ص ۱۲۷-۱۱۳

بررسی شیوه ها و راهکار های پیشگیری از جرایم اینترنتی از دیدگاه اساتید ارتباطات و فعالان حوزه فضای مجازی

علی گرانمایه پور [۱] ، فرزانه طاهرسلطانی [۲]

[۱] عضو هیات علمی گروه مطالعات فرهنگی و رسانه دانشگاه علوم و ارتباطات و مطالعات رسانه - دانشگاه آزاد اسلامی

[۲] دانشجو کارشناس ارشد علوم ارتباطات ، دانشگاه آزاد اسلامی واحد علوم و تحقیقات تهران

نام نویسنده مسئول:
فرزانه طاهرسلطانی

چکیده

ایـن پژوهش به منظور بررسی شیوه ها و راهکار های پیشگیری از جرایم اینترنتی از دیدگاه اساتید ارتباطات و فعالان حوزه فضای مجازی انجام گرفته است. در واقع این پژوهش به دنبال شناخت انواع جرایم اینترنتی و بررسی راهکارهایی برای پیشگیری از این جرایم می باشد. پژوهش حاضر به لحاظ روش، توصیفی ، به لحاظ اجرا ، پیمایشی و از نظر هدف کاربردی است. و جامعه آماری موردنظر، شامل ۳ گروه از متخصصان حوزه فضای مجازی است که شامل(اساتید علوم ارتباطات ، کارشناسان و خبرگان پلیس فتا در حوزه جرایم سایبر وفضای مجازی ؛ کارشناسان و فعالان حوزه اینترنت و فضای مجازی می باشند. که تعداد کل افراد جامعه، ۳۰۰ نفر هستند.و پس از استخراج پرسشنامه ها ، با استفاده از نرم افزار SPSS به توصیف و تبیین یافته ها پرداخته شد. نتایج پژوهش حاکی از آن است که خلاءهای قانونی اثر بیشتری نسبت به عوامل انسانی در افزایش جرائم اینترنتی دارند و بین جرائم اینترنتی و عدم وجود قوانین به روز و کارآمد رابطه وجود دارد. یافته های تحقیق نشان میدهد که هرچه آگاهی کاربران نسبت به حفظ امنیت خودشان در فضای مجازی کمتر باشد، این امر سبب افزایش جرائم اینترنتی خواهد بود و گسترش آموزش عمومی کاربران در پیشگیری از جرائم اینترنتی نقش بسزایی دارد و عوامل فردی چون عدم آگاهی و دانش در خصوص فضای مجازی می تواند اثر بیشتری در شکل گیری جرائم اینترنتی نسبت به عوامل قانونی داشته باشد. بنابراین بالا بردن سطح آگاهی و دانش کاربران جامعه یکی از مهمترین راه ها و ابزاری است که می تواند موجب پیشگیری و مانعی برای جرایم سایبری گردد.

واژگان کلیدی: روش ها و راهکارها ، پیشگیری ، جرایم اینترنتی

ISSN: 2538-3787
http://www.Joce.ir

مقدمه

فناوری اطلاعات تحولات شگرفی در روند فعالیت جامعهٔ بشری به وجود آورده است، به گونه ای که زندگی امروزی بدون استفاده از این فناوری با دشواری های فراوانی مواجه است. با گسترش اینترنت و ظهور فضای مجازی، به دلیل ویژگی های خاص این فضا مانند امکان تحصیل هویتهای گوناگون، گمنامی و سهولت انجام اعمال مختلف، ضمن مهاجرت بسیاری از جرایم از فضای فیزیکی به فضای مجازی موجب بروز جرایم نوینی نیز شده است که قابل مقایسه با هیچ یک از جرایم موجود کلاسیک نبوده و چه بسا از نظر دامنه تأثیر، خطرناکتر باشد. توسعه فناوری های نوین هر روز ابعاد جدیدتری پیدا می کند و در حال در هم نوردیدن و حضور فعال در تمامی زمینه ها و حوزه های بشری است. همین گستردگی و توسعهٔ فراگیر آن موجب شده تا بسیاری از ابعاد آن ناشناخته بوده و محل مناسبی برای مجرمان در اجرای عملیات مجرمانهٔ آنها باشد. فضای سایبر در کنار برخورداری از مزایا و آثار مثبت فراوان، منشاء تهدیدهایی جدی برای کلیهٔ افراد، سازمان ها و کشورهای جهان از توسعه یافته و غیر توسعه یافته شده است(جلالی، ۱۳۹۱).

بنابراین می توان گفت که با شیوع استفاده از رایانه در زندگی شخصی و روابط اداری، بزهکاری و تخلف در استفاده از رایانه نیز، واقعه ای اجتناب ناپذیر است. آنچه امروز تحت عنوان جرایم رایانه ای نام برده می شود، مجموعه ای از همین تخلفات و بزهکاری هاست که از طریق رایانه یا مؤثر بر رایانه اتفاق می افتد و مصادیق متعددی از آن نیز در ذهن ما نقش بسته است. از زمان ابداع اینترنت تا زمانی که استفاده از اینترنت شکل عمومی پیدا کرد، تصور از پیش تعیین شده ای درباره این امکان ارتباطاتی و اتفاقاتی که در آن می افتد، وجود نداشت (شاهبندرزاده و یوسفی ده بیدی، ۱۳۹۱) و این فضای بی پاسبان و رها که هر لحظه بر گسترهٔ آن افزوده می شود، فرصت بسیار مناسبی را برای ارتکاب و اختفای جرایم سایبری که تهدیدهای آن به مراتب در مقایسه با محیط واقعی بیشتر است ، به مرتکب اعطا می کند. علاوه بر این، گمنامیِ هر کاربر اینترنتی کشف و شناسایی مرتکب را اگر نگوییم غیر ممکن بسیار دشوار ساخته است، به نحوی که این انحرافات، یکی از چالش های اصلی تمامی جوامع بشری شده است، به که تهدیدهای آن به مراتب در مقایسه با محیط واقعی بیشتر است زیرا می توان به تعداد فرصت های آن، تهدیدهای اجتماعی، اخلاقی، حقوقی و سیاسی برشمرد (کیزا[1] ۲۰۱۳). از این رو، آنچه اخیراً ذهن سیاست گذاران را به خود مشغول داشته است، این است که در قبال جرایم سایبری سودمندترین تدبیر چیست؟ بنابراین این پژوهش نیز قصد دارد تا به بررسی شیوه ها و راهکار های پیشگیری از جرایم اینترنتی از دیدگاه اساتید ارتباطات و فعالان حوزه فضای مجازی بپردازد.

۱-بیان مسأله

رایانه و فناوری های مرتبط با آن ابزاری ضروری است که جنبه های مختلف قابل توجهی از زندگی اجتماعی و شخصی از قبیل آموزش، کسب و کار، فرهنگ و فعالیت های اوقات فراغت را تحت تأثیر قرار می دهد.

استفاده گسترده از رایانه های شخصی و اینترنت با سرعت بالا انحرافات مرتبط با رایانه و رفتارهای جنایی از قبیل هک کردن، بارگذاری موسیقی به صورت غیر قانونی، برنامه های نرم افزاری، سرقت رمز عبور دیگران و... به صورت قابل توجهی افزایش داده است (روبرت و اولسون[2]، ۲۰۱۰).

بنابراین می توان گفت که امروزه با توجه به گسترش استفاده از فناوری اطلاعات و انجام بسیاری از امور سازمان ها و افراد در فضای مجازی و در واقع رواج استفاده از اینترنت، گرایش و تمایل به انجام جرم در این محیط نیز به دلایل مختلف افزایش یافته است. بسیاری از افرادی که در محیط های واقعی به دلایل متعدد از جمله شرم و حیا، و ترس از برخورد پلیس و دلایل دیگر اقدام به انجام ارتکاب عمل مجرمانه نمی کنند، در این فضا به دلیل ویژگی های فضای مجازی تمایل به ارتکاب جرم پیدا می کنند. با توجه به این موارد و عدم وجود محدودیت مکانی و زمانی، تمایل به ارتکاب جرم در این فضا به سرعت درحال افزایش است. باتوجه به روند رو به رشد وقوع جرایم سایبری به دلیل ماهیت و ویژگی های فضای مجازی و نقش اساتید ارتباطات و فعالان حوزه فضای مجازی در پیشگیری از وقوع جرایم در فضای فیزیکی و مجازی، این پژوهش در صدد است تا بررسی شیوه ها و راهکار های پیشگیری از جرایم اینترنتی از دیدگاه اساتید ارتباطات و فعالان حوزه فضای مجازی بپردازد. در واقع این پژوهش به دنبال پاسخ به این سؤال اساسی است که آیا وجود خلاء های قانونی در افزایش جرائم اینترنتی در فضای مجازی موثر است؟- آیا عدم آگاهی کاربران از چگونگی حفظ امنیت در فضای مجازی از عوامل سوءاستفاده کلاهبرداران است؟- آیا مهم ترین نقطه ضعف پیشگیری از جرائم اینترنتی عدم وجود قوانین به روز و کار آمد است؟

[1] Kizza
[2] - Robert & Olsonl

ISSN: 2538-3787
http://www.Joce.ir

۲-اهمیت و ضرورت پژوهش

رایانه و فناوری های مرتبط با آن ابزاری ضروری است که جنبه های مختلف قابل توجهی از زندگی اجتماعی و شخصی از قبیل آموزش، کسب و کار، فرهنگ و فعالیت های اوقات فراغت را تحت تأثیر قرار می دهد. با استفاده گسترده از رایانه های شخصی و اینترنت با سرعت بالا انحرافات مرتبط با رایانه و رفتارهای جنایی از قبیل هک کردن، بارگذاری موسیقی به صورت غیر قانونی، برنامه های نرم افزاری، سرقت رمز عبور دیگران و... به صورت قابل توجهی افزایش پیدا کرده است(هیگینس وریکرت[1] ۲۰۰۸). باگسترش و توسعه این فضا، جرائم رایانه ای مرتبط با امور غیر اخلاقی نیز گسترش یافته و تأثیر منفی بر نظام اجتماعی و پایه ای – 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(کوچی و داودی، ۱۳۹۴).

پیشگیری از جرم، نخستین گام برای تحقق عدالت کیفری است و فضای سایبر به اقتضای ویژگی های خاصی که دارد، برای پیشگیری وضعی بسیار مساعد است. رهایی بستر، گمنامی کاربران، آسیب پذیری آماج، دشواری شناسایی بزهکاران، سهولت ارتکاب جرم، گستردگی خسارت، کثرت بزهدیدگان و کم سن بودن اغلب کاربران، ضرورت پیشگیری وضعی از این جرایم را دو چندان ساخته است، لذا با اعمال شیوه های پیشگیری از جرم، می توان تا حد مطلوبی از این جرایم پیشگیری نمود(بهره مند و همکاران، ۱۳۹۳) چرا که ثابت شده که افراد با داشتن یک رایانهٔ متصل به اینترنت و سواد رایانه ای اندک می توانند مجرمی بالقوه باشند. عدم مجاورت فیزیکی بزهکار و بزهدیده نیز ارتکاب این جرایم را آسانتر کرده است(بهره مند و همکاران، ۱۳۹۳). اگر چه نمی توان هیچ جامعه ای را بدون جرم تصور کرد، در مقابل، انسان نیز هیچ گاه نسبت به وقوع جرم بی تفاوت نبوده و در راستای مبارزه با آن در تلاش است. با وجود این جهت مقابله با ارتکاب جرم در محیط مجازی نیازمند تدابیر و راهکارهای نوینی هستیم.

امید است سیاستگذاران و برنامه ریزان در امر پیشگری از جرایم اینترنتی بتوانند با بهره گیری از نتایج این پژوهش به راهکارهای مفید و سودمند در این زمینه دست یابند.

۳-سئوالات پژوهش

۱- آیا وجود خلاء های قانونی در افزایش جرائم اینترنتی در فضای مجازی موثر است؟

۲- آیا عدم آگاهی کاربران از چگونگی حفظ امنیت در فضای مجازی از عوامل سوءاستفاده کلاهبرداران است؟

۳- آیا مهم ترین نقطه ضعف پیشگیری از جرائم اینترنتی عدم وجود قوانین به روز و کار آمد است؟

۴-فرضیات پژوهش

۱-به نظر می رسد وجود خلاء های قانونی بیشتر از عوامل انسانی درافزایش جرائم اینترنتی موثر است.

۲-به نظر می رسد بین عدم آگاهی کاربران از چگونگی حفظ امنیت خودشان در فضای مجازی و افزایش جرائم اینترنتی رابطه وجود دارد.

۳- به نظر می رسد بین افزایش جرائم اینترنتی و عدم وجود قوانین به روز و کار آمد رابطه وجود دارد.

۵-مروری بر ادبیات تحقیق

در این بخش به مبانی نظری و ادبیات تحقیق پژوهش پرداخته ایم.

۵-۱- جرایم اینترنتی و پیشینه آن در الگوی مصرف آن

۵-۱-۱- تعریف جرائم اینترنتی

در مورد تعریف جرم رایانه ای، خرم آبادی (۱۳۸۳) جرایم رایانه ای را جزء جرایم مرتبط با فناوری اطلاعات می دانند و اینگونه بیان می کنند که اصطلاحات جرم رایانه ای و جرم مرتبط با رایانه، اولین و قدیمی ترین اصطلاحاتی هستند که برای نسل اول جرایم فناوری اطلاعات مورد استفاده قرار گرفته اند و علت انتخاب عناوین جرم رایانه ای وجرم مرتبط با رایانه برای اینگونه جرایم این بوده که رایانه به عنوان هدف یا وسیله ارتکاب جرم در این گونه جرایم محوریت داشته است .

[1] Higgins & Ricketts

ISSN: 2538-3787
http://www.Joce.ir

تعریف جرایم از منظر سازمان های مختلف:

- سازمان OECD:

سوء استفاده از رایانه شامل هر رفتار غیرقانونی، غیراخلاقی یا غیر مجاز مربوط به پردازش خودکار در انتقال داده است.

- سازمان ملل متحد:

جرم رایانه ای می تواند شامل فعالیت های مجرمانه ای باشد که ماهیتی سنتی دارند اما از طریق ابزار مدرنی مثل رایانه و اینترنت صورت می گیرد.

-کمیته اروپایی مسائل جنایی در شورای اروپا:

هر فعل مثبت غیرقانونی که رایانه در آن ابزار یا موضوع جرم باشد. به عبارت دیگر هر جرمی که ابزار و هدف تأثیرگذاری آن رایانه باشد.

- پلیس فدرال آلمان:

جرایم متضمن اعمال توأم با بی مبالاتی یا حوادثی که موجب تخریب عملکرد سیستم رایانه یا استفاده از آن باشد، جرم رایانه ای است. یک مضمون مشترک در میان تعاریف از جرم و جنایات رایانه ای، استفاده غیر قانونی از رایانه و دستگاه های مرتبط با رایانه به وسیله افراد، گروه ها یا سازمان های خاص با دانش رایانه است. تعداد چشمگیری از مکالمات بر انواع متعددی از جرم و جنایت تمرکز کرده اند، که شامل کپی غیر قانونی و تجاری از نرم افزارهای شرکت های تجاری، دسترسی غیر قانونی به سیستم رایانه های اشخاص و ایجاد انتشار برنامه های ویروس رایانه ای با استفاده از نمونه های غیرتصادفی از دانشجویان دانشگاه است (هیگینس، ۲۰۰۷**).**

۵-۱-۲- طبقه بندی مرسوم از جرایم رایانه ای

جاسوسی، کلاهبرداری، سرقت خدمات مهمترین گونه های جرایم رایانه ای می باشند. امکان ارتکاب این جرایم بر خلاف فضای مادی در جهان سایبر به گونه ای دیگر است. بدین منظور شیوه های پیشگیرانه از ارتکاب این جرایم نیز متفاوت اند. پس ابتدا باید کلیاتی راجع به این جرایم دانست.

۵-۱-۲-۱- جاسوسی رایانه ای

«جاسوسی رایانه ای عبارت است از جمع آوری مخفیانه و غیر قانونی اطلاعات مرتبط با امور سیاسی و نظامی یک کشور یا اطلاعات مربوط به مردم آن. به این تعریف باید ویژگی حساس بودن اطلاعات را نیز اضافه کرد. تعیین مصادیق جاسوسی و مراحل آن همواره مناقشه آمیز بوده و قانونگذاران با هدف تضمین امنیت ملی، به طور شفاف، ماهیت، اقسام و مراحل آن را تعریف نکرده اند. به طور خلاصه می توان گفت تعیین اطلاعات مورد نیاز، جمع آوری اطلاعات و بالاخره تحلیل آن سه مرحله مهم این جرم تلقی می‌شوند.»(عالی پور،۱۳۸۸).

۵-۱-۲-۲- کلاهبرداری رایانه ای

شاید بتوان گفت کلاهبرداری رایانه ای در زمره جرایم نسل اول رایانه است که در این نسل علی رغم وضعیت فعلی رایانه صرفا می توانست در ارتکاب جرم صرفاً به عنوان یک وسیله متقلبانه محسوب گردد و بنابراین می توان کلاهبرداری رایانه ای را به عنوان یکی از اولین جرایم رایانه ای پس از دخالت بی چون و چرای رایانه در زندگی بشر دانست(رستمی، ۱۳۹۲).

کلاهبرداری رایانه ای در زمره جرایمی است که با تکیه بر فناوری برتر انجام می پذیرد. این جرم در ایران امروز در قانون تجارت الکترونیکی و فصل سوم قانون جرایم رایانه ای تبلور یافته است. به موجب ماده ۶۷ قانون تجارت الکترونیکی مصوب ۱۳۸۲ «هر کس در بستر مبادلات الکترونیکی یا استفاده غیر مجاز از داده پیام ها، برنامه ها و سیستم های رایانه ای و وسایل ارتباط از راه دور و ارتکاب افعالی نظیر، ورود، محو و توقف داده پیام، مداخله در عملکرد برنامه یا سیستم رایانه ای و... دیگران را بفریبد و یا سبب گمراهی سیستم های پردازش خودکار و نظایر آن شود و از این راه برای خود یا دیگری وجوه، اموال و یا امتیازات مالی کسب کند و اموال دیگران را ببرد» مرتکب جرم کلاهبرداری شده است. به موجب تبصره این ماده شروع به کلاهبرداری جرم محسوب و مجازات آن حداقل مجازات مقرر در این ماده می باشد. همچنین فصل سوم قانون جرایم رایانه ای مصوب ۱۳۸۸ در مواد ۱۲ و ۱۳ از سرقت و کلاهبرداری رایانه ای به این ترتیب یاد کرده است:

ISSN: 2538-3787
http://www.Joce.ir

ماده (۱۲) هرکس به طور غیرمجاز داده‌های متعلق به دیگری را برباید، چنانچه عین داده‌ها در اختیار صاحب آن باشد، به جزای نقدی از یک تا بیست میلیون ریال و در غیر این صورت به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد.

ماده (۱۳) هرکس به طور غیرمجاز از سیستم‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سیستم وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند علاوه بر رد مال به صاحب آن به حبس از یک تا پنج سال یا جزای نقدی از بیست تا یکصد میلیون ریال یا هر دو مجازات محکوم خواهد شد.

در سطح بین المللی نیز کلاهبرداری رایانه ای تعریف شده است. برای مثال سازمان همکاری اقتصادی و توسعه اروپا[1] در گزارش سال ۱۹۸۶ خود تحت عنوان جرایم مرتبط با رایانه، تحلیل سیاست های اقتصادی، کلاهبرداری رایانه ای را به شرح زیر تعریف کرده است: «کلاهبرداری رایانه ای عبارت است از وارد کردن، تغییر،دادن، پاک کردن و یا متوقف کردن داده ها و یا برنامه های رایانه ای که به طور ارادی و با قصد انتقال غیر قانونی وجوه یا هر چیز با ارزش دیگری صورت گرفته باشد.»(www.OECD.org) همچنین شورای اروپا در توصیه نامه شماره R(۸۹)۹ خود مصوب ۱۹۸۹، کلاهبردای رایانه ای را به شرح ذیل تعریف کرده است:

«هر گونه وارد کردن، تغییر دادن، حذف کردن یا متوقف کردن داده ها یا برنامه های رایانه ای یا دیگر مداخلات در پردازش داده های رایانه ای که به قصد تحصیل امتیاز غیر قانونی برای خود شخص یا شخص دیگر انجام شود و بر نتیجه پردازش اثر گذارد و به این طریق موجب ایجاد زیان اقتصادی یا تصرف مال دیگری شود کلاهبرداری رایانه ای نامیده می شود.»(خرم آبادی، ۱۳۸۶، ۸۹).

۵-۱-۲-۳- سرقت خدمات

استفاده غیر مجاز از سیستم های پردازش داده که عموما به نام سرقت خدمات یا سرقت زمان شناخته شده است در زمینه پردازش داده ها بسیار رایج است. موضوع این جرم، خدمات پردازش، ذخیره سازی و انتقال سخت افزار کامپیوتری نیز غالباً برنامه و دیگر داده هایی است که به وسیله کارمندان پردازش داده ها برای مقاصد خود استفاده می کنند. در بیشتر موارد سرقت خدمات خصوصاً اگر توسط کارمندان ارتکاب یابد، خسارت قابل ملاحظه ای به شرکت مربوطه به بار نمی آورد و در مقایسه با سایر جرایمی که نام بردیم خطر کمتری دارد. با این حال ممکن است منافع شرکت با سوء استفاده از سیستم های پردازش از راه دور داده ها یا هنگامی که شرکت خدمات یا مشتریانش را در اثر سیستم تحریم یا ممانعت از به کار گیری نیروی کارمندان از دست می دهد به شدت آسیب ببیند(رستمی، ۱۳۹۲).

۵-۲- نگاهی به قوانین و مقررات مربوط به جرایم اینترنتی

۵-۲-۲- مصادیق جرایم رایانه ای در قوانین ایران

- کلاهبرداری کارت اعتباری:

شایعترین جرمی که در سال های اخیر در فضای سایبر گزارش شده کلاهبرداری کارت اعتباری است. دزدی و سوء استفاده از کارت های اعتباری بی حد و حصر است. عوامل بی شماری از جمله: وسوسه، دسترسی آسان و عدم لزوم مهارت های فنی خاص برای موفقیت در این جرم، از دلایل ارتکاب به این جرم است.

- افترا و نشر اطلاعات از طریق پست الکترونیک:

پست الکترونیک مرسوم ترین و گسترده ترین سرویس اینترنت است و توسط آن علاوه بر فایل های متنی، صوت، تصویر فایل های ویدئویی نیز به دیگر کاربران اینترنت قابل ارسال است. هر کاربر می تواند در شبکه های بین المللی از طریق یک آدرس پست الکترونیک مشخص شناخته شود که با دسترسی به رمز آن می توان به آسانی در آن تقلب کرد.

-تطهیر پول نامشروع رایانه ای در فضای سایبر:

تطهیر پول نامشروع از جرایم کلاسیک بوده که دارای سابقه و قدمت زیادی است و با فناوری رایانه و بسط شبکه های بین المللی، مصادیق جدید این جرم در فضای سایبر به کمک اینترنت، پست الکترونیک و شبکه های بین المللی ارتباطی صورت می پذیرد. نحوهٔ ارتکاب بدین نحو است که باندهای بزرگ نامشروع توسط نامهٔ الکترونیکی یا اینترنت بدون هیچ گونه اثر و نشانی درخواست ارسال مبالغی پول به حساب شخص معینی را (به وی) می کنند و در تقاضای خود نحوهٔ ارسال پول و دستمزد و مدت استرداد را بیان و در

[1] Organization for Economic Cooperation and Development (OECD)

ISSN: 2538-3787
http://www.Joce.ir

صورت قبول طرف، نوع و نحوهٔ تضمین های لازم را اعلام می دارند و اصولاً در زمان استرداد پول یک عنوان مشروع در تجارت الکترونیک را با منشا تجاری انتخاب و با هدف خود هماهنگ می کنند.

- دسترسی غیر مجاز درمحیط سایبر:

دسترسی غیر مجاز به داده ها یا سامانه های رایانه ای از جمله جرایمی است که در محیط سایبر به وقوع می پیوندد. دسترسی غیر مجاز را به عنوان جرمی مادر تلقی می کنند، زیرا دارای نقشی مؤثر در وقوع سایر جرایم سایبری است. در برخی موارد دسترسی غیر مجاز عامل تسهیل کننده در وقوع سایر جرایم سایبری و حتی جرایم سنتی است و در برخی موارد دیگر مقدمهٔ ارتکاب جرم تلقی می شود. از نظر میزان وقوع و میزان خسارت هم در سطح بالایی قرار دارد.

- جمع آوری اطلاعات شخصی:

مجرمان اطلاعات شخصی افراد را از قبیل شماره کارت ملی، اطلاعات گواهینامه، شماره تلفن، آدرس شخصی و نظایر آن جمع آوری کرده و سپس آن را با قیمت مناسبی به فروش می رسانند. این اطلاعات توسط افراد مختلف به خصوص نفوذگرها به منظور شناسایی اطلاعات سری افراد استفاده می شود. یکی از کاربردهای بالقوهٔ این اطلاعات شخصی، دزدی شخصیت است. دزدی شخصیت می تواند یک مشکل اساسی برای بخش های قضایی باشد. افراد، اطلاعات دیگران را از روی اینترنت جمع آوری کرده و سپس خود را جای آنان معرفی می کنند (شاه محمدی و تاهو، ۱۳۹۳).

۳-۶- شیوه ها و راهکارهای قانونی و فنی پیشگیری از جرایم اینترنتی

۱-۳-۶- شیوه ها و راهکاری پیشگیری از جرایم اینترنتی در قانون ایران پیشگیری از منظر رویکرد:

بر این اساس، پیشگیری بر دو نوع پیشگیری کیفری(از طریق سازوکارهای نظام عدالت کیفری) و غیر کیفری(از طریق سازوکارهای خارج از نظام عدالت کیفری) تقسیم می شود(عباچی، ۱۳۸۷). پیشگیری کیفری را می توان از یک منظر بر دو نوع، پیشگیری قضایی و پیشگیری انتظامی تقسیم کرد:

پیشگیری قضایی:

در پیشگیری قضایی سیاست پیشگیری از این منظر که دولت(دستگاه حاکم) به عنوان اولین نهاد در مقابل جرم و مجرم (بزهکار) قرار می گیرد و از طریق اعمال قانون و سیاست های تقنینی در مقابل بزهکار، به اصلاح آنان می پردازد، مورد توجه قرار می گیرد.

پیشگیری انتظامی:

در نقش اول پلیس به عنوان ضابط قوهٔ قضائیه عهده دار امر پیشگیری انتظامی است و در چهارچوب سیاست های کیفری یا جنایی و تحت نظارت مقامات قضایی عمل می کند و در نقش دوم، پلیس به عنوان سازمان یا نهاد همچون سایر سازمان ها و دستگاه های دولتی و غیر دولتی اقداماتی را انجام می دهد که جلوهٔ اقدامات اجتماعی پلیس یا فعالیت های جامعه محوری پلیس محسوب می شود (بیات و همکاران،۱۳۸۷).

پیشگیری مبتنی بر فناوری اطلاعات:

فناوری اطلاعات تأثیرات اساسی و مثبتی در زندگی انسان ها داشته است و این قابلیت را دارد که در امر پیشگیری از جرم نیز مورد استفاده قرار گیرد. از آنجا که بهره برداری از فناوری اطلاعات در برخورد با جرایم سایبری باعث می شود که : ۱- ارتکاب جرم سخت شود، ۲- هزینهٔ ارتکاب جرم به دلیل قابلیت پیگرد و دستگیری سارقان، افزایش یابد؛ ۳- مجرمان سایبری به طور مؤثرتر و سریع تر دستگیر شوند. بنابراین پیشگیری مبتنی بر فناوری اطلاعات، نوعی پیشگیری وضعی تلقی می شود. ردیابی هویت مجازی، گشت فضای مجازی، جمع آوری ادلهٔ جرم و مستند سازی صحنه جرم از مصادیق پیشگیری وضعی تلقی می شوند. روش های مختلف پیشگیری مبتنی بر فناوری اطلاعات برای پیشگیری از جرایم سایبری تبیین می شود.

ISSN: 2538-3787
http://www.Joce.ir

الف) ردیابی هویت مجازی:

نشانی پروتکل اینترنت یا نشانی هویت مجازی، عددی است که به هریک از دستگاه ها و رایانه های متصل به شبکهٔ رایانه ای کـه بـر مبنـای نمایه IP/TCP از جمله اینترنت کار می کند، اختصاص داده می شـود. پیـام هـایی کـه دیگر رایانه هـا بـرای ایـن رایانـه مـی فرسـتند بـا ایـن نشـانه عـددی همـراه اسـت و مسیریاب های شبکه آن را مانند نشانی گیرنده در نامه های پستی تعبیر می کننـد، تـا بالاخره پیام به رابط شبکهٔ رایانه مورد نظر برسد. هر نشانی کامل، شامل یک پیشـوند و یک پسوند است و طوری تخصیص داده می شوند که یکتا باشـند، بنـابراین ویژگـی اول تضـمین مـی شـود. اگـر دو رایانـه بـه دو شـبکهٔ مختلـف متصـل شـده باشـند، نشانی هایشان پیشوندهای متفاوت خواهند داشت، اما اگر دو رایانه به یک شبکه وصل باشند، نشانی هایشان دارای پسوندهای متفاوت خواهد بود.

ب) گشت فضای مجازی:

یکی از شـیوه هـای مبتنـی بـر فنـاوری اطلاعـات بـرای پیشگیری از جرایم سایبری، گشت فضای مجازی است. گشت فضای مجازی با هدف کشف پیش دستانه جرایم رایانه ای انجام می شود. به عبـارت دیگـر گشـت زنـی در فضای سایبر به منظور پیشگیری از وقوع جرم یاکشف جرم انجام مـی گیـرد. مراحـل انجام گشت فضای مجازی عبارتند از:

انتخاب کلید واژه ها:

با توجه به موضوع مورد نظر، کلید واژه هایی انتخاب می شوند که به ما در رابطه با آن موضوع یا مصداق کمک می کند تا به ادلهٔ جرم برسیم.

- انتخاب موتور جستجو و انجام جستجو:

بعد از تعیین موضوع یا مصداق جرم و انتخاب کلید واژه ها، یکی از موتورهای جستجوی مطرح در فضای مجـازی از جملـه بینگ، یاهو و گوگل نتخاب و کلید واژه ها مورد جستجو قرار می گیرد.

- بررسی صفحات حاصل از جستجو:

بعد از انجـام جسـتجو، صـفحات حاصـل از جستجومورد بررسی قرار می گیرد که در این فرایند، تک تک سایت هـا، وبـلاگ هـا، پایگاه ها و گلوگاه های خبری به صورت دقیق بررسی می شود و در صورت وجود ادلهٔ جرم در صفحات، از طریق اطلاعات موجـود در آن هـا از قبیـل شـماره تمـاس، پسـت الکترونیکی، اطلاعات آدرسی که بتواند در جهت رسیدن به صاحب اصـلی وبـلاگ یـا وب سایت کمک کند، مستند می شود.

ج) کنترل و نظارت بر فضای مجازی:

کنترل و نظارت مسـتلزم انجـام نظـارت بـر فعالیت شبکه های ارتباطی، وب سایت ها، ارائـه دهنـدگان خـدمات اینترنـت اسـت.

فعالیت های انجام شده در طی کنترل و نظارت عبارتند از:

- ✓ مراجعه به مراکز وب سایت ها، شبکه های ارتباطی و مراکـز ارائـه دهنـدهٔ خـدمات اینترنت و میزبانی و کافی نت ها.
- ✓ بازرسی محتوای موجود در سامانه ها، شبکه ها و وب سایت ها و بررسـی و تحلیـل داده های ترافیکی جمع آوری شده توسط ارائه دهندگان خدمات اینترنت و همچنین استفاده از نرم افزارهای مرتبط.
- ✓ در صورت لزوم شنود با مجوز موبایل یا تلفن عوامل مرتبط با شبکه ها، وب سایت ها یا ارائه دهندگان دارای ادلهٔ مجرمانه.
- ✓ در صورت مواجه با مصادیق مجرمانه، انعکاس مصادیق جرم به مبادی ذی ربط.

د) جمع آوری ادلهٔ الکترونیکی جرم:

اولین فردی که وارد صحنهٔ جرم مـی شـود موظف به تشخیص، انتخاب، حفاظت، حمل و یـا ذخیـرهٔ مـدرک الکترونیکـی اسـت. ممکن است که هر کدام از کارکنان دستور جمع آوری مدارک الکترونیکی را داده یـا خود در جمع آوری مدارک مشارکت کنند. شاید لازم باشد مسؤلان آزمایشـگاهی در صحنهٔ جرم به عنوان دستیار عمل کرده و در بررسی مدارک ایفای نقش کنند. در این بین وظیفهٔ مدیران این است که اطمینان حاصل کنند افراد تحت امر آن ها بـه خـوبی آموزش دیده و در برخورد با مدارک الکترونیکی به اندازهٔ کافی مجهز

ISSN: 2538-3787
http://www.Joce.ir

هستند(جوکز، ۱۳۸۹). هر فرد مسؤل باید حساسیت و ماهیت مدارک الکترونیکی، شیوه هایی که برای انتخاب و حفاظت از آن ها وجود دارد را درک کند. آیین دادرسی باید به گونه ای باشد که اجازه بررسی صحنهٔ جرم الکترونیکی را صادر کند. ادلهٔ الکترونیکی، داده ها و اطلاعاتی هستند که توسط ابزار الکترونیکی ذخیره یا انتقال داده می شوند و حائز اهمیت تخصصی هستند. همان طور که اثر انگشت یا DNA ادله ای مخفی هستند، مدرک الکترونیکی نیز همان حالت را دارد. مرحلهٔ جمع آوری شامل جستجو برای شناسایی، جمع آوری و مستند سازی مدرک الکترونیکی است.

هـ) مستندسازی صحنهٔ جرم:

مستند سازی صحنهٔ جرم موجب ثبت آن واقعه در تاریخ برای همیشه خواهد شد. مستند سازی صحنه در جریان تحقیقات، فرآیندی ثابت و دائم است. ثبت صحیح محل و وضعیت رایانه ها، وسایل ذخیره، دیگر وسایل الکترونیکی و ادلهٔ قراردادی حائز اهمیت است. صحنهٔ جرم را باید همراه با جزییات آن مستند سازی کرد. صحنهٔ فیزیکی را مشاهده و مستند سازی می کنیم. وضعیت و محل سیستم رایانه ای از جمله وضعیت برق رایانه (روشن، خاموش یا در حال استراحت) را مستند سازی کنیم. اکثر رایانه ها دارای چراغ وضعیت هستند که نشان می دهد رایانه روشن است، به همین صورت چنانچه صدای پنکه (فن رایانه) به گوش برسد، احتمالاً سیستم روشن است و به علاوه اگر سیستم رایانه گرم باشد ممکن است نشان دهندهٔ این باشد که دستگاه روشن بوده یا اینکه به تازگی خاموش شده است. قطعات الکترونیکی مربوطه را مشخص و مستند سازی کنیم که جمع آوری نخواهند شد. صحنهٔ جرم در نفوذ غیر مجاز، شامل سیستم های رایانه ای میزبان، سرویس گیرنده مخابرات و رایانهٔ بزهکار است. ممکن است رایانهٔ میزبان در ایران و رایانهٔ بزهکار در ایالات متحده باشد و یا بالعکس. پراکندگی جغرافیایی صحنهٔ جرم بسیار زیاد و معمولاً دور از هم و در محدودهٔ مرزهای جغرافیایی کشورهای مختلف است. در جرم (نفوذ غیر مجاز) نیز آثار ادلهٔ شناسایی، جمع آوری و تجزیه و تحلیل می شود که اغلب شامل نشانی هویت مجازی نام کاربر، که اغلب شامل نشانی هویت مجازی است پلیس برای شناسایی هویت مظنون، از مصاحبه و تحقیقات محلی، آثار انگشت و چهره نگاری استفاده می کند. در جرم نفوذ غیر مجاز پلیس برای شناسایی هویت مظنون از (IP) مشخصات سیستم عامل و سخت افزار مظنون، شناسه، گذر واژه و فایل های نگهداری شده در مسیری که مظنون طی کرده و...) همچنین آثار انگشت و روش های شناسایی هویت معمول در کشف جرایم کلاسیک بهره می برد. برای بررسی صحنهٔ جرم نفوذ غیر مجاز و شناسایی و جمع آوری آثار و ادلهٔ جرم از سخت افزارها و عمدتاً نرم افزارهای تخصصی که بر اساس استانداردهای بین المللی تولید شده اند استفاده می شود(شاه محمدی و تاهو، ۱۳۹۳).

۴-۵- پلیس فتا و نقش آن در پیشگیری از جرائم رایانه ای

۱-۴-۵- تاریخچه شکل گیری پلیس فتا

فرمان فرماندهی معظم کل قوا(حفظه الله تعالی)

مقام معظم رهبری در نامه ای به رئیس جمهور، ضمن برشماری سیاست های کلی برنامه پنجم توسعه در چارچوب سند چشم انداز بیست ساله ایجاد ساختار یکپارچه نرم افزار با هدف ارتقاء سطح امنیت از فضای سایبری کشور را نیز به شرح زیر ابلاغ فرمودند:

"ایجاد سامانه یکپارچه نر م افزاری اطلاعاتی، ارتقاء سطح حفاظت از اطلاعات رایانه ای، توسط علوم و فن آور ی های مرتبط با حفظ امنیت سامانه های اطلاعاتی و ارتباطی به منظور صیانت از فضای تبادل اطلاعات، تقویت مخابراتی، مقابله با تخلفات در فضاهای رایان های و صیانت از جرم فردی و عمومی (پرچ، ۱۳۹۲).

چشم انداز جمهوری اسلامی ایران در افق ۱۴۰۴ هجری شمسی

سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور

تصویب نامه در خصوص تعیین سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور:

هیئت وزیران در تاریخ ۱۳۸۷/۳/۵ بنابه پیشنهاد شماره ۱/۲۵۵۹۹ مورخه ۱۳۸۶/۷/۲۴ وزارت ارتباطات و فن آوری اطلاعات به استناد بند (ج) ماده 44 قانون برنامه چهارم توسعه اقتصادی، اجتماعی و فرهنگی جمهوری اسلامی ایران -مصوب ۱۳۸۳ و با رعایت تصویب نامه شماره ۱۶۴۰۸۲/ت ۳۷۳ مورخه ۱۳۸۶/۱۰/۱۰ تصویب نمود . سند راهبردی امنیت فضای تولید و تبادل اطلاعات تصویب شد. این تصویب نامه در تاریخ ۱۳۸۷/۱۲/۷ به تأیید ریاست جمهوری وقت رسیده است.

ISSN: 2538-3787
http://www.Joce.ir

چشم انداز کلان کشور

تأمین امنیت فضای تولید و تبادل اطلاعات کشور با هدف ، عدم بروز اختلال در زیرساخت های حیاتی کشور و اعتماد و آسودگی خاطر آحاد شهروندان جامعه برای انجام تمامی امور قانونی از جمله فعالیت های اقتصادی، اجتماعی و فرهنگی به منظور صیانت از حاکمیت و اقتدار ملی در افق۱۴۰۴ در حوزه وظایف ناجا (پرچ، ۱۳۹۲).

۲-۴-۵- اهم وظایف پلیس فتا

- ممانعت از تعرض به ارزش ها و هنجارهای جامعه در حوزه وظایف ناجا
- حفاظت و صیانت از هویت دینی و ملی در حوزه های وظایف ناجا
- رشد فعالیت های علمی، اقتصادی، اجتماعی در جا معه اطلاعاتی در حوزه وظایف ناجا
- مراقبت و پایش از این فضا برای تبدیل نشدن به بستری برای انجام هماهنگی ها و عملیات ها جهت تحقق فعالیت های غیرقانونی(شاکر، ۱۳۹۴).

۳-۴-۵- چالش ها و فرصت های پلیس فتا برای مقابله با جرایم اینترنتی

- برای دسترسی به اینترنت هیچ گونه مجوز دولتی لازم نیست.
- دسترسی به اینترنت با پست الکترونیکی نیاز به هیچ گونه تائیدیه ای از طرف هیچ سازمان دولتی ندارد.
- هیچ دستورالعمل یا بخشنامه ای وجود ندارد که سرویس دهندگان را موظف کند اطلاعات مربوط به مشترکان، کاربران و محتوای داده های تبادل شده را به سازمان های دولتی ارائه دهند.
- هیچ قانون یا دستورالعملی برای منع رمزگذاری محتوای داده های مبادله شده وجود ندارد.
- هیچ قانونی وجود ندارد که سرویس دهندگان ملزم به کنترل محتوا نماید.
- هیچ سیاست و اقدام مشخصی در مورد سانسور یا بلوکه کردن سایت ها، گروه های مباحثاتی و آدرس های پست الکترونیکی وجود ندارد و ایران فاقد یک سیستم فیلترینگ ملی و مرکزی است.
- هیچ قانونی وجود ندارد که سرویس دهندگان را مسئول محتوای سایت های روی سرویس بداند.
- کافه های اینترنتی به سرعت در حال رشد است و هیچ قانون خاصی برای نحوه ی تأسیس و نحوه ی اداره وجود ندارد، این کافه ها تابع قانون اماکن عمومی هستند(هاقف، ۱۳۸۸).

۶- روش تحقیق

پژوهش حاضر به لحاظ روش، توصیفی، به لحاظ اجرا، پیمایشی و از نظر هدف کاربردی است.

تحقیق پیمایشی بهترین روش موجود برای آن دسته از پژوهندگان اجتماعی است که علاقه مند به جمع آوری داده های اصلی برای توصیف جمعیت های بسیار بزرگی هستند که نمی توان به طور مستقیم آن ها را مشاهده کرد (ببی۱۳۸۱؛۵۳۰)

۶-۱- جامعه آماری

جامعه آماری موردنظر، شامل ۳ گروه از متخصصان حوزه فضای مجازی است که شامل (اساتید علوم ارتباطات ، کارشناسان و خبرگان پلیس فتا در حوزه جرایم سایبر و فضای مجازی ؛ کارشناسان و فعالان حوزه اینترنت و فضای مجازی می باشند که تعداد کل افراد جامعه، ۳۰۰ نفر بوده که از این تعداد، ۱۲۶ نفر زن و ۱۷۴ نفر مرد هستند.

۶-۲- حجم نمونه و روش نمونه گیری

حجم نمونه: نمونه انتخاب شده از بین این سه گروه بوده و همه افراد انتخاب شده اند.

روش نمونه گیری: از روش تمام شمارشی برای این پرسشنامه استفاده شده است. یعنی تمامی افراد جامعه مورد بررسی قرار گرفته اند.

ISSN: 2538-3787
http://www.Joce.ir

۶-۳- ابزار تحقیق

ابزار تحقیق پیش رو، پرسشنامه با موضوع بررسی روش ها و راهکارهای پیشگیری از جرائم اینترنتی است.

۶-۴- روش‌های گردآوری اطلاعات

در این پژوهش، جهت جمع آوری اطلاعات در زمینه مبانی نظری و تدوین ادبیات پژوهش از روش کتابخانه ای (جمع آوری اطلاعات از اسناد موجود) و از روش میدانی (مشاهده افراد و وقایع) و برای گردآوری اطلاعات از پرسشنامه استفاده کرده ایم.

۶-۵- قلمرو پژوهش

قلمرو زمانی : تابستان ۱۳۹۵ قلمرو مکانی : شهر تهران

۶-۶- روایی و پایایی پرسشنامه

در این پژوهش برای اطمینان از پایدار و قابل اطمینان بودن تحقیق، روایی پرسشنامه سنجیده شده است. به این صورت که تعداد ۱۵ پرسشنامه در اختیار اساتید علوم ارتباطات ، کارشناسان و خبرگان پلیس فتا ؛ کارشناسان و فعالان حوزه اینترنت و فضای مجازی قرار داده در زمینه تعداد و تناسب موضوعات و ابعاد پژوهش سوال شد.و پس از جمع آوری نظرات، اصلاحات لازم با نظر نهایی اساتید محترم راهنما و مشاور انجام شد. سپس داده های بدست آمده از مطالعات مقدماتی را با استفاده از نرم افزار Spss ضریب آلفای کرونباخ را محاسبه گردید.

فرمول آلفای کرونباخ:

$$r_a = \frac{j}{j-1}\left(1 - \frac{\sum sj^2}{s^2}\right)$$

مقدار ضریب آلفای کرونباخ بدست امده از نرم افزار Spss نشان می دهد که مقدار آن برابر ۰/۸۹۳ می باشد. یعنی پرسشنامه ی حاضر، حدودا ۹۰ مورد اعتماد بوده و دارای اعتبار بالایی است .

برای بررسی آزمون فرض های پرسشنامه، ابتدا نرمال یا غیر نرمال بودن داده ها را می سنجیم.

جدول (۱) بررسی نرمال یا غیر نرمال بودن داده ها

آزمون کلموگروف اسمیرنف		جرائم اینترنتی
فراوانی		300
پارامتر های نرمال	میانگین	74.16
	انحراف معیار	16.678
آماره آزمون		.081
میزان سطح معنا داری		.000

طبق اطلاعات جدول (۱)، با توجه به اینکه در سطح اطمینان ۵ درصد، مقدار p-value = ۰،۰۰ بنابراین داده های بدست آمده از پرسشنامه، نرمال بوده و بنابراین فرضیه ها توسط آزمون های پارامتری سنجیده خواهد شد.

۷- یافته ها

فرضیه ۱: وجود خلاءهای قانونی بیشتر از عوامل انسانی در افزایش جرائم اینترنتی مؤثر است.

برای بررسی این موضوع از آزمون T مستقل جهت مقایسه‌ی دو عامل استفاده می‌کنیم:

ISSN: 2538-3787
http://www.Joce.ir

جدول (۲)، اطلاعات توصیفی پاسخگویان - فرضیه ۱

	عامل	تعداد	میانگین	انحراف استاندارد	میانگین خطای استاندارد
جرائم اینترنتی	خلاءهای قانونی	300	11.97	3.968	.229
	عوامل انسانی	300	9.59	2.965	.171

جدول (۲)، اطلاعاتی در مورد تعداد پاسخگویان (۳۰۰ نفر)، میانگین امتیازات در هر عامل (۱۱/۹۷ و ۹/۵۹) و انحراف معیار عوامل (۳/۹۶۸ و ۲/۹۶۵) را نشان می‌دهد.

با توجه به نرمال بودن مشاهدات از آزمون(student – t – test) دو نمونه مستقل استفاده می کنیم.

جدول (۳): آزمون T مستقل- فرضیه ۱

		مقدار آزمون در حالت برابری واریانس		t-test for Equality of Means				
		F	سطح معنی داری	t	درجه آزادی	سطح معنی داری (آزمون دوطرفه)	اختلاف میانگین	اختلاف خطای استادارد
جرائم اینترنتی	فرض برابری واریانسها	13.762	.000	8.345	598	.000	2.387	.286
	فرض عدم برابری واریانسها			8.345	553.547	.000	2.387	.286

با توجه به جدول بالا ابتدا فرض تساوی واریانس تساوی ما بررسی می شود:

$$\begin{cases} H_0: \sigma_1^2 = \sigma_2^2 \\ H_1: \sigma_1^2 \neq \sigma_2^2 \end{cases}$$

با توجه به P-Value محاسبه شده (.000) مربوط به آزمون Levense ، نتیجه می گیریم که فرض تساوی واریانس دو جامعه رد می شود.

بنابراین برای آزمون تساوی میانگین های از P-Value سطر دوم جدول که (.000) استفاده می کنیم.

$$\begin{cases} H_0: \mu_1 = \mu_2 \\ H_1: \mu_1 \neq \mu_2 \end{cases}$$

با توجه به P-Value = .000<۰,۰۵ فرض تسائی میانگین های در جامعه رد می شود و با توجه به بزرگتر بودن میانگین جرایم اینترنتی خلاء های قانونی اعلام می کنیم که تفاوت آماری معنی دار بین خلاءهای قانونی و عوامل انسانی وجود دارد و خلاء های قانونی سهم بیشتری در جرایم اینترنتی دارد.بدین معنا که وجود خلاءهای قانونی بیشتر از عوامل انسانی در افزایش جرائم اینترنتی مؤثر است.

فرضیه ۲: بین عدم آگاهی کاربران از چگونگی حفظ امنیت خودشان در فضای مجازی و افزایش جرائم اینترنتی رابطه وجود دارد.

این فرضیه را با استفاده از ضریب همبستگی پیرسون (با توجه به نرمال بودن مشاهدات)می‌سنجیم:

ISSN: 2538-3787
http://www.Joce.ir

جدول (۴): میزان همبستگی- فرضیه ۲

		کل	عدم آگاهی
جرائم اینترنتی	ضریب همبستگی پیرسون	1	.777**
	سطح معنی داری (دوطرفه)		.000
	تعداد	300	300

$$\begin{cases} H_0: \rho_{xy} = 0 \\ H_1: \rho_{xy} \neq 0 \end{cases}$$

مشاهدات بدست آمده از جدول بالا نشان می دهد میزان همبستگی و شدت رابطه‌ی جرائم اینترنتی و عدم آگاهی کاربران از چگونگی حفظ امنیت خودشان در فضای مجازی می باشد. طبق اطلاعات بدست آمده، p-value =0.000 یعنی با اطمینان ۹۵ درصد (یا خطای کمتر از ۵ درصد 0.000<0.05)، بین جرائم اینترنتی و عدم آگاهی کاربران رابطه وجود دارد و فرضیه پذیرفته می‌شود. مقدار ضریب همبستگی پیرسون برای این فرضیه برابر است با: ۰/۷۷۷ می توان گفت رابطه‌ی قوی بین این دو عامل وجود دارد.

فرضیه ۳: بین افزایش جرائم اینترنتی و عدم وجود قوانین به روز و کارآمد رابطه وجود دارد.

این فرضیه را (با توجه به نرمال بودن مشاهدات) با استفاده از ضریب همبستگی پیرسون می‌سنجیم:

جدول (۵): میزان همبستگی- فرضیه ۶

		کل	عدم وجود قوانین به روز
جرائم اینترنتی	ضریب همبستگی پیرسون	1	.658**
	سطح معنی داری (دوطرفه)		.000
	تعداد	300	300

$$\begin{cases} H_0: \rho_{xy} = 0 \\ H_1: \rho_{xy} \neq 0 \end{cases}$$

در جدول بالا، میزان همبستگی و شدت رابطه‌ی جرائم اینترنتی و عدم وجود قوانین به روز و کارآمد را نشان می‌دهد.طبق اطلاعات بدست آمده، p-value =0.000 یعنی با اطمینان ۹۵ درصد (یا خطای کمتر از ۵ درصد (0.000<0.05)، بین جرائم اینترنتی و عدم وجود قوانین به روز و کارآمد رابطه وجود دارد و فرضیه پذیرفته می‌شود. مقدار ضریب همبستگی پیرسون برای این فرضیه برابر است با: ۰/۶۵۸.

ISSN: 2538-3787
http://www.Joce.ir

۸- نتیجه‌گیری

همانطور که از قبل می دانیم پرسشنامه ی حاضر، بین ۳۰۰ نفر از سه گروه مختلف توزیع شد. نتایج بدست آمده از بررسی فرضیات موردنظر، به شرح زیر می باشد:

-در فرضیه ی ۱ قصد داشتیم دریابیم وجود خلاءهای قانونی بیشتر از عوامل انسانی در افزایش جرائم اینترنتی مؤثر است یا خیر؟

با توجه به بررسی های انجام شده (نتایج آزمونt مستقل و ۰,۰۰۰ = p-value یعنی با اطمینان ۹۵ درصد) دریافتیم که فرضیه ما درست بوده و با توجه به آراء پاسخ دهندگان، خلاءهای قانونی اثر بیشتری نسبت به عوامل انسانی در افزایش جرائم اینترنتی دارند. رضوی (۱۳۸۶) در پژوهشی با عنوان"جرایم سایبری و نقش پلیس در پشگیری از این جرایم و کشف آن ها" گزارش کرد کشور ما به هیچ کدام از کنوانسیون های بین المللی مربوط به جرایم سایبری نپیوسته است و با توجه به خلاء موجود در قوانین داخلی، نیروهای انتظامی برای پیشگیری از این جرایم و کشف آن ها، در عمل با مشکلاتی مواجه هستند.

-در فرضیه ۲ قصد داشتیم دریابیم آیا بین عدم آگاهی کاربران از چگونگی حفظ امنیت خودشان در فضای مجازی و افزایش جرائم اینترنتی رابطه وجود دارد یا خیر؟

بررسی ها نشان داد با (ضریب همبستگی ۰,۷۷۷ و ۰,۰۰۰= p-value یعنی با اطمینان ۹۵ درصد) بین این دو رابطه ی قوی با یکدیگر داشته و به عبارتی هرچه آگاهی کاربران نسبت به حفظ امنیت خودشان در فضای مجازی کمتر باشد، این امر سبب افزایش جرائم اینترنتی خواهد بود.

- در فرضیه ۳ عنوان شد که آیا بین افزایش جرائم اینترنتی و عدم وجود قوانین به روز و کارآمد رابطه وجود دارد یا خیر؟

بررسی ها نشان داد(با ضریب همبستگی ۰/۶۵۸ و ۰,۰۰۰ = p-value یعنی با اطمینان ۹۵ درصد) بین جرائم اینترنتی و عدم وجود قوانین به روز و کارآمد رابطه وجود دارد و فرضیه پذیرفته شد.

ارائه راهکارها و پیشنهادات

-بر اساس یافته های این پژوهش دریافتیم خلاءهای قانونی اثر بیشتری نسبت به عوامل انسانی در افزایش جرائم اینترنتی دارند و بین جرائم اینترنتی و عدم وجود قوانین به روز و کارآمد رابطه وجود دارد در این زمینه می توان گفت قانونگذاران می بایست به طور پیوسته به توسعه اینترنت پاسخ داده و موثر بودن ماده قانونی موجود را به خصوص با سرعت توسعه در فناوری شبکه دنبال کنند. که البته به روز کردن قوانین جرایم اینترنتی برای تعقیب اشکال جدید جرایم سایبری آنلاین زمانبر بوده و مجازات های قانونی نتوانسته از جرائم پیشگیری کند.و مهمترین خلاء برای روش های حقوقی کیفری تاخیر بین شناخت پتانسیل سوءاستفاده از فناوری های جدید و اصلاحیه های ضروری برای این قوانین می باشد و مادامی که سرعت ابتکارات شبکه ای دارای شتاب است این خلاء باقی می ماند.

- یافته های تحقیق نشان می دهد که هرچه آگاهی کاربران نسبت به حفظ امنیت خودشان در فضای مجازی کمتر باشد، این امر سبب افزایش جرائم اینترنتی خواهد بود و گسترش آموزش عمومی کاربران در پیشگیری از جرائم اینترنتی نقش بسزایی دارد و عوامل فردی چون عدم آگاهی و دانش در خصوص فضای مجازی می تواند اثر بیشتری در شکل گیری جرائم اینترنتی نسبت به عوامل قانونی داشته باشد. باگسترش روز افزون علم و فناوری، شیوه های ارتکاب جرم در فضاهای مجازی نیز تغییر یافته و مجرمان از شگردهای جدیدی برای کلاهبرداری، سرقت و... استفاده می کنند، که در این رابطه اطلاع رسانی و آگاهسازی کاربران از شیوه های ارتکاب جرم، نقش بسزایی در پیشگیری از وقوع جرایم اینترنتی دارد. مجرمان با جامعه ای از افراد غیر مطلع و آسیب پذیر تحت عنوان هدف مواجه هستند؛ بنابراین افزایش سطح دانش تخصصی و امنیتی و نیز اطلاع کاربران از شیوه های مقابله با شگردهای مجرمانه موجب می‌شود تعداد افرادی که به صورت بالقوه در معرض این آسیب قرار دارند، کاهش یابد؛ از سوی دیگر احتمال موفقیت مجرمان نیز در ارتکاب جرم به همین نسبت کاهش می‌یابد. بالا بردن سطح آگاهی و دانش کاربران جامعه یکی از مهمترین راه ها و ابزاری است که می تواند مانع فریب آنها توسط مجرمان سایبری گردد. اما زمینه های پیشگیری جرایم سایبری بسیار گسترده می باشد.

- بستر و زمینه مشارکت مردمی و تمامی دستگاه های دولتی و غیر دولتی خصوصا رسانه ملی (صدا و سیما) نقش مهم و بزرگی در آموزش به جامعه در جهت بالا بردن سطح آگاهی جامعه و پیشگیری از جرائم اینترنتی دارد.

- یکی از مهم‌ترین راهکارهایی که در زمینه پیشگیری از جرایم اینترنتی پیشنهاد می‌شود، آموزش از طریق نظام آموزشی است که می توان از ظرفیت آموزش‌و پروش در پیشگیری از وقوع جرم استفاده کرد.

ISSN: 2538-3787
http://www.Joce.ir

پیشنهادات پژوهشی

- با در نظر گرفتن پیچیدگی و چندبعدی بودن موضوع (عوامل موثر در ایجاد و پیشگیری از جرایم اینترنتی) لازم به نظر می رسد که تحقیقاتی صورت بگیرد که از روشهای مختلف، بخصوص از روشهای کیفی مانند مشاهده و مصاحبه استفاده شود، تا به درک عمیق تری از موضوع دست یابیم.

- تحقیقاتی صورت بگیرد که به بررسی رابطه بین میزان آموزش و آگاهی جامعه در پیشگیری از جرایم اینترنتی را در جامعه های آماری مختلف از جمله دانشجویان و دانش آموزان بپردازد و تفاوت آنها را مورد بررسی و تحقیق قرار دهد.

- بررسی عوامل موثر دیگر نظیر عوامل فرهنگی، سلامت اجتماعی و روانی بر در میزان جرایم اینترنتی انجام بگیرد.

- توصیه می شود تاثیر رسانه های تصویری و غیر تصویری از جمله تلویزیون، ماهواره، رادیو در بالا بردن سطح آگاهی جامعه در مقوله جرایم اینترنتی بررسی و مطالعه شود.

ISSN: 2538-3787
http://www.Joce.ir

منابع و مراجع

[۱] بهره مند حمید، کوره پز، حسین محمد، سلیمی، احسان(۱۳۹۳)، راهبردهای وضعی پیشگیری از جرایم سایبری، شمارهٔ ۷، آموزه های حقوق کیفری، صفحات ۱۴۷-۲۰۹.

[۲] پرچ، شعبان (۱۳۹۲)، پایان نامه ارشد(آسیب شناسی حفاظتی اینترنت بر روی کارکنان فتا.

[۳] جلالی، علی اکبر(۱۳۹۱)، رفتار شناسی مجرمان در فضای سایبر، فصلنامهٔ کارآگاه، دورهٔ دوم، سال ششم، شمارهٔ ۲۱.

[۴] جوکز، یونی و همکاران (۱۳۸۹).جرم و اینترنت، ترجمه: رسول نجار، تهران: دانشگاه علوم انتظامی امین.

[۵] خرم آبادی ع ا.(۱۳۸۶). کلاهبرداری رایانه ای از دیدگاه بین المللی و وضعیت ایران، فصلنامه حقوق، مجله حقوق و علوم سیاسی، ۳۷ (۲).

[۶] رضوی، محمد(۱۳۸۶)، جرایم سایبری و نقش پلیس در پشگیری از این جرایم و کشف آن ها، فصلنامه دانش انتظامی، دوره ۹ ، شماره ۱ ، صفحات ۱۲۰ - ۱۴۰.

[۷] سایت دبیرخانه کارگروه تعیین مصادیق محتوای مجرمانه (۱۳۹۱). مصادیق محتوای مجرمانه، قابل دسترسی در آدرس http://peyvandha.ir/gozaresh/ .

[۸] سلمان زاده، محمود، «جنگ اطلاعات و امنیت» خبرنامه انفورماتیک، سازمان برنامه و بودجه کشور، شمارهٔ ۸۰ آذرودی ۱۳۸۰، ص ۲۰.

[۹] شاهبندرزاده، حمید ، یوسفی ده بیدی، شهلا (۱۳۹۱)، تعیین درجه اهمیت جرایم رایانهای از دیدگاه صاحب نظران انتظامی استان بوشهر ، فصلنامه نظم و امنیت انتظامی، سال پنجم، شماره اول ، صفحات ۱۳۷-۱۵۵ .

[۱۰]شاه محمدی، غلامرضا، تاهو، منصور(۱۳۹۳)، بررسی شیوه های پیشگیری از جرایم سایبری، مبتنی بر فناوری اطلاعات، پژوهش های اطلاعاتی و جنایی، دوره ۹ ، شماره ۳ ، صفحات ۹۹ -۱۱۹ .

[۱۱]صحرا رستمی(۱۳۹۲)، پایان نامه کارشناسی ارشد ، پیشگیری از جرایم رایانه ای، دانشگاه آزاد اسلامی واحد خوراسگان

[۱۲]عباچی، مریم (۱۳۸۷).مبانی و مقدمات تدوین برنامه ملی پیشگیری از جرم در ایران، فصلنامهٔ مطالعات پیشگیری از جرم، تحقیقات کاربردی پلیس پیشگیری ناجا، سال سوم، شمارهٔ نهم، صص ۷۲-۲۳.

[۱۳]کوچی، سعید، داودی، ابراهیم(۱۳۹۴)، نقش آموزش کارکنان در پیشگیری از جرائم فضای مجازی (مطالعه موردی کارکنان فرماندهی انتظامی تهران بزرگ)، فصلنامه پژوهشهای حفاظتی ـ امنیتی دانشگاه جامع امام حسین(علیه السلام)، سال سوم، شمارهٔ ۱۳، صفحات ۶۹ – ۸۹ .

[۱۴]نشریه آموزه های حقوق کیفری : بهار و تابستان ۱۳۹۳ , دوره - , شماره ۷ ; از صفحه ۱۴۷ تا صفحه ۱۷۶.

[15] Kizza, Joseph M., Guide to Computer Network Security, London, Springer Publications Ltd., 2013.

[16] Higgins, G. E., & Fell, B. (2005). An application of deterrence theory to software piracy. Journal of Criminal Justice and Popular Culture , 166–184.

[17] Higgins, G. E., & Ricketts, M. L. (2009). Digital piracy: A latent class analysis.Social Science Computer Review , 24–40.

[18] Higgins, D. (2007). Digital piracy: An examination of low self-control and motivation using short-term longitudinal data. cyberpsychology & Behavior 10 ,523-529.2004].